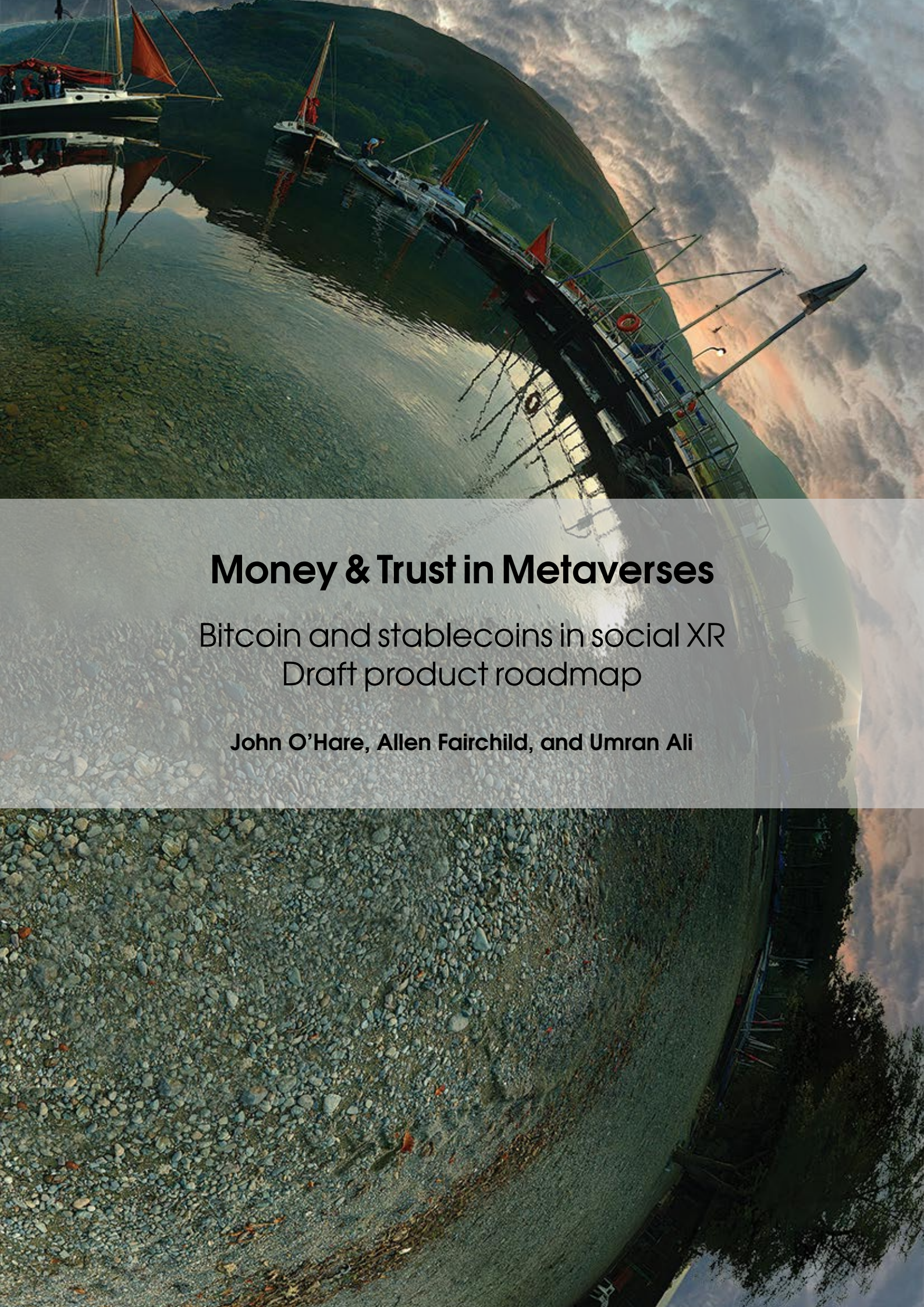


Money & Trust in Metaverses

Bitcoin and stablecoins in social XR
Draft product roadmap

John O'Hare, Allen Fairchild, and Umran Ali

Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)
2022 John O'Hare & Allen Fairchild & Umran Ali

PUBLISHED BY JOHN@XRSYSTEMS.UK (R&D LEAD - PATHWAY)

RAW GITHUB HYPERLINK

You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.
Under the following terms:

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

First printing, March 2022



Contents

I State of the art and proposal

0.1 Conflict of interest statements . . . 13

1 Introduction . . . 14

1.1 Overview . . . 14

1.2 Introduction . . . 16

1.2.1 Notes on progress . . . 19

2 Decentralisation& Web3 . . . 21

2.1 Semantic web . . . 21

2.2 Spatial web . . . 23

2.3 Web3 . . . 24

2.3.1 Emerging consensus . . . 24

2.4 Example applications . . . 27

2.4.1 Podcasting2.0 . . . 27

2.4.2 Crowd funding . . . 27

2.4.3 Distributed exchanges . . . 27

2.4.4 NFT marketplaces . . . 27

2.4.5 Non blockchain webs of trust . . . 28

2.4.6 Distributed DNS applications . . . 28

2.4.7 Impervious browser . . . 28

2.4.8 TBD - Web5 . . . 29

2.5 The common thread . . . 29

3 DLT, Blockchain, and Bitcoin . . . 31

3.1 What's this for sorry? . . . 34

3.2 A panoply of tech . . . 35

3.3 Ethereum **36**
3.3.1 Mining and Gas 38
3.3.2 Upgrade roadmap 38
3.4 Bitcoin **40**
3.4.1 The Bitcoin Network Software 42
3.4.2 Mining and Energy concerns 42
3.4.3 Technical overview 48
3.4.4 Upgrade roadmap 53
3.5 Extending the BTC ecosystem **55**
3.5.1 Keet by holepunch 55
3.5.2 Block & SpiralBTC 55
3.5.3 BTCPayServer 55
3.6 Lightning (Layer 2) **56**
3.6.1 Micropayments 57
3.6.2 BOLT12 and recurring payments 57
3.6.3 Fedimint and Fedi app 57
3.6.4 LNURL-auth 59
3.6.5 LNBits 59
3.6.6 Etleneum 60
3.6.7 Message passing 60
3.7 Liquid federation (layer 2) **60**
3.8 Bitcoin Layer 3 . . . . . **62**
3.8.1 LNP/BP and RGB 62
3.8.2 Taro 64
3.8.3 Slashpay 65
3.8.4 Spacechains 65
3.8.5 Statechains, drivechain, softchains 66
3.9 Other chains and networks **66**
3.9.1 Layer 1 chains 66
3.10 Risks and mitigations **68**
3.10.1 Digital assets 69
3.10.2 Bitcoin specifically 70

4 Money in the real world **72**
4.1 Defining money **72**
4.1.1 Global currency interactions 73
4.2 International money transfer networks **74**
4.2.1 Swift, ISO 20022, and correspondence banking 75
4.2.2 VISA etc 75
4.2.3 Money transfer operators 75
4.2.4 Digital disruptive fintech 75
4.2.5 Stablecoins 77

4.3 Central bank digital currencies . . . 81
4.4 Bitcoin as a money . . . 85
4.4.1 Spending it . . . 85
4.4.2 Saving with it . . . 87
4.5 Risks (money, not technical) . . . 89
4.5.1 Risks to Bitcoin the money . . . 89
4.5.2 Bitcoin externalities . . . 91
4.6 Does DeFi matter to SMEs . . . 96
4.7 Do DAOs matter to SMEs . . . 97
4.7.1 Bisq DAO . . . 98
4.7.2 Risks . . . 98

5 Distributed Identity & Trust . . . 99
5.1 Applications of DID/SSI . . . 99
5.2 Classic DID/SSI . . . 100
5.3 Newer Technologies . . . 101
5.3.1 Lightning . . . 101
5.3.2 Slashtags . . . 101
5.3.3 Microsoft ION . . . 101
5.3.4 Nostr . . . 102
5.4 Micropayment based web . . . 103
5.5 Risks & Challenges? . . . 103

6 Non Fungible Tokens . . . 105
6.1 NFT key use cases . . . 107
6.1.1 Art . . . 107
6.1.2 Computer & Video Games . . . 111
6.2 Broader and metaverse uses . . . 114
6.3 Objects in our metaverse . . . 115
6.3.1 Liquid tokens . . . 115
6.3.2 Sovryn and RSK . . . 116
6.3.3 Stacks and STX . . . 116
6.3.4 Ethereum . . . 116
6.3.5 Solana . . . 116
6.3.6 Satoshi Ordinals . . . 116
6.3.7 Peerswap . . . 116
6.3.8 FROST on Bitcoin . . . 116
6.3.9 Spacechains . . . 117

7 Metaverses . . . 118
7.1 Toward an open metaverse . . . 118
7.1.1 Primitives . . . 119

7.2 History **121**
7.3 Video conferencing, the status quo **122**
7.3.1 Pandemic drives adoption 123
7.3.2 Point to Point Video Conferencing 125
7.3.3 Triadic and Small Group 125
7.3.4 Other Systems to Support Business 126
7.3.5 Mona Lisa Type Effects 126
7.4 What's important for human communication **127**
7.4.1 Vocal 127
7.4.2 Nonverbal 128
7.5 Psychology of Technology-Mediated Interaction **133**
7.5.1 Proxemics 133
7.5.2 Attention 135
7.5.3 Behaviour 135
7.5.4 Presence, Co-presence, and Social Presence 136
7.6 Other Systems to Support Business **138**
7.6.1 Spatially Faithful Group 139
7.6.2 Holography and Volumetric 140
7.6.3 Simulated Humans 140
7.7 Theoretical Framework toward metaverse **143**
7.7.1 Problem Statement 143
7.7.2 Core Assumptions 143
7.7.3 Peripheral Assumptions 145
7.8 Post 'Meta' metaverse **145**
7.9 Market analysis **146**
7.10 NFT and crypto as metaverse **148**
7.11 Immersive and third person XR **148**
7.11.1 More like a digital twin 149
7.11.2 More like a metaverse 149
7.11.3 More like crypto NFT virtual land 151
7.11.4 More like industrial application 152
7.11.5 More like meeting support 152
7.12 The future **154**
7.12.1 Mixed reality as a metaverse 154
7.12.2 Augmented reality 154
7.12.3 Ubiquitous displays 154
7.13 Risks **154**
7.14 TL;DR **155**

8 Our proposition **157**
8.1 Money in metaverses **157**
8.1.1 AI economic actors in mixed reality 157

8.2 Our socialisation best practice . . . 157
8.2.1 Emulation of important social cues . . . 158
8.2.2 Federations of webs of trust and economics by Melbots . . . 159
8.3 Security evaluation . . . 159
8.4 Potential applications . . . 159
8.4.1 Global cybersec course delivery . . . 160

II Guides for deploying the software

8.5 Lab - virtualisation, networking, Bitcoin . . . 164
8.5.1 Overview . . . 164
8.5.2 Prerequisites . . . 164
8.5.3 Network details . . . 164
8.5.4 Server configuration . . . 164
8.5.5 Proxmox VE . . . 164
8.5.6 Setup an internal only network in Proxmox VE . . . 166
8.5.7 Install and configure Internet gateway server virtual machine . . . 166
8.5.8 Install and configure a Debian virtual machine . . . 168
8.5.9 Deploying the nix-bitcoin node . . . 169
8.6 Lab - Vircadia . . . 175
8.6.1 Overview . . . 175
8.6.2 Deploy a Vircadia domain server . . . 175
8.6.3 Deploy a Vircadia metaverse server . . . 181

III Appendix

8.7 Acknowledgements and thanks . . . 195
8.8 Author Biographies . . . 195



List of Figures

1.1 The landing page of global financial giant Goldman Sachs shows the hype. 17
1.2 PGIM cite the 'digiconomist' paper 17
1.3 The Gartners Hype Cycle for 2022. 19
1.4 Web 3, Metaverse, and Bitcoin are inter-sectional technologies. 20

2.1 Semantic Web Stack (CC0 image) 22
2.2 Deloitte Spatial Web Overview Reused with permission. 23
2.3 Edelman 2020 trust barometer (rights requested) 24
2.4 A meme showing differing approached to logging in on a website. 25
2.5 DNSSEC ceremony in a faraday cage 29
2.6 ARK slide on Web3. Rights requested 30

3.1 Dan Held: Bitcoin prehistory used with permission. 32
3.2 Bitcoin Topics used with permission @djvalerieblove. 32
3.3 Intersecting disciplines. Reused with permission Dhruv Bansal 33
3.4 The narrative use of Bitcoin has evolved, by Nic Carter and Hasufly. 34
3.5 "This new chart from Block is financial privilege visualized." 35
3.6 Ethereum is thought to look like a speculative bubble. Rights requested . 37
3.7 The rate of token generation has changed unpredictably over time. Rights requested 39
3.8 Growth in settlement value on the Bitcoin network (Forbes). 41
3.9 Bitpaint: Contributions to the Bitcoin ecosystem. Reused with permission. 42
3.10 Bitcoin network vs TOP500 supercomputers 43
3.11 Intimate tie between energy and money, Henry Ford 44
3.12 Hash rate suddenly migrates from China (Reuse rights requested) 45
3.13 Goldman suggest growth opportunity and potential demonetisation of gold? 47

3.14 Given a start point on the curve and a number of reflection operations it's trivial to find a number at the end point, but impossible to find the number of hops from the two end points alone. (CC Mastering Bitcoin second edition) 50
3.15 Seedsigner is an inexpensive open source project which scans the master seed in from a QR code to enable signing. One device can run a quorum based wallet (multisig). 53
3.16 Arcane research lightning adoption overview. 58
3.17 A key fob with a Bolt12 QR code 59
3.18 Two of the many prebuilt and kit options for Lightning 'point of sale' . . . 61
3.19 Allocations given at the beginning of public blockchain, by Messari. . . 67

4.1 Comparison of mobile based payment systems 76
4.2 The UK signs into law regulation of digital representatives of value 80
4.3 More than half of central banks surveyed by the BIS said they saw issuance of a CBDC as possible. 82
4.4 Potential market exposure to Bitcoin as a money 88
4.5 Nassim Taleb's Turkey Problem 91
4.6 Cycle theory revisited blog post (Image used with permission) 92
4.7 Bitcoin distribution is skewed to s few early holders, but it likely **is** fair. (Image used with permission) 93
4.8 Supply of bitcoin that hasn't moved for over 1 year 93

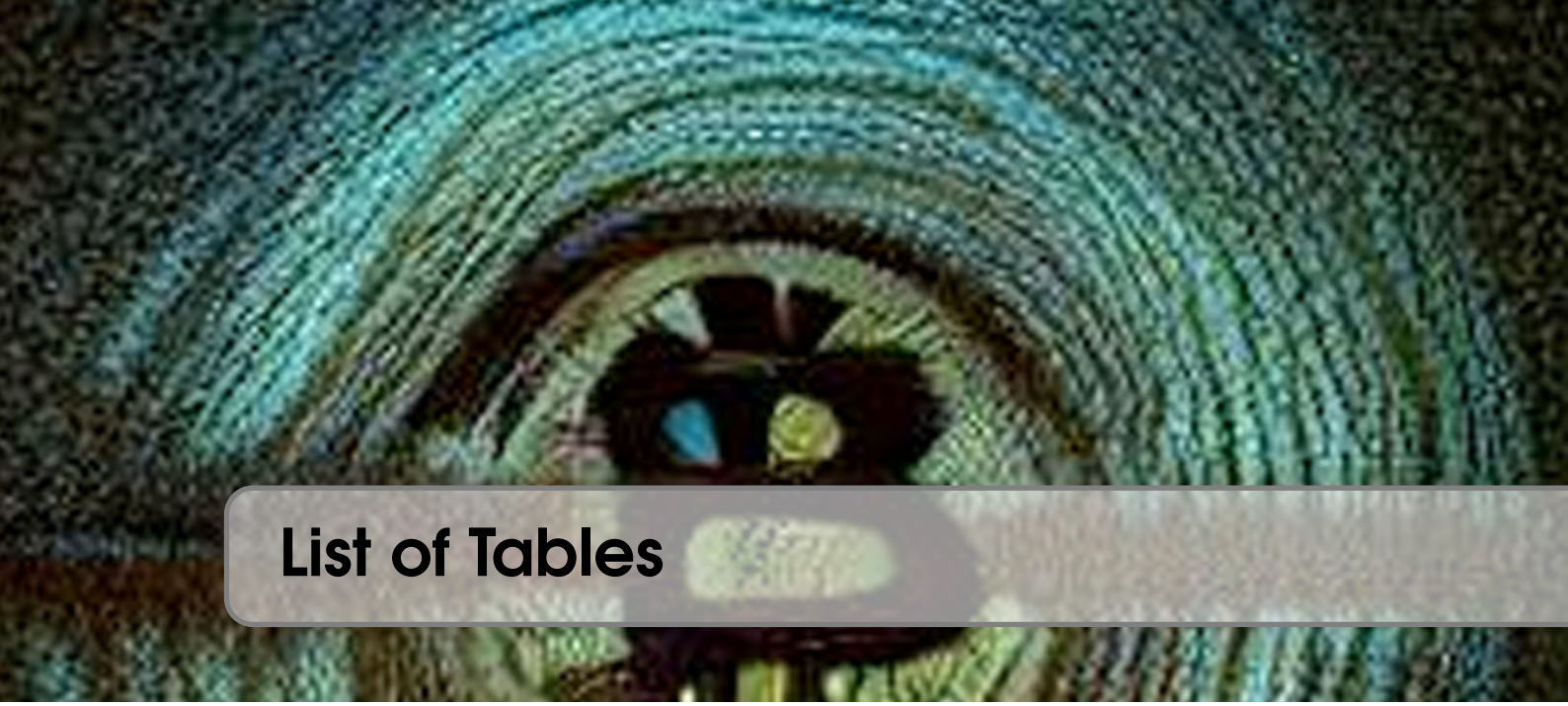
5.1 Part of the DID SSI specs 100
5.2 Comparison of distributed file stores 104

6.1 Solana NFT markets are enjoying growth compared to Opensea on Ethereum, even in the downturn. 106
6.2 Beeple: First 5000 days, taken from the Christies website, assumed fair use. 108
6.3 The bubble bursts on Yuga Bored Apes for now. 111

7.1 Elon Musk agrees with this on Twitter. It's notable that Musk is now Twitters' biggest shareholder, and has been vocal about Web2 censorship on the platform. 122
7.2 Eye tracked eye gaze awareness in VR. Murray et al. used immersive and semi immersive systems alongside eye trackers to examine the ability of two avatars to detect the gaze awareness of a similarly immersed collaborator. 133
7.3 Bands of social space around a person Image CC0 from wikipedia. . . . 134
7.4 The Venn diagram shows areas of research which have been identified in blue. These interlock and overlap as shown. The most relevant identified researchers from the literature are shown in black close to the fields of study which they represent. This diagram is a view of the core assumptions for the research, with the most important fields at the centre. 144
7.5 IPSOS poll predicted applications 148

8.1 High level overview showing the components for sats, stablecoins on lightning, asssets, and trust 158
8.2 Functional elements for infrastructure. 161
8.3 Client server C4 diagrams. 162

8.4 Ubuntu 20.04 Desktop Settings 176
8.5 Ubuntu 20.04 Desktop Settings - Network 177
8.6 Vircadia build settings and installation screen grab 178
8.7 Vircadia build Qt warning 178
8.8 Vircadia server configuration landing page 180
8.9 Vircadia server configuration import page 181
8.10 Vircadia server configuration import page 182
8.11 Vircadia server configuration import page 183
8.12 Vircadia server configuration import page 184
8.13 Vircadia server configuration import page 185



List of Tables

State of the art and proposal

1 Introduction 14

2 Decentralisation& Web3 ... 21

3 DLT, Blockchain, and Bitcoin 31

4 Money in the real world ... 72

5 Distributed Identity & Trust . 99

6 Non Fungible Tokens 105

7 Metaverses 118

8 Our proposition 157

0.1 Conflict of interest statements

The authors may own small numbers of the various tokens referenced in the text for experimentation and/or investment purposes. At this time that is only sufficient Ethereum to operate a Web3 wallet, and Bitcoin locked on the Lightning network. No NFTs are owned at this time. There are no financial stakes in the development of any of these ecosystems.



1. Introduction

1.1 Overview

Money is a social construct, like trust. Both are very important and ephemeral things, and are being tested in a global digital world. We are a long way from the village structures in which we evolved. We are now expected to casually adapt to the efficiencies promised by teams working in global mixed reality. This chaotic and intangible mix of value, trust, and socialisation is not well understood.

We wanted to explore exciting new developments in the transmission of value, and trust, in metaverses. The problem is that each of these topics alone are enormously complex, and the intersections seem to be more so. We have been researching the current state-of-the-art, and the emerging consensus narrative, to try to figure out how the collision of these technologies might serve smaller scale businesses.

We started out with security best practices in mind. How can we enable small and especially developing companies, to have a foot in the door on a global stage, without their cybersecurity costs spiralling?

Fortunately, we discovered a wealth of carefully crafted open source tools which can support this exploration. We have tried to assemble them cogently, to deliver a kit for experimentation, to curious technically minded SMEs, and we have applied our own security knowledge on top of an already top class set of tools. It's certainly not production ready, but it's good enough to commit small amounts of money into, for experimentation purposes.

Whilst researching, it seemed that every door we opened was full of interesting and useful treats. What was supposed to be a short technical paper quickly became a 200-page book, and a deployable virtual machine stack, with a dozen different open source components in it.

To that end, this book supports the virtual machine and software stack, which supports anyone who thinks this material might be useful. Below is a précis of the chapters of the book, which will hopefully give an insight into what "this stuff" is. The reader can decide to download the book and the system "How To" guide. All of it is open source, all of it can be contributed to on GitHub, all of it will be developed forward, and none of it is really finished yet.

Chapter 1 is an introduction to the book which is about value transmission, with distributed trust, in global social mixed reality systems.

Next is a summary of Web3, as it stands right now. Web3 is a complex term that is cropping up far more in the technical press, so we wanted explain what it might mean. Honestly, it's still pretty confusing. There are a bunch of legacy explanations which are Web3.0 (note the '0' there), but these are withering on the vine. Then there's the new VC funded, super hyped, and potentially useless Web3 incarnations, which again cover a slew of intersecting technologies. Note they dropped the zero to reboot the brand! This doesn't mean there's nothing to see here. The astonishing amount of money and developer talent, and the clear market hunger for things like NFTs (non-fungible tokens) suggest that there's a future for Web3, it's just really unclear what the value could be for our curious SME.

In the next chapter we took a look at blockchain, which is very intersectional with Web3. Even on its own this is a very complex emergent set of disciplines.

The blockchain chapter was especially interesting to research. It turns out there's a *lot* of ways to get this technology wrong. Even very appealing options on paper, turn out to have very shaky foundations. There are really valuable things here, but given the complexity, and the size of that chapter, we decided to focus down on the most promising of the technology stacks, which interestingly turned out to be the original; the Bitcoin network.

Even Bitcoin isn't just Bitcoin anymore. It's a swarm of open source tools which can (in theory) accomplish a great many things. These newer, ancillary elements to Bitcoin, are emergent right now. Some of them won't be around until later in the year and it's questionable whether they will even work out. With that said there's already enough here for us to cherry pick some useful components and start to map those forward into our metaverse proposal.

In looking around at the available options, it seems possible that the features which are important to Web3, can also (potentially) arise from the Bitcoin technology that we think most secure. This was somewhat unexpected, so we started mapping that over too.

The next chapter is about Money. In expanding our research on Bitcoin, we found that it's impossible to think about the tech without opening up a whole line of questions about money itself. This is fine because we set out to look at global value transfer for business. It's not a trivial subject though, and this section tries to overview why value and Bitcoin are so enmeshed, then what other options there might be in the end (because Bitcoin has kicked off a whole slew of global adoption outside of itself).

The distributed identity management, and trust chapter follows. Identity management is crucial to metaverse applications which have a value transaction layer. It's not an easy section to write about, because there's a lot of research, it's not our field, and finding the value to SMEs has actually been very difficult. It's by no means clear that blockchain is the right tool for this component, and newer cryptographic products are emerging. This section is likely to be overhauled a few times in the coming months as we settle on technologies that we believe are simple and secure enough.

In chapter 7 we take another look at NFTs. It's impossible to ignore this stuff now. It's fundamentally a bit broken, but there are probably use cases, and the money and development attention it's getting are incredible. We try to navigate our hypothetical SME through this as best we can. It's not that we didn't understand it completely, just that the tech moves so very fast that it's impossible to even describe what's going on accurately at any given point.

We're actually pretty excited about future versions of this technology, based around Bitcoin, because that allows us to keep just one value stack in the lab. We've mapped that forward into the open source tools that we recommend. This very much ended up looking like our priors; our cyber security values, and our wish to build toward a simpler product using only Bitcoin. To broaden the discourse a little asked another author, with much more of a foot in the content creation world, to collaborate with us on this chapter. This will benefit from smoother integration over the coming months.

Chapter 8 is a big one for us as it's our research area prior to opening up the Bitcoin box(es). Metaverse, or at least one of the current definitions of metaverse, is just social interaction in mixed reality (VR/AR/XR). We've been studying that for decades, so this section is more academic and tried to boil down what we think is most important to map forward into the server stack. The choices we made here guided us toward the selection of free and open source metaverse software, which we selected from a bunch that we reviewed. You can make your own choices and gain insight from the systems we looked at.

We also take a look at the other definitions of metaverses which are doing the rounds on the web, try to unpick which is which, and what they are for, then we attempt to weave back together the best of both. This ends up looking a bit like the Venn at the top of the book, where we have transmission of provable identity, non-fungible tokens bearing value or data, distributed files, actual money (including micropayments) and a social layer based on our best knowledge about mixed reality.

It's exceptionally fortunate timing for this book that the UK government has signalled enthusiasm for so called 'stablecoins' at the same time that the Bitcoin network is being upgraded to transmit these GBP equivalent tokens around. This gives us a very good idea what it is we can build into our application stack to support businesses.

Past this stage in the book we get into the murky and half developed tail end, where we're interfacing with our design choices, and the stack which can be deployed into the cloud.

1.2 Introduction

This document presents a high level view of technologies and their potential within the emergent Web3 and metaverse narrative, focusing around the transmission of value within and across such global networks, with a further focus on the Bitcoin monetary network. It was written to organise the thoughts of the authors, who were unfamiliar with Bitcoin technologies until recently.

As adoption of these technologies increases it will be necessary for people, and AI actors, to pass economic value between themselves. These 'goods and services' interactions, within the virtual social spaces should be underpinned by a trust system, which scales globally and presents low friction. Current secure international payment rails are poorly suited to such interactions; indeed it is likely with legacy systems, that parties would be forced to leave the metaverse application, and instead navigate their banking applications to exchange value with overseas entities in a secure fashion. This might conceivably take several days.

Fortunately, the whole landscape of money and value transfer is changing. Huge global financial players are entering the space. HSBC have just bought metaverse 'land' in The Sandbox, JP Morgan have opened a 'lounge' in another. The worlds largest hedge fund Bridgewater is stepping into acquisition of digital assets, and the world's largest

pension fund manager Blackrock partnered with Coinbase and is adding these asset to their management engine (which manages tens of trillions of dollars). Fidelity asset management are about to add Bitcoin to their pension plans and are offering a dedicated metaverse tradable fund, while Citigroup have a minisite dedicated to "Metaverse and Money". The front page of Goldman Sachs recently says it all (Figure 1.1).

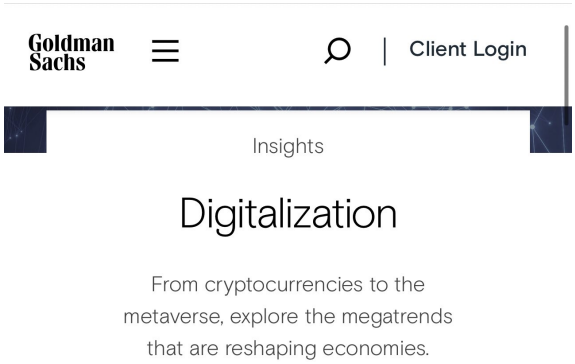


Figure 1.1: The landing page of globalfinancial giant Goldman Sachs shows the hype.

In Gartners 2022 hype cycle report one of their three "trend themes" says: *"The future of digital experience is immersive. A collection of emerging technologies supports such experiences through dynamic virtual representations, environments and ecosystems of customers and people, as well as new modes of user engagement. With these technologies, individuals can control their own identities and data and experience virtual ecosystems that can be integrated with digital currencies. These technologies help reach customers in new ways to strengthen or open new revenue streams. The technologies to watch that deliver evolving and expanding immersive experiences are metaverse, non-fungible tokens (NFTs), super apps and Web3, decentralized identity, digital humans, digital twin of the customer and internal talent marketplaces."*

Of their recent investments KPMG global said: *"We've invested in a strong cryptoassets practice and we will continue to enhance and build on our capabilities across Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs) and the Metaverse, to name a few"*. This is not to say that all fund managers are so positive. PGIM who manage over a trillion pounds globally have come out very strongly against the technology, with a slew of reports to warn off investors (Figure 1.2).

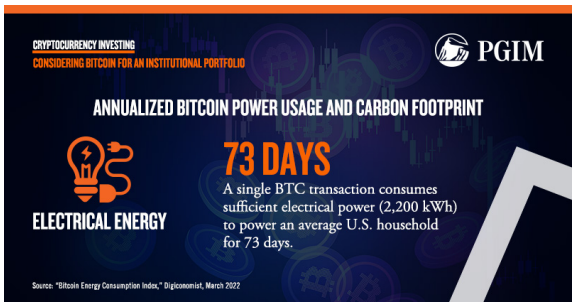


Figure 1.2: PGIM cite the 'digiconomist' paper

It's possible that for such organisations it makes better business sense to take a punt on hype bubbles like this, than to do a proper due diligence with a team of internal staff

who understand their business. These endorsements should be taken with a large pinch of salt. As Alex Johnson says: *"At some point in the future, it's possible that the digital worlds being built today will have aggregated sufficient user attention and engagement that financial services companies will need to invest in the metaverse as an acquisition and customer service channel. But we're not there yet. Until the metaverse is a little less empty, resist the temptation to colonize it with branches and billboards."*

Meanwhile, Meta (ex Facebook) are launching their own META Web3 and metaverse token (after abandoning Libre, their global cryptocurrency), and Google have recently blogged: *"Web3 also opens up new opportunities for creators. We believe new technologies like blockchain and NFTs can allow creators to build deeper relationships with their fans. Together, they'll be able to collaborate on new projects and make money in ways not previously possible. For example, giving a verifiable way for fans to own unique videos, photos, art, and even experiences from their favourite creators could be a compelling prospect for creators and their audiences. There's a lot to consider in making sure we approach these new technologies responsibly, but we think there's incredible potential as well. Finally, we couldn't have a piece about innovation without touching on the metaverse! We're thinking big about how to make viewing more immersive. "*

It's already the case that the recent bubble of hype is dwindling, but the enormous investment into teams and startups will potentially bear fruit in the next couple of years, and this perhaps has implications for small and medium-sized enterprises (SMEs).

In the UK the government has stated it's ambition to be a global cryptoasset technology hub, and announced plans for the Royal Mint to issue a (novelty) NFT. Like the assertion by major global businesses it is too early to tell how 'sticky' these claims are, but the UK legal system is clear in it's view that all crypto assets are 'property'.

A Law Commission consultation on "digital assets" has proposed a new **third category** of property:

- *it is composed of data represented in an electronic medium, including in the form of computer code, electronic, digital or analogue signals;*
- *it exists independently of persons and exists independently of the legal system;*
- *it is rivalrous such that use by one prejudices the ability of others;*

Consensus seems to be that this is a thorough paper, and demonstrates strong knowledge of digital assets by the authors.

Gartner's hype cycle 2022 features Web3, distributed identity, NFTs, and Metaverse and can be seen in Figure 1.3. With all this attention it seems timely to explore the potential of recent technologies, which can address metaverse interactions in *business to business* (B2B), *business to customer* (B2C), and the newer C2C (social commerce; *creator to consumer, customer to customer, consumer to consumer[1])*. Figure 1.4 demonstrates how some of these domains intersect.

This book seeks to overview and explain the available open source technologies. It supports an open source github repository which enables SMEs to access these emergent platforms and ecosystems. It aims to build toward a minimum viable product for trust minimised transfer of value within a social immersive space.

Referencing is in two styles; academic works and books are numeric, while opinion pieces, gray statistics, and pertinent news articles are hyperlinked from the text. This hybrid style yields about twice the citation density of a normal PhD thesis, which is a lot. For this reason the normal blue hyperlink colour was eschewed in favour of a more aesthetic "gray". There is also a version of the PDF which complies with accessibility best

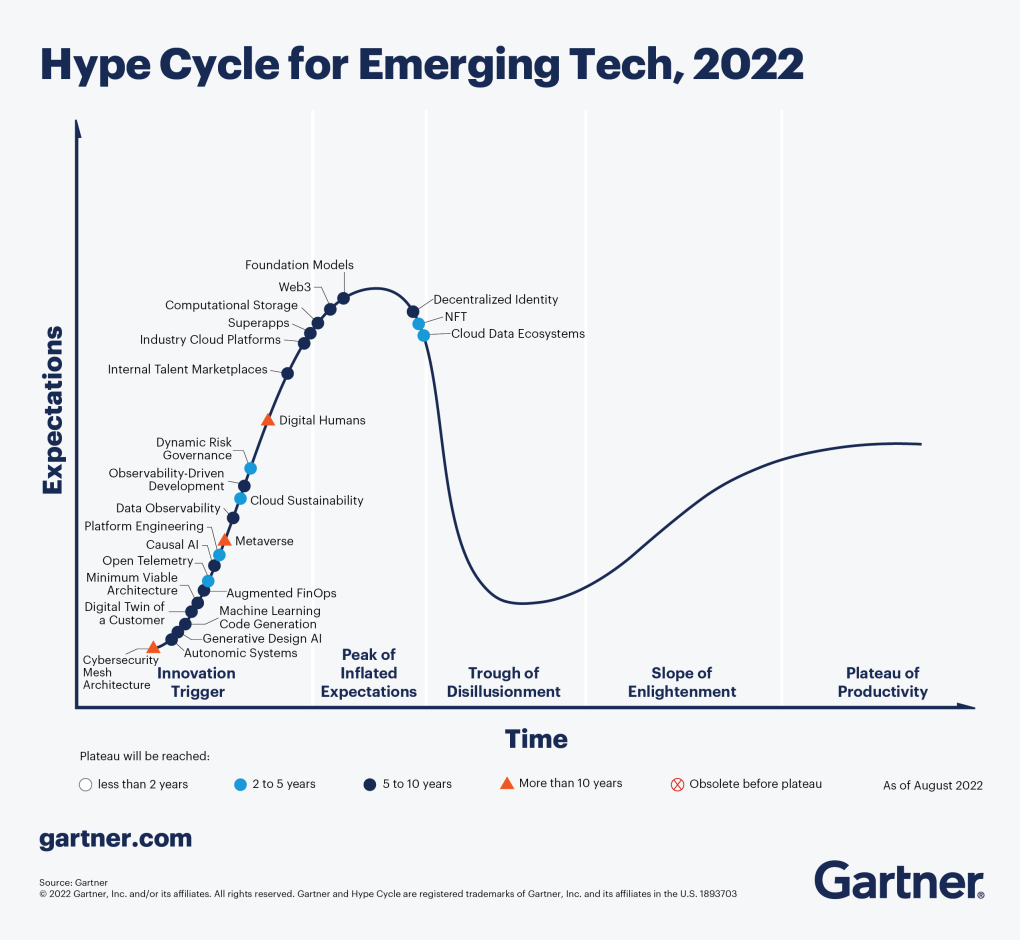


Figure 1.3: The Gartners Hype Cycle for 2022.

practice if this is a problem.

1.2.1 Notes on progress

This version of the book is "minimally complete". The real interesting work of combining the primitives into a new direction for integration of Bitcoin and VR is just beginning. We are now inviting the wider community to submit pull requests into github as contributors. It's been a useful document creation process to form our thoughts, and it's enough to bring a reader up to "the state of the art" if all of the thousand links and papers are considered. It's an open ended project though.

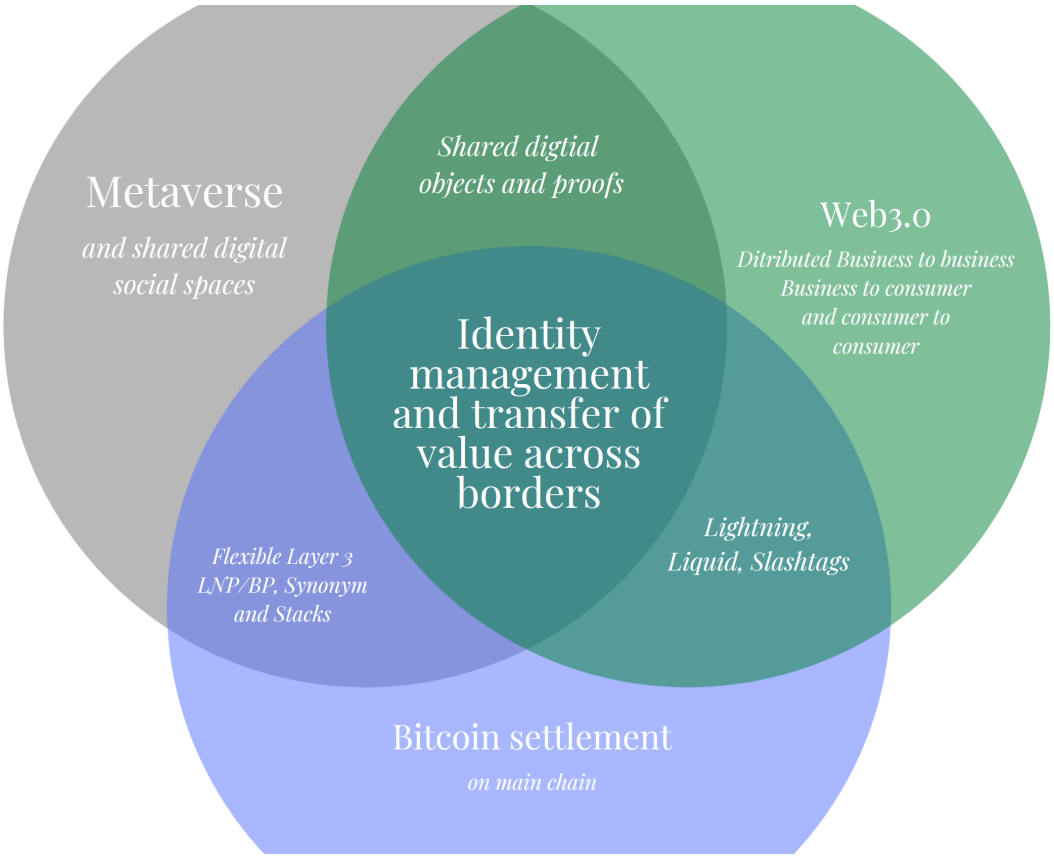


Figure 1.4: Web 3, Metaverse, and Bitcoin are inter-sectional technologies.



2. Decentralisation& Web3

When this chapter was first started in early 2022 ‘Web3’ was at the peak of it’s hype. Web3 is still a rapidly evolving set of technologies and specifications, which are drifting further from their origin. Decentralised web is perhaps a more useful name.

2.1 Semantic web

The “semantic web” definition of Web3.0 has been somewhat overhauled by other innovations in decentralised internet technologies, now evolving toward the slightly different Web3 moniker. Tim Berners Lee (of WWW fame) first mentioned the semantic web in 1999 [2].

“I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A "Semantic Web", which makes this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The "intelligent agents" people have touted for ages will finally materialize.”

Attention developed around three core themes, ubiquitous availability and searchability of data, intelligent search assistants, and highly available end points such as phones, and ‘internet of things’ devices. This is certainly manifesting in home devices, but few people think of this as a Web3 revolution. The framework can be seen in Figure 2.1.

Since ratification of the standards by the World Wide Web (W3C) consortium it seems that their imperative toward decentralisation has become lost. Instead, it can be seen that Facebook, Amazon, Google, and Apple have a harmful oligopoly on users data [3]. This is at odds with Berners-Lee’s vision, and he has recently spoken out about this discrepancy.

It is worth taking a look at his software implementation called Solid, which is far more mindful of the sovereignty of user data.

“Solid is an exciting new project led by Prof. Tim Berners-Lee, inventor of the World Wide Web, taking place at MIT. The project aims to radically change the way Web applications work today, resulting in true data ownership as well as improved privacy. Solid (derived from "social linked data") is a proposed set of conventions and tools for building decentralized social applications based on Linked Data principles. Solid is modular and

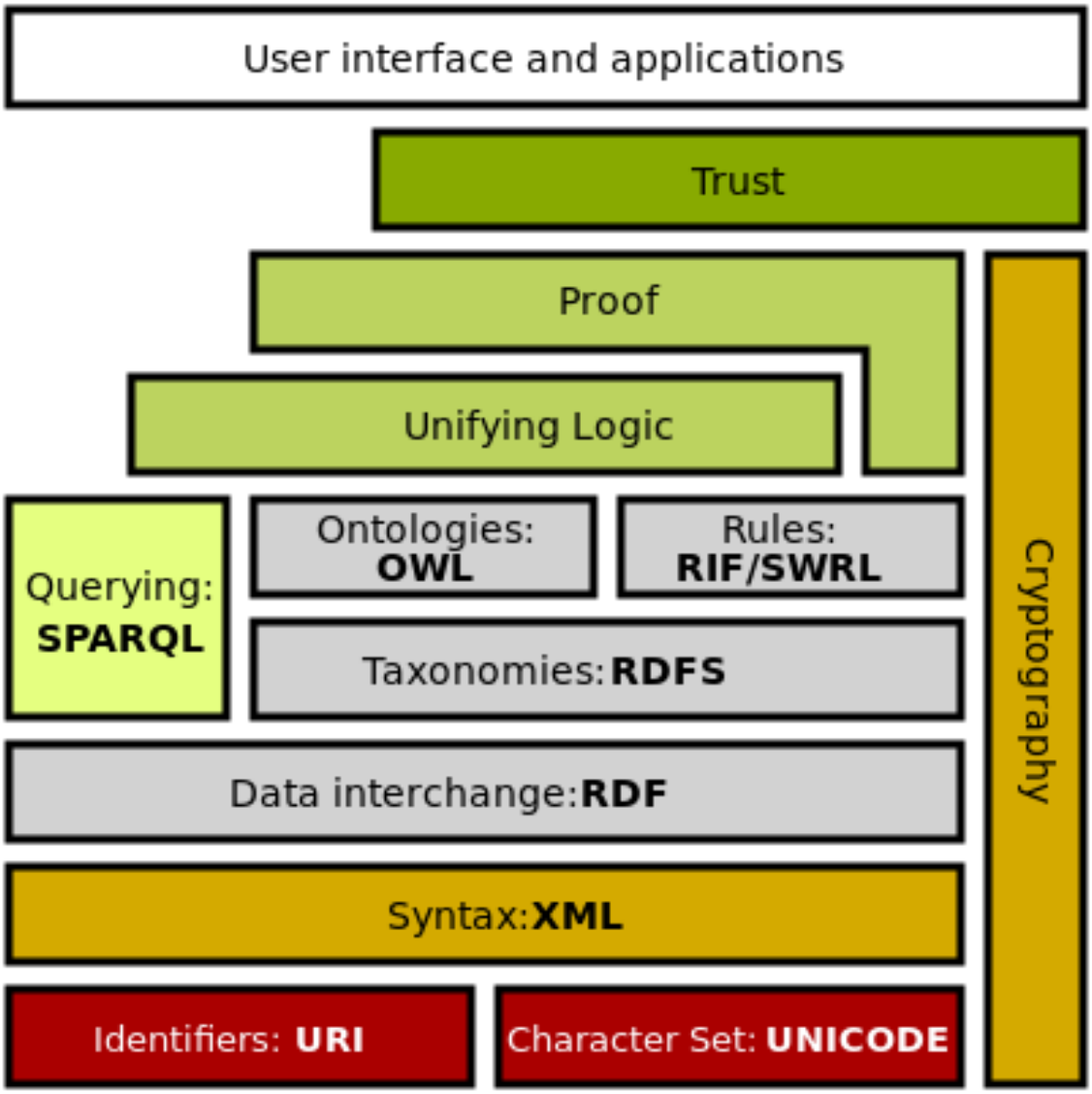


Figure 2.1: Semantic Web Stack [CC0 image]

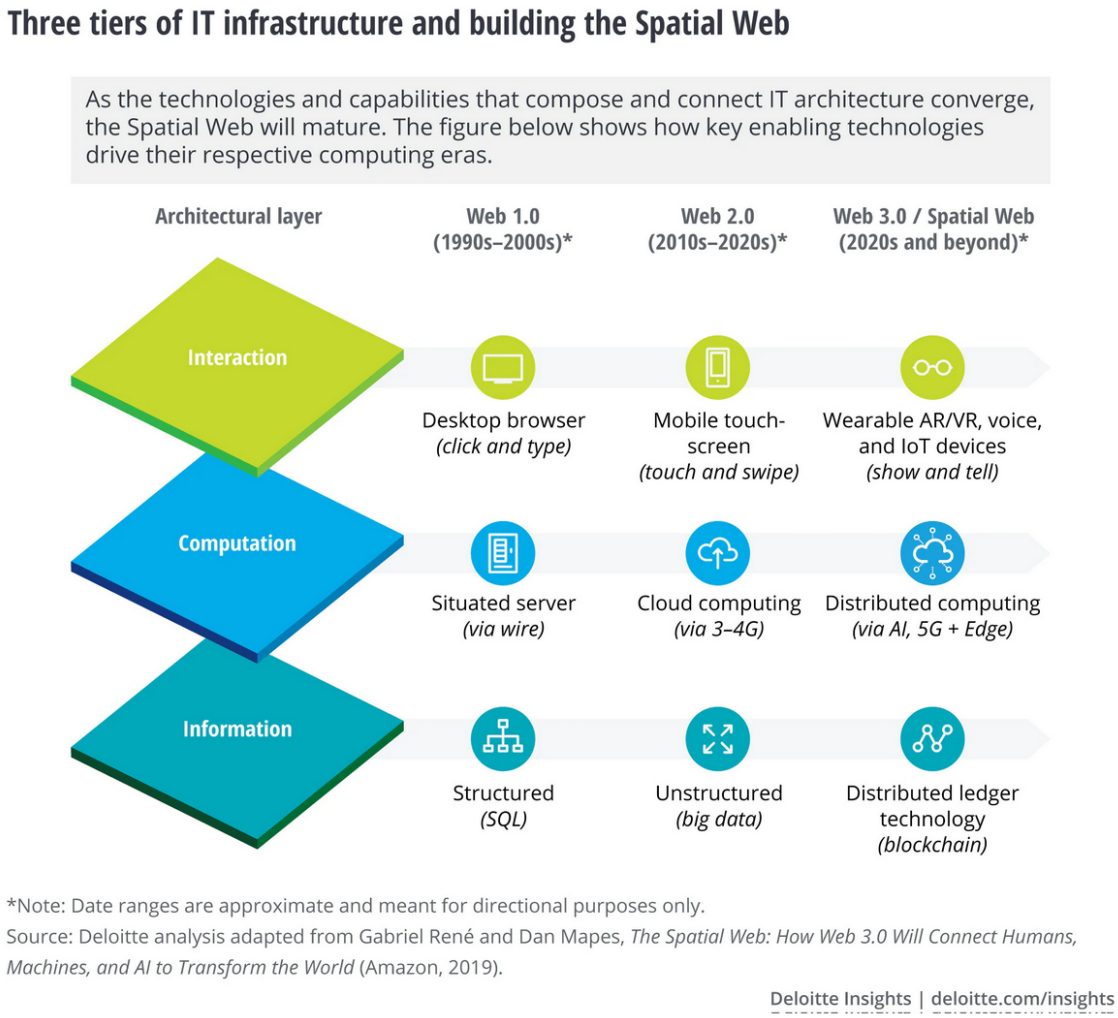


Figure 2.2: Deloitte Spatial Web Overview Reused with permission.

extensible and it relies as much as possible on existing W3C standards and protocols."

Excitement around this kind of differentiated trust model, hinted at in ubiquitous availability of data (and implemented explicitly in Solid), has led to exploration of different paths by cryptographers, and this will be described later. For instance, one of the main developers of Solid, Melvin Carvelho, is now a lead developer at Nostr, another very interesting option which will be described later. This technology space is prolific, but still comparatively young and small.

2.2 Spatial web

"The Spatial Web", a blurring of the boundaries between digital and geospatial physical objects, seems to have developed from the strands in the original W3C scope around devices in the real world. It has been concentrating around AR and VR but is being marketed and amplified with the same references to availability of data (See Figure 2.2 from a Deloitte accounting report). This too is finding little traction in practice, though obviously the component technologies continue to enjoy rapid development. Nonetheless, this interpretation of Web3 becomes valuable when examining Metaverse later.

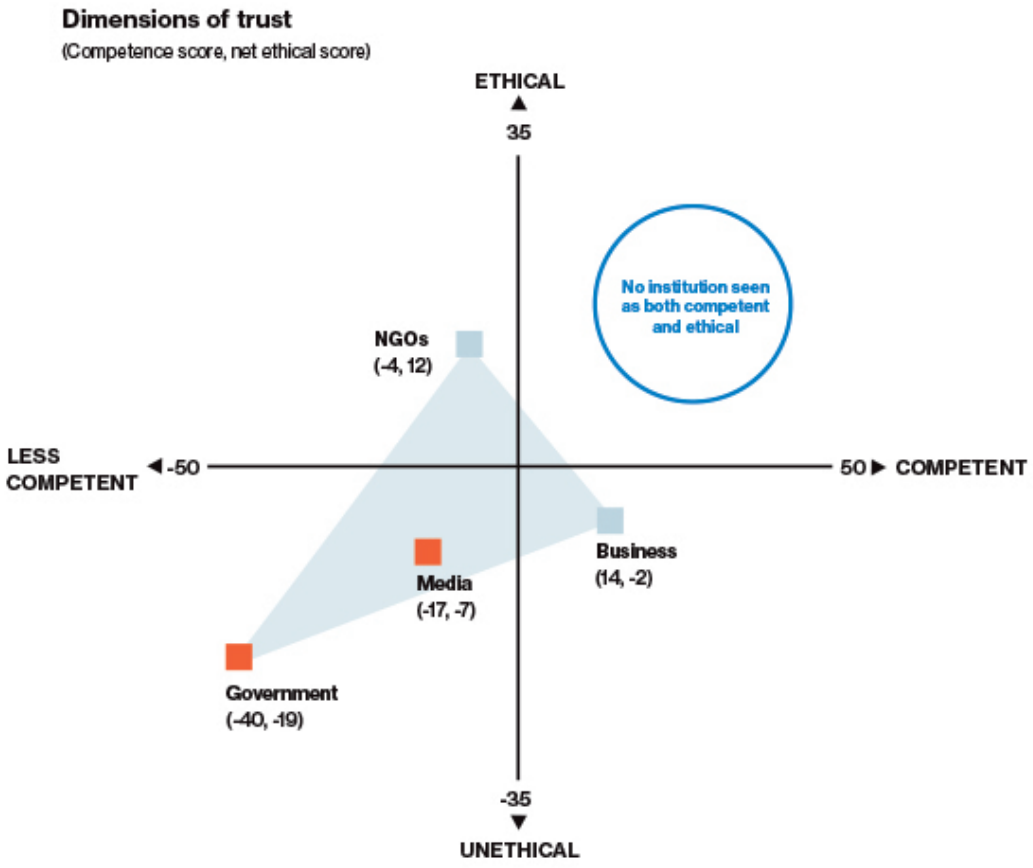


Figure 2.3: Edelman 2020 trust barometer [rights requested]

2.3 Web3

More recently Web3 is being touted as a way to connect content creators directly to content consumers, without centralised companies acting as gatekeepers of the data. It implies that all users have a cryptographic key management system, to which they attach metadata, that they make requirements of peers with whom they communicate, and that they maintain trust 'scores' with peers.

It seems likely that this new model is less driven by a market need, and more by the high availability of tools which allow this to happen (the ecosystems described later). Add to this a social response to the collapse in trust of companies such as Facebook and other social media platforms (Figure 2.3). There is perhaps a wish by consumers to pass more of the economic incentive to content creators, without the 'rent seeking' layer afforded by businesses, and a healthy dose of mania driven market speculation.

2.3.1 Emerging consensus

It's possible to frame Web3 as a hugely complex and inefficient digital rights management system (DRM). DRM is something that users of the internet are increasingly familiar and comfortable with. It's somewhat debatable whether decentralising this is worthwhile. The thesis of the developers of the technology seems to be that without it, control of 'value' will

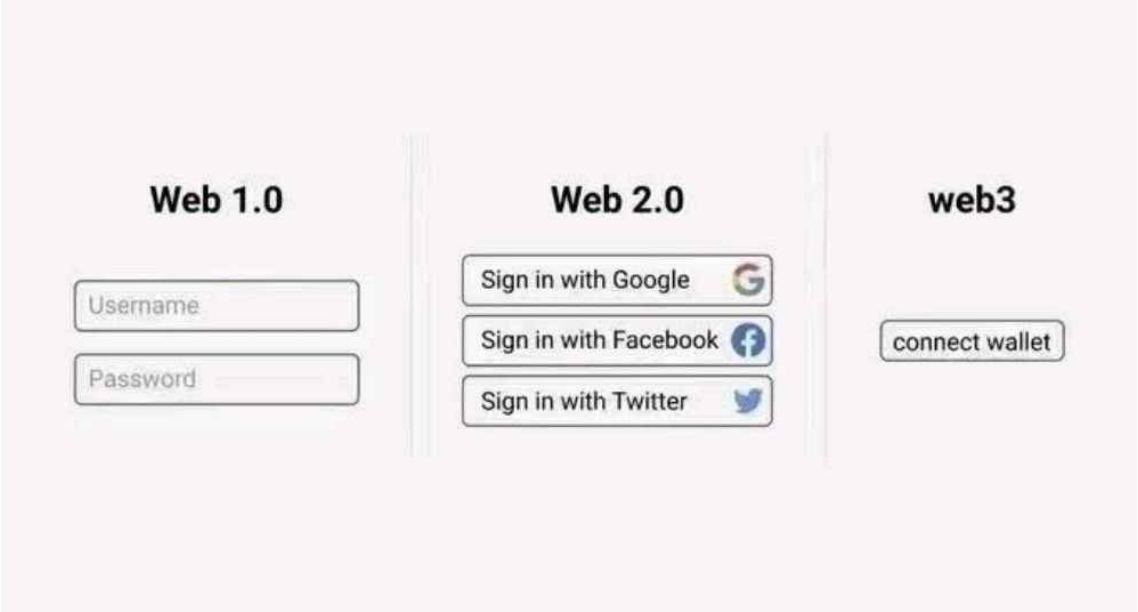


Figure 2.4: A meme showing differing approached to logging in on a website.

accrete over time, to one or more hegemonic controlling entities. It's a strong argument, but there is a substantial counter argument emerging that users just don't want this stuff. The nervousness of legislators in the USA to the attempt by Facebook/Meta to enter this peer-to-peer value transmission space is telling in terms of the perception of who is driving Web3.

At the end of 2021 and the beginning of 2022 there is much furore on the internet over what Web3 might be, and who it 'serves'. Enthusiasts feel that products such as Sign-In with Ethereum (EIP-4361) will give users choice over their data sovereignty, and a meme to this effect is seen in Figure 2.4. In practice though users are expecting to use badly written, buggy, economically vulnerable 'crypto' wallets to log into websites. The quality of this wallet software is improving of late with the so called "wallet wars" seeing commerce grade offerings from Coinbase and shares platform 'Robinhood'. These two companies alone have over 100 million users. It's likely that these wallets will evolve to offer the full spectrum of Web3 functionality. With that said it doesn't seem to make much sense yet on the face of it. There are in fact examples of the technology completely failing at censorship resistance. Popular 'Web3' browser extension Metamask and NFT platform Opensea have both recently banned countries in response to global sanction pressure. This failure to meaningfully decentralise will be explored further in the distributed identity section.

The current hype cycle is ignoring the legacy definitions described above and instead focusing almost exclusively on Ethereum based peer-to-peer projects (more on these later). It can be seen that the description is somewhat in the eye of the beholder.

This new hyped push for Web3 is being driven by enormous venture capital investment. A16Z are a major player in this new landscape and have released their ten principles for emergent Web3.

- Establish a clear vision to foster decentralized digital infrastructure
- Embrace multi-stakeholder approaches to governance and regulation
- Create targeted, risk-calibrated oversight regimes for different web3 activities

- Foster innovation with composability, open source code, and the power of open communities
- Broaden access to the economic benefits of the innovation economy
- Unlock the potential of DAOs
- Deploy web3 to further sustainability goals
- Embrace the role of well-regulated stablecoins in financial inclusion and innovation
- Collaborate with other nations to harmonize standards and regulatory frameworks
- Provide clear, fair tax rules for the reporting of digital assets, and leverage technical solutions for tax compliance

This list seems targeted toward the coming regulatory landscape, and could be considered at odds with the original tenants of an organically emergent, decentralised internet. Indeed principles such as 'furthering sustainability goals' seem downright incongruous. The community they claim to wish to support here are openly critical of these major institutional players and their motives, with even more pointed criticisms coming from outside of the Web3. This book and lab steer well clear of these companies and their applications.

Dante Disparte, chief strategy officer of 'Circle' venture capital, said in testimony to a US senate hearing; that Web 1 was 'read', Web 2 was 'read write', and that Web 3 will 'read write own'. The important takeaway here is not so much this oft quoted elevator pitch for Web3, but the fact that legislative bodies now consider this technology a force which they need to be aware of and potentially contend with.

Jeremy Allaire, again of Circle', talks about the recent legislative order in the USA as follows: *"this is a watershed moment for crypto, digital assets, and Web 3, akin to the 1996/1997 whole of government wakeup to the commercial internet. The U.S. seems to be taking on the reality that digital assets represent one of the most significant technologies and infrastructures for the 21st century; it's rewarding to see this from the WH after so many of us have been making the case for 9+ years."*

We will see in the following chapters that participation in this new Web3 is contingent on owning cryptocurrencies. It's estimated that about 6% of people in the UK own some cryptocurrency, with skews to both younger demographics, and smaller holdings. The legislative landscape in the UK is comparatively strict with strong "know your customer / anti money laundering" (KYC/AML) data collection mandated in law. Users of UK exchanges must provide a great deal of personal financial information, and undertake to prove that the wallets they are withdrawing to are their own. From the perspective of the UK SME it seems this seriously limits the potential audience for new products. Europe meanwhile has recently voted through even more restrictive regulation, applying the "transfer of funds regulation" to all transactions coming out of exchanges, enforcing a database of all addresses between companies, and reporting transactions above 1000 Euros to authorities. They have narrowly avoided enforcing KYC on all transfers to private wallets. The "Markets in Crypto Assets (MiCA) legislation is an onerous overhead that will likely make it impossible for smaller businesses in the sector to operate within the EU. This is still short of the ban that they have discussed in private. It seems that this EU position has prompted the UK government to seize the potential competitive advantage offered, and there will be more on this later.

It's a complex evolving narrative, and clearly contradictions are common. Right now there seems little appeal for stepping into Web3. Into the confusion, this book advances a narrow take, and toolset, which might extract some value from the technologies, while maintaining a low barrier to entry.

2.4 Example applications

It's handy here to get a feel for what this looks like. These aren't things that this book wishes to contribute to, or even have a firm opinion on, they're just representative of current activity in the decentralised web space.

2.4.1 Podcasting2.0

Podcasting 2.0 leverages RSS (the original dissemination system for podcasts) and the Bitcoin Lightning network, to enable so-called 'value for value' broadcasting. Subscribers use one of a variety of apps to stream micro-transactions of Bitcoin directly to the content creators as they listen to the podcast. No intermediate business takes a cut. Some variation on this model exists, such as John Carvalho's crowd funded podcast "The Biz" which progressively unlocks more minutes for everyone based on crowd funded donations.

2.4.2 Crowd funding

At time of writing a crowd funding initiative based around a digital decentralised construct called a DAO (explained later in detail) managed to raise $46 million dollars to bid for a copy of the US constitution at Southerbys auction house. The attempt narrowly failed, but the press heralded this new era of "Web3" economic might. This model might be the only use for DAOs and is likely just a way to avoid regulatory scrutiny. There is more detail on DAOs later.

2.4.3 Distributed exchanges

There are dozens of decentralised exchanges deployed on various blockchains. These platforms allow users to trade back and forth between various tokens (including 'normal money' stablecoins) and charge a fee for doing so. They operate within the logic of the smart contracts [4], within the distributed blockchains. This makes them extremely hard to ban, and as a result they operate in a legal grey area. At the extreme end of this is "distributed apps" (dApps) and "Decentralised Finance" (DeFi) which allows users access to complex financial instruments without legal or privacy constraints. DeFi will be touched on briefly later.

This is a huge area, and of only limited interest to the topics expanded in this book. It's perhaps worth noting BitcoinDEX, which runs in JavaScript in a web browser. It is effectively uncensorable, auditable by the user, and has no counter party risk since it operates entirely in the Bitcoin network. It is clearly an early prototype but manages this complex feature without the more expressive logic of more 'modern' public blockchains.

2.4.4 NFT marketplaces

NFT markets are far more centralised services which match 'owners' of digital assets with potential buyers. The concept is a staple of the more recent interpretation of Web3, even though in practice these seem to be centralised concerns. Opensea claims to be the largest decentralised NFT marketplace, but they have the ability to remove listings in response to legal challenges. This seems to fly in the face of Web3 principles. NFTs are currently a deeply flawed technology but seem likely to persist and will be covered later.

2.4.5 Non blockchain webs of trust

New products like Slashtags and Nostr (covered later) use a web of trust decentralised peer-to-peer (ish) model which assigns metadata and trust scores to 'any' data and connection, with a security model rooted in the Bitcoin cryptographic 'keys' but crucially not the bitcoin network. This makes it interoperable with bitcoin but not reliant upon it. In principle this allows users to build complex networks of inherited trust bi-directionally with their networks over time. Every connection to a peer can be a new schema, with individual metadata managed by the user. These are new and have low adoption at this time. The user controls the source of the data and can allow them to be used by centralised services. This flips the authentication and data management paradigm of Web2 around, putting the user in charge of their data. This is a familiar concept to the DID/SSI communities (described later) but with significant investment. As Slashtags and Nostr use keys as endpoints they act as a web of naming and routing, bypassing the existing web infrastructure of DNS. It is likely very complex to use in practice and will be revisited later. Slashtags is being paired with the Hypercore protocol for peer-to-peer data sharing, more specifically the 'hole punching' capability of the hypercore system which ensures connections through firewalls[5]. The first application by the affiliated Hyperdivision team is an open source peer-to-peer live video streaming app called Dazaar. Once again, it's not clear yet who wants or needs this bit-torrent style service.

2.4.6 Distributed DNS applications

There are many perceived problems with having centralised authorities for overseeing the database which translates between human readable internet names and the underlying machine-readable address notation. The databases which manage this globally are already somewhat distributed, and this distributed trust model is managed through a cryptographic chain of trust called DNSSEC which is capped by a somewhat bizarre key ceremony seen in Figure 2.5. The authority around naming is centralised in ICANN. There has been talk for many years about 'properly' distributing this database using decentralised/blockchain technologies[6]. The nature of this problem means that it either moves from control by ICANN, or it does not, and so far it has not, but there are many attempted, and somewhat mature attempts, at this difficult problem. Of these Namecoin is the most prominent, and is a fork of Bitcoin. The ubiquity of Bitcoin in such systems is perhaps becoming apparent.

2.4.7 Impervious browser

It might be that the future of Web3 comes in the guise of integrated suites such as the proposed Impervious web browser. They say that "without centralized intermediaries" it features:

- Zoom, without Zoom.
- Google Docs, without Google.
- Medium, without Medium.
- WhatsApp, without WhatsApp.
- Payments, without banks.
- Identity, without the state.

This is obviously leading marketing hype, and they're already late for their release deadline, but what they're talking about here is an integration of the components mentioned in this book. If they can get critical mass around this browser then perhaps the Web3 market can



Figure 2.5: DNSSEC ceremony in a faraday cage

be kickstarted. CEO Chase Perkins has recently presented on this.

2.4.8 TBD - Web5

Promisingly Jack Dorsey's company TBD is working on a project called "Web5". Details are scant but the promise is decentralised and/or self hosted data and identity running on Bitcoin, without recourse to a new token. *"Components include decentralized identifiers (DIDs), decentralized web node (DWNs), self-sovereign identity service (SSIS) and a self-sovereign identity software development kit (ssi-sdk)"*.

Web5 leverages the ION identity stack which is expanded later in the book. All this looks to be exactly what our metaverse system requires, but the complexity is likely to be quite high as it is to be built on existing DID/SSI research which is pretty complex and perhaps has problems.

2.5 The common thread

One feature which persists throughout all of these interpretations of Web3 is the need for decentralised trust. According to Nathaniel Whittemore, a journalist for Coindesk, "The Web3 moniker positions this industry in opposition to big tech". Alternatively the many detractors of the technology think it simply provides avenues for incumbents to experiment with new models of control and monetisation, increasing systemic risk at no cost to themselves.

Overall then, perhaps the space is hype, and is certainly rife with scams. The degree to which it even accomplishes decentralised trust is highly debatable, and meanwhile the limited numbers of Web3 and supporting crypto companies display lamentable cyber security practice themselves, creating honeypots of personal data from users of the ecosystem.

With that said the component parts necessary to deliver on the promise **do** exist. If

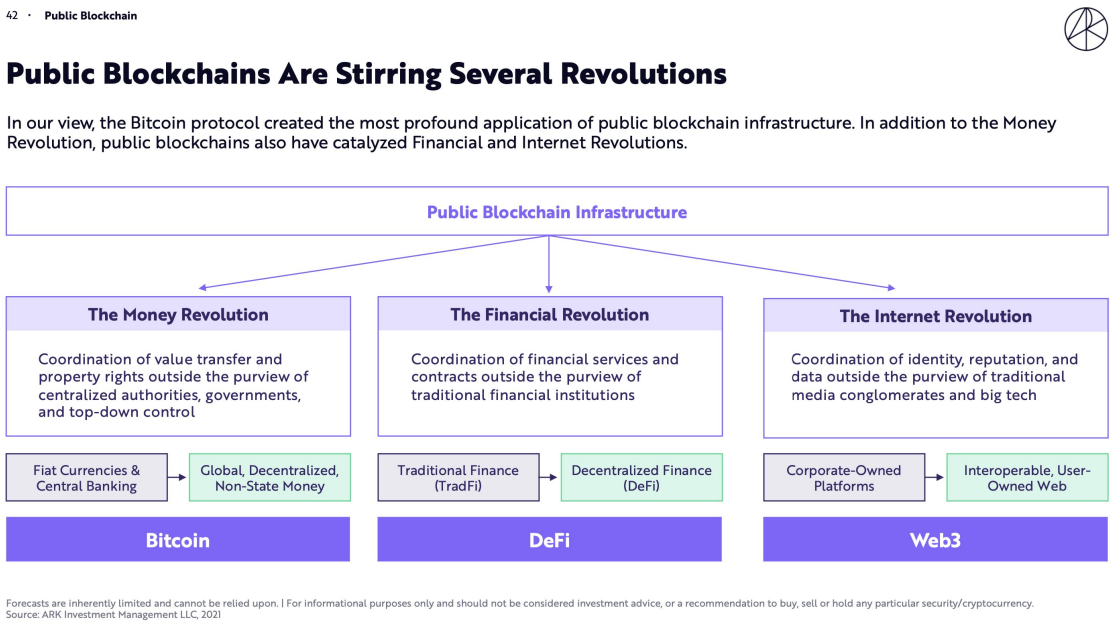


Figure 2.6: ARK slide on Web3. Rights requested

there is to be no central controlling party(s) as in the Web 2 model then nothing can happen without a cryptographically secure underpinning, allowing digital data to be passed around without a prior arrangement.

The following chapter will describe how much has been done by computer scientists over the past decades to support that. From this base layer we also get the potential for secure and trust minimised identity management. This nascent field of distributed identity management is explained later. From distributed trust models we can see 'trustless' transmission of economic value. The ability to send value from one person to another person or service without a third party.

This whole area is 'crypto', which is increasingly seeping into the human consciousness, and saw an astonishing $30B of capital investment in 2021 alone. At time of writing the industry is an over 2 trillion dollar market.

Of their 2022 'Big Ideas' report, ARK investment LLC (who manage a $50B tech investment) said the following (Figure 2.6), which connects some of the dots already mentioned, and leads us into the next section which is Blockchain and Bitcoin:

"While many (with heavily vested interests) want to define all things blockchain as web3 we believe that web3 is best understood as just 1 of 3 revolutions that the innovation of bitcoin has catalyzed.

- *The Money Revolution*
- *The Financial Revolution*
- *The Internet Revolution"*

All the new crypto technologies circling the Web3 narrative are bound tightly together, but there is currently very little meaningful value to be seen.

The rest of this book will focus on the trust and value transfer elements of this shift in internet technologies, and attempt to build a case for it's use in decentralised, open source, metaverse applications.



3. DLT, Blockchain, and Bitcoin

Distributed ledger technology (DLT) is a data structure distributed across multiple managing stakeholders. A subset of DLT is blockchain, which is a less efficient, immutable data structure with a slightly different trust model. Rauchs et al. of the Cambridge Centre for Alternative Finance provide a detailed taxonomy and conceptual framework [7]. It can be seen in their paper that the definitions are somewhat unclear in literature.

DLT, and especially blockchain, are rapidly gaining ground in the public imagination, within financial technology companies (FinTech), and in the broader corporate world.

The technology and the global legislative response are somewhat immature, and misapplications of both technologies are commonplace.

Distributed trust models emerged from cryptography research in the 1970s when Merkle, Diffie, and Hellman at Stanford worked out how to send messages online without a trusted third party [8, 9].

Soon after the 1980s saw the emergence of the cypherpunk activist movement, as a reaction to the emerging surveillance state [10, 11]. These early computer scientists in the USA saw the intersectionality between information, computation, economics, and personal freedom [12]. Online discussion in the early nineties foresaw the emergence of trans-national digital markets, what would become the WWW [13, 14]. The issues of privacy and the exchange of digital value (digital / ecash) were of foremost importance within these discussions and while privacy was within reach thanks to "public/private key pairs", ecash proved to be a more difficult problem.

Adam Back's 1997 'hashcash' [15] paved the way for later work by implementing the concept of what would become 'proof of work' [16, 17]. This was built upon by Dai [18], Szabo [4], Finney [19], and Nakamoto amongst others. In all it took 16 years of collaboration on the mailing lists (and dozens of failed attempts) to attack the problem of trust-minimised, distributed, digital cash. The culmination of these attempts was Bitcoin [20]. This is illustrated by Dan Held in Figure 3.1. This is now a wider ecosystem of technologies and societal challenges 3.2.

There is enormous complexity and scope, as seen in Figure 3.3, and yet genuinely useful products are elusive. It is surprisingly hard to pin down a simple explanation for the features which define a blockchain. These "key takeaway" from Investopedia are a neat summary however.

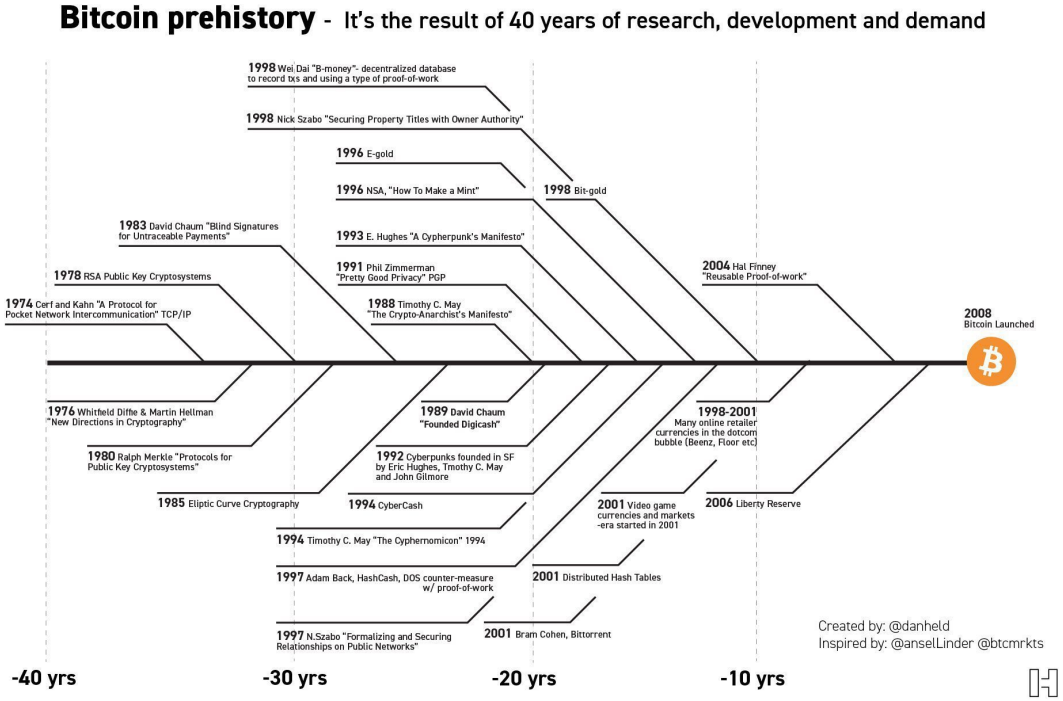


Figure 3.1: Dan Held: Bitcoin prehistory used with permission.



Figure 3.2: Bitcoin Topics used with permission @djvalerieblove.

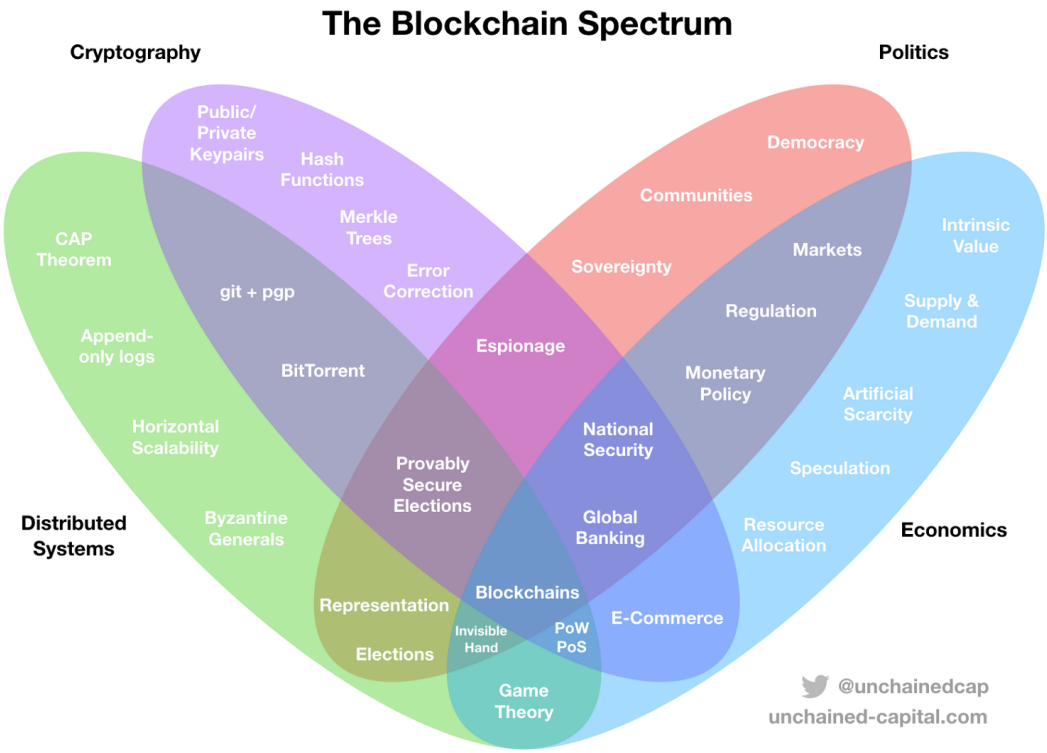


Figure 3.3: Intersecting disciplines. Reused with permission Dhruv Bansal

- *Blockchain is a specific type of database.*
- *It differs from a typical database in the way it stores information; blockchains store data in blocks that are then chained together.*
- *As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order.*
- *Different types of information can be stored on a blockchain but the most common use so far has been as a ledger for transactions.*
- *In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.*
- *Decentralized blockchains are "append only". In effect this means that the data entered becomes irreversible over time. For Bitcoin, this means that simple economic transactions are permanently recorded and viewable to anyone.*

In principle blockchains provide a **differentiated trust model**. With a properly distributed system a blockchain can be considered "trust-minimised", though certainly not risk minimised. This is important for some, but not all people. There is not much emboldening of text within this book. If you start to question the whole reason for this 'global technology revolution' then it always comes back to those three words.

It can in fact be argued that the whole concept of distributed cryptographic blockchains is somewhat strained, as the vast majority of the technology offerings are not distributed, and worse, meaningful distribution may indeed be practically impossible without a trusted

third party [21]. "There are many scenarios where traditional databases should be used instead"[22].

3.1 What's this for sorry?

The proponents of blockchains argue, that in an era when data breaches and corporate financial insolvency intersect with a collapse in trust of institutions, it is perhaps useful to have an alternative model for storage of data, and value. That seems like a lot of effort for a questionable gain. It's far more likely it's simply speculation.

While writing this book the questions of 'what is this *really for* and how can it possibly be worth it', came up again and again. In truth it's a very difficult question, without a clear enough answer. It's beyond the scope of this book to figure this out properly, but references to advantages and disadvantages will be made throughout.

It seems that the engineers who created Bitcoin wanted very much to solve a technical problem they saw with money (from their understanding of it), and the transmission of money digitally. As the scale and scope have increased so has the narrative evolved as seen in Figure 3.4, but it's never really kept pace with the level of the questions posed.

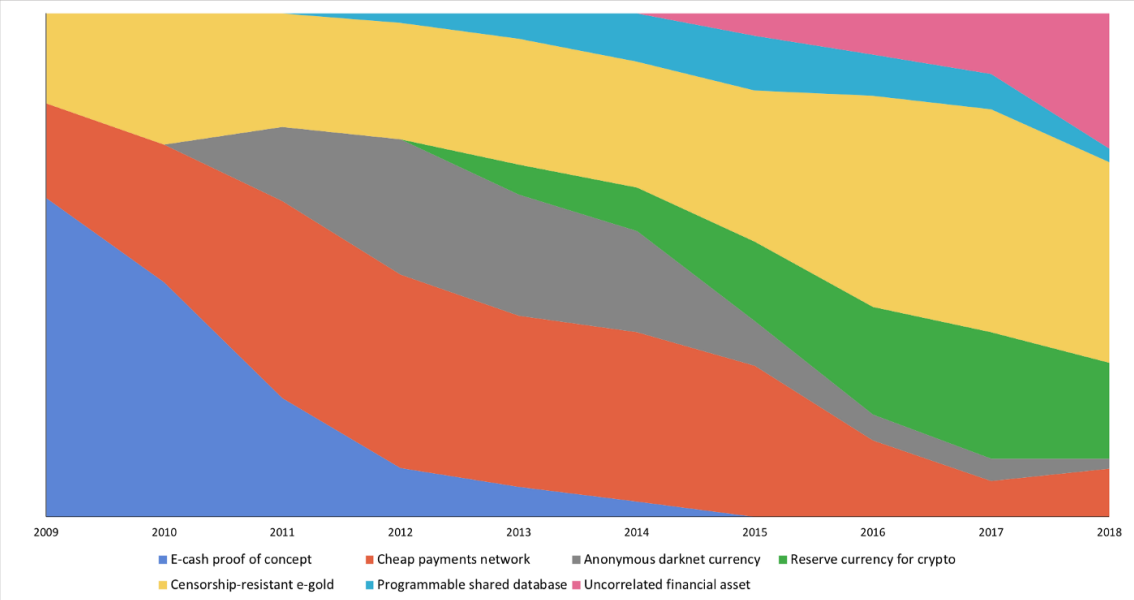


Figure 3.4: The narrative use of Bitcoin has evolved, by Nic Carter and Hasufly.

A cost benefit analysis that excludes speculative gains seems to fail for pretty much all of blockchain/DLT. Bitcoin is more subtle as it possibly *can* circumvent the legacy financial systems. This still leaves huge questions. To quote others in the space, is Bitcoin now the iceberg or the life raft?

For the most cogent defence of the technology as it stands in this moment, Gladstein (and others) offer a vision for the asset class, in the 87% of the world he says don't have access to the benefits enjoyed by the developed west [23]. He points to Block and Wakefield Research's report which finds those living under financially oppressive regimes are the most optimistic about the technology as in Figure 3.5. This argument is suggestive of huge and untapped markets for services which may be accessible to developed nations through telepresence/metaverse interfaces.

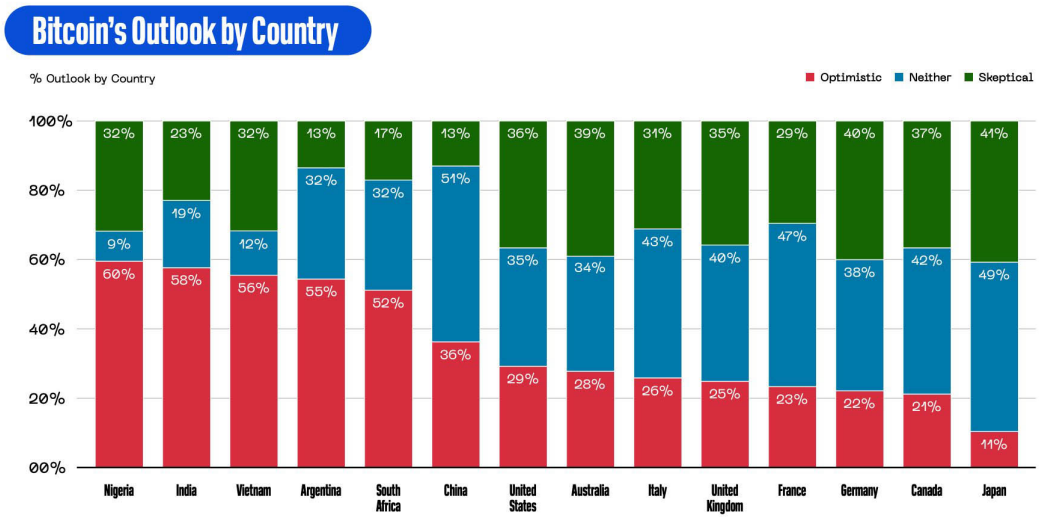


Figure 3.5: "This new chart from Block is financial privilege visualized."

Country	% of pop own crypto	Country	% of pop own crypto
Ukraine	12.7	South Africa	7.1
Russia	11.9	Nigeria	6.3
Venezuela	10.3	Colombia	6.1
Singapore	9.4	Vietnam	6.1
Kenya	8.5	Thailand	5.2
USA	8.3	United Kingdom	5.0
India	7.3	Brazil	4.9

Gladstein's is a carefully developed and well researched book, but is written from the perspective of (just) Bitcoin 'being the raft'. Later in this book we will consider if it might be the iceberg, but this is not the domain expertise we offer in this book.

To further contextualise this Mike Novogratz claims the adoption figures at the top of the page. Raoul Pal of RealVision says: *Crypto adoption is now massively outperforming the internet. It's been growing at about 165% a year versus 85% for the internet for the same period of time now.*

Thanks to a natural fit with strong encryption, and innate resistance to censorship by external parties, these systems do lend themselves well to 'borderless' applications, and are somewhat resistant to global regulation (for good or ill). Given the rates of adoption seen above it seems that this stuff is coming regardless of their somewhat marginal usefulness. This provides us an excellent use case to explore for metaverse applications, and this will be the focus.

3.2 A panoply of tech

Within DLT/blockchain there seem to be as many opinions on the value of the technology as there are implementations. A host of well engineered open source code repositories makes the cost of adoption relatively low.

There are thousands of different 'chains' and many more tokens which represent value on them. A majority of these are code forks of earlier projects. Most are defunct yet still have some residual 'value' locked up in them as a function of their 'distributed' tokens.

Because the space is comparatively new, subject to scant regulation, and often open source, it is possible to clone a github, change a few lines of code, and front it with a website in order to create 'scams', and this happens frequently [24].

The following sections give an overview of the major strands of the technology. First is Ethereum, mainly to discount it's use for our needs, and move on to more appealing options.

3.3 Ethereum

Ethereum [25] is the second most secure public blockchain (by about 50%)[26], and second most valuable by market capitalisation (though this comparison is somewhat stretched). It is the natural connection from Web3 to the rest of the book, so it will be considered first.

It is touted as 'programmable money'. It, unlike bitcoin, is (nearly) Turing complete [27], able to run a virtual machine within the distributed network (albeit slowly), and can therefore process complex transactional contracts in the settlement of value. This has given rise to the new field of 'distributed finance', or DeFi (described later), alongside many interesting trust-minimised immutable ledger public database ideas.

There are trade-offs and problems with Ethereum (Eth/Ether) which currently increase the 'participation floor' and make the network far less suitable for entry level business-to-business use. The ledger itself being a computational engine, with write only properties, is enormous. Specialist cloud hardware is required to run a full node (copy of the ledger), and partial nodes are the norm. Many partial nodes are run by one specialist cloud provider (Infura), which has recently been forced to exclude Venezuela from the network. Similarly large mining pools are refusing to process addresses on an OFAC sanction list. A staggering 50% runs on Amazon AWS servers. Critics of the project point to these vulnerabilities to outside influence as an existential threat to the aims of the technology. If it can be censured, then what advantage is there over the founders simply running a high speed database to the same purpose?

This is a function of the so called 'scalability trilema' [28], in which it seems that only two features from the list of decentralization, scalability or security can be chosen for blockchains [29].

Moreover the network is centrally controlled by its creator and the 'miners'. There is a strong case to answer that Eth is neither distributed, nor trustless, and in fact therefore fails to be differentiated from a DLT, undermining some of it's claims. The history of Ethereum is a fascinating case study in human greed. By the time the whitepaper had it's first limited release, Bitcoin (covered next) had already passed $1000 per token. This led to the creators ambitions for a 'fair release' of tokens being voted down by powerful funders, leading to the explosion of similarly structured 'pre-mined' coins in the ICO craze, which followed on the Ethereum network. Laura Shin is possibly the most experienced journalist and author in the space and has covered this crazy era in her book 'The Cryptopians' [30]. It's a tough read for the newcomer though, perhaps finish this primer first!

With that said there are many talented developers doing interesting work on the platform, and innovation is fast paced. It is entirely normal for technology projects to launch their distributed ledger idea on and within the Ethereum network. These generate



Figure 3.6: Ethereum is thought to look like a speculative bubble. Rights requested

tradable 'ERC-20' tokens, which can accrue value or demonstrate smart contract utility (based on the Solidity programming language). Because the value locked and generated in the Ethereum platform comes not just from the ETH token, but all the ERC technologies built upon it, there are hundreds of billions of pounds 'within' the network. All of these projects, and indeed the core technology of Ethereum are subject to exploits and vulnerabilities and tens of billions of pounds have been lost [31]. Most of this money is pure market speculation (as is the case across blockchains). Many analysts cannot see this as anything but a speculative bubble, with all the predictable crash yet to come. This can be seen in the context of other bubbles in Figure 3.6. It seems that most of the projects in crypto more generally, but certainly with ETH and the NFTs within it are a new kind of social gambling, where online communities can reinforce groupthink around their speculative choices. With all this said most of the couple of million people who use NFTs use Ethereum, and if this market of creators and consumers is to be brought into a mixed reality space then they will need a way to bring their objects with them.

Such is the level of nefarious activity on these networks (within Ethereum) that they have a poor reputation, and are difficult to audit, launch, and maintain. The overriding problem of using a blockchain for utility applications (rather than just as money) is that people can, and will, simply lie for criminal purpose when entering data into the ledger. It is far more likely that Ethereum is simply a speculative bubble than any of the claims for utility being born out. Add to that Morgan Stanleys recent assertion that Ethereum is itself threatened by newer contender chains and it's future becomes unclear. The report correctly identifies that "High transaction fees create scalability problems and threaten user demand. High costs make Ethereum too expensive for small-value transactions.". It is this high cost of use that most excludes the ERC-20 networks from our consideration.

3.3.1 Mining and Gas

Ethereum has a significant barrier to entry because of high fees to use the network. The system is Turing complete; able to programatically replicate any other computational system. This includes endless loops in code, so it is trivial to lock up the computational bandwidth of the whole system, in a smart contract commitment, through a web wallet.

To mitigate this existential 'denial of service attack' the 'gas' system demands that users spend some of their locked up value to operate on the network. In this way a transaction loop would quickly erode the available gas and stop looping. As the popularity of the system has grown, so too have the gas fees. It can sometimes cost over £10,000 to do a single transaction, though it is typically a few tens of pounds. Appallingly if the user pitches their mining fee offer too low, then the money gets spent anyway! A website just plucks random Ethereum addresses out of the aether to show you the level of this expense for participants. People can even buy NFTs of the worst examples of these, as 'tokens', wasting more money. This is a huge problem for potential uses of the network.

It is currently a proof of work system like Bitcoin (this is described in the next section), and has a commensurate energy footprint to secure the network. It also ties up global supply of PC graphics cards used for it's mining model, making them far more expensive. This has generated ill will in the global gamer community for instance, and damped the ambitions of NFT developers because of their inability to sway this crucial customer demographic. Much more on this later.

3.3.2 Upgrade roadmap

Part of the challenge Ethereum faces is wrapped up with it's complex token emission schedule. This is the rate at which tokens are generated and 'burnt' or destroyed in the network. The total supply of tokens is uncertain, and both emission and burn schedules are regularly tinkered with by the project. The changes to the rate at which ETH are generated can be seen in Figure 3.7. In addition, a recent upgrade (EIP-1559) results in tokens now being burnt at a higher rate than they are produced, deliberately leading to a diminishing supply. In theory this increases the value of each ETH on the network at around 3% per year. It's very complex, with impacts on transaction fees, waiting time, and consensus security, as examined by Liu at al. [32]. Additionally, there is now talk (by Butlerin, the creator of Ethereum) of extending this burn mechanism further into the network.

Ethereum was designed from the beginning to move to a 'proof of stake' model where token holders underpin network consensus through complex automated voting systems based upon their token holding. This is now called Ethereum Consensus Layer. The

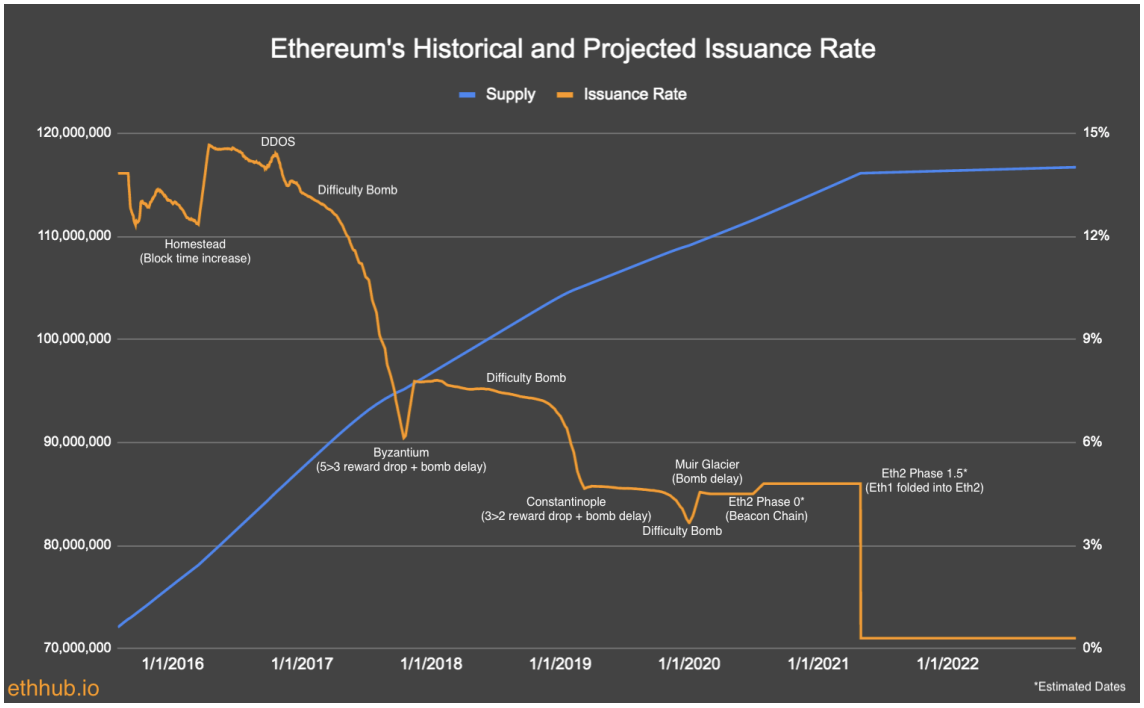


Figure 3.7: The rate of token generation has changed unpredictably over time. Rights requested

purpose of the upgrade is to reduce the carbon footprint of the network, a laudable goal. It will not lower the cost to users nor improve performance. "The Merge" event which enables this is now slated for September 2022. If this is successful then four major entities will control the rules of the chain, and have already agreed to censor certain banned addressees.

Proof of stake has problems in that the majority owners 'decide' the truth of the chain to a degree, and must by design have the ability to over-ride prior consensus choices. Proof of stake is probably inherently broken [33]. This has for malicious actors who have sufficient control of the existing history of the chain, thought to be in the region of $50M [34]. Like much of the rest of 'crypto' the proposed changes will concentrate decisions and economic rewards in the hands of major players, early investors, and incumbents. This is a far cry from the stated aims of the technology. The move to proof of stake has recently earned it the MIT breakthrough technology award, despite not being complete. It's clearly a technology which is designed to innovate at the expense of predictability. This might work out very well for the platform, but right now the barrier to participation (in gas fees) is so high that we do not intend for Ethereum to be in scope as a method for value transfer within metaverses.

3.3.2.1 Consequences of hard forks

Ethereums strategy has been that of uncontentious "canonical hard forks". These regular changes to the distributed codebase are well managed so as to not result in bifurcations of the network such as the Ethereum Classic fork. In a contentious hard fork two different versions of the chain move forward with different incentives and design choices. This could conceivable happen in the switch to POS, and indeed there are some signs that Ethereum miners are already gearing up to move back to supporting "classic" which will be a huge boon to the legacy fork. If there is another contentious split at "The Merge" point, with a

cabal of miners supporting the current system and trying to remove the difficulty bomb which is supposed to clean this problem up, then there will suddenly exist 2 copies of every NFT and asset on the chain. This is unlikely as it would require some buy in from nodes and users, but an under discussed risk to the system. Were it to happen many people would choose the wrong chain and sell the asset on the wrong side of the bet.

3.4 Bitcoin

The first blockchain was the Bitcoin network [20], some two decades after Haber et al. first described the idea [35]. Prior to Bitcoin these structures were called 'timechains' [36]. It can be considered a triple entry book keeping system [37, 38], the first of it's kind, integrating a 'provable' timestamp with a transaction ledger, solving the "double spend problem" [39, 40, 41]. Some see this as the first major innovation in ledger technology since double entry was codified in Venice in fourteen seventy five[42].

It was created pseudonomously by an individual or group calling themselves 'Satoshi Nakamoto' in 2009, as a direct response to the perceived mishandling of the 2008 global financial crisis [36], with the stated aim of challenging the status quo, with an uncensorable technology, to create a money which could not be debased by inflation policy, and outside of the politically captured fintech incumbents. It's interesting to note that the narrative around the use case for Bitcoin has shifted over it's lifetime.

The "genesis block" which was hard coded at the beginning of the 'chain' contains text from The Times newpaper detailing the second bank bailout.

There will only ever be (just short of) 21 million bitcoins issued, of which around 19 million have already been minted, and around 4 million lost forever. This 'hard money' absolute scarcity is a strong component of the Bitcoin meme landscape. These are basically arbitrary figures though; a combination of the issuance schedule, and an 'educated guess' by Nakamoto: [36]

"My choice for the number of coins and distribution schedule was an educated guess. It was a difficult choice, because once the network is going it's locked in and we're stuck with it. I wanted to pick something that would make prices similar to existing currencies, but without knowing the future, that's very hard. I ended up picking something in the middle. If Bitcoin remains a small niche, it'll be worth less per unit than existing currencies. If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit."

In theory there is no barrier to access, and equality of opportunity to accumulate and save over long periods. This is not true of chains and tokens since, which lock up some of their value for seed investors to cash out later. None of the blockchains since are decentralised in the same way [43]. Bitcoin was probably a singular event.

Each Bitcoin can be divided into 100 million satoshis (sats), so anyone buying into Bitcoin can buy a thousandth of a pound, assuming they can find someone willing to transact that with them.

Satoshi Nakamoto (the name of the publishing entity) disappeared from the forums forever in 2010. Bitcoin has the marks of cypherpunks and anarcho capitalism. The IMF has recently conceded that the Bitcoin poses a risk to the traditional financial systems, so it could be argued that it is succeeding in this original aim.

Although there were some earlier experiments (hashcash, b-money etc), Bitcoin is the first viably decentralised 'cryptocurrency'; the network is used to store economic

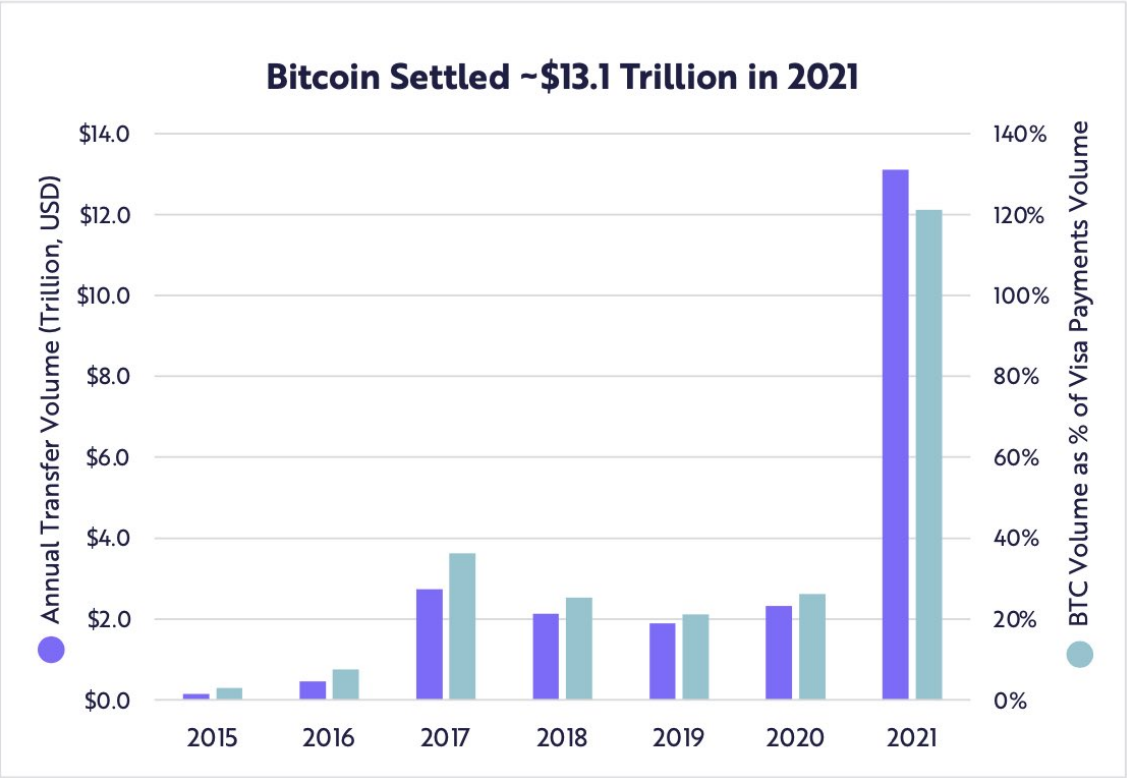


Figure 3.8: Growth in settlement value on the Bitcoin network (Forbes).

value because it is judged to be secure and trusted. It is a singular event in that it became established at scale, such that it could be seen to be a fully distributed system, without a controlling entity. This is the differentiated trust model previously mentioned. This relative security is the specific unique selling point of the network. It is many times more secure than all the networks which came after based on a like for like comparison of transaction 'confirmations'. This network effect of Bitcoin is a compounding feature, attracting value through the security of the system. It is deliberately more conservative and feature poor, preferring instead to add to it's feature set slowly, preserving the integrity of the value invested in it over the last decade. At time of writing it is a top quartile largest global currency and has settled over $13 trillion Dollars in 2021, though Makarov et al. contest this, citing network overheads, and speculation [44]. Institution grade 'exchange tradable funds' which allow investment in Bitcoin are available throughout the world, and the native asset can be bought by the public easily through apps in all but a handful of countries as seen in Figure 3.8.

Only around 7 transactions per second can be settled on Bitcoin. The native protocol does not scale well, and this is an inherent trade-off as described by Croman et al. in their positioning paper on public blockchains [45]. Over time, competition for the limited transaction bandwidth drives up the price to use the network. This effectively prices out small transactions, even locking up some value below what is a termed the 'dust limit' of unspent transactions too small to ever move again [46].

Bitcoin has developed quickly, with a faster adoption than even the internet itself. It is already a mature ecosystem, and is seeing adoption as a corporate treasury asset.

Adoption by civil authorities is increasing, and legislators the world over are being

forced to adopt a position. California has an explicitly Web 3 and blockchain executive order to invetigate and support opportunities. Many city treasuries have added it to their balance sheet. Honduras has launched "Bitcoin Valley" as a tourist initiative, and the Swiss city of Lugano is launching a huge initiative alongside Tether. It is already legal tender in the country of El Salvador[47] and the Central African Republic, and will be soon in Madeira and Roatán island. This means it *must* be accepted as a means of payment. CAR are also launching their own Bitcoin sidechain (like Liquid described later) as a pan African initiative. In places such as Panama it simply has legal status and *can* be accepted without double taxation.

Global asset manager "Fidelity" wrote the following in their 2021 trends report. *"We also think there is very high stakes game theory at play here, whereby if Bitcoin adoption increases, the countries that secure some bitcoin today will be better off competitively than their peers. Therefore, even if other countries do not believe in the investment thesis or adoption of bitcoin, they will be forced to acquire some as a form of insurance. In other words, a small cost can be paid today as a hedge compared to a potentially much larger cost years in the future. We therefore wouldn't be surprised to see other sovereign nation states acquire bitcoin in 2022 and perhaps even see a central bank make an acquisition."*

3.4.1 The Bitcoin Network Software

There isn't a single GitHub which can be considered the final arbiter of the development direction, because it is a distributed community effort with some 500 developers out of a wider 'crypto' pool of around 9000 contributors (the vast majority are spread across disparate Ethereum and some Solana projects). Development and innovation continues but there is an emphasis on careful iteration to avoid damage to the network. Visualisation of code commitments to the various open source software repositories can be seen at Bitpaint youtube channel and in Figure 3.9.

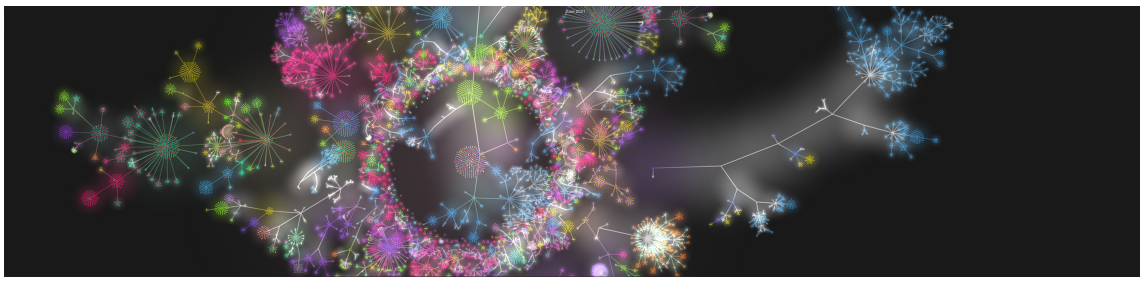


Figure 3.9: Bitpaint: Contributions to the Bitcoin ecosystem. Reused with permission.

Bitcoin core is the main historical effort (with around a dozen major contributors guiding the direction), but there are alternatives (LibBitcoin in C++, BTCD in Go, and BitcoinJ in Java), and as innovation on layer one slows, attention is shifting to codebases which interact with the base layer asset. Much more on these later.

3.4.2 Mining and Energy concerns

3.4.2.1 Mining process overview

Bitcoin mining is the process of adding public transactions into the ledger, in return for two economic rewards, paid in Bitcoin. These are the mining fee, and the block reward. The transactions which are added into the next 'block' of the chain are selected preferentially

based on the fee they offer, which is up to the user trying to get their transaction into the chain. This can be within the next 10 minutes (next block), or a gamble out toward 'never' depending how competitive the network is at any time. Miners try to find a sufficiently low result from a cryptographic hash function [48](a random process), and upon finding it, they can take their pre-prepared 'block' of transactions sourced from their local queue (mempool), and add it into the chain, for confirmation by other miners. In return they take all the fees within that mined block, and whatever the block reward is at the time. When the network started the block reward was 50 Bitcoin, but has halved repeatedly every 210,000 blocks (four years) and now stands at 6.25 BTC. The rate of mining is kept roughly at one block every 10 minutes, by a difficulty adjustment every 2016 blocks (2 weeks). This in a complex interdependent mechanism and is explained very well in this article. These components are explained in slightly more detail later.

3.4.2.2 Energy & policy response

Bitcoin uses a staggering amount of energy to secure the blockchain (Figure 3.10), and this has climate repercussions. A simple back of the envelope use of the IEA total energy supply, and the Cambridge Bitcoin energy use estimate puts the network at around 0.1% of global energy use.

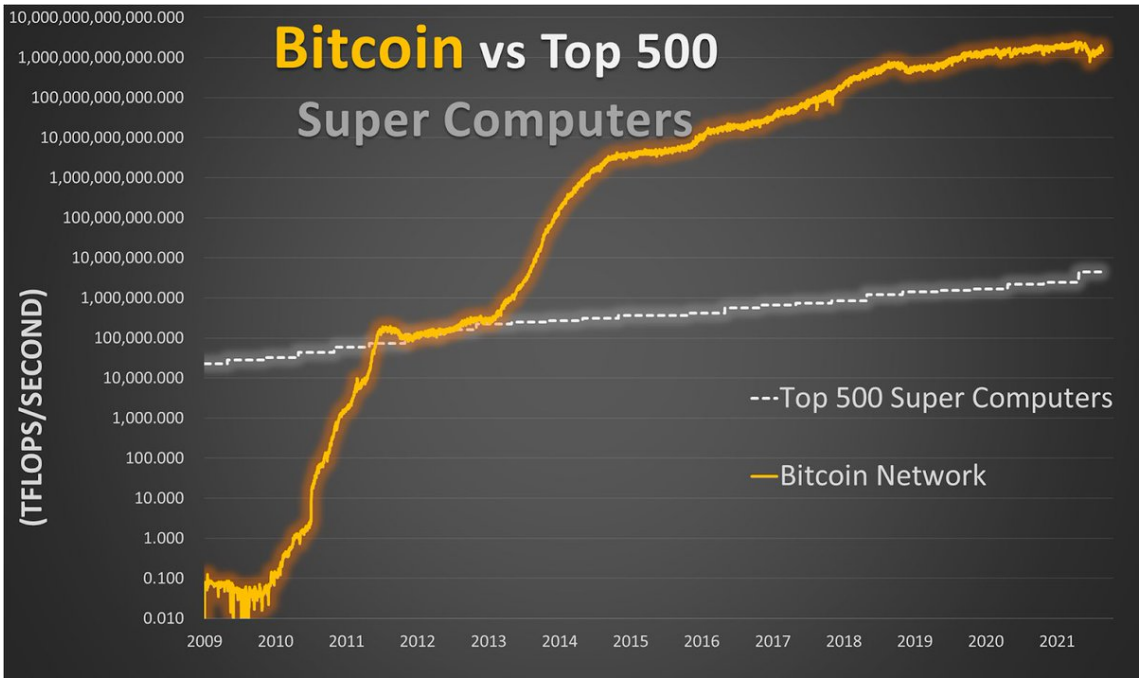


Figure 3.10: Bitcoin network vs TOP500 supercomputers

It is an industrial scale global business with 'mining companies' investing hundreds of millions of pounds at a time in specialist ASIC mining hardware and facilities. The latest purpose designed Intel chip touts both Web3 and metaverse applications. This is "proof of work", and is essential to the technology, and is still thought by some to be the best available option. The Cambridge Bitcoin Energy Consumption Index monitors this energy usage. Their 2022 report sees American mining leading globally.

Such businesses can mine a Bitcoin for around $5k-$10k per coin, so the profit margins are considerable (based on 30-40 Joule/terahash and power rate less than 5 cents/kilowatt


ERCHANDISE
ISED IN THE
IS GUARANTEED

New York

First to Last—the T

XXI No. 27,412 (Copyright, 1921, New York Tribune Inc.) SUNDAY, DECEMBE

Artist
Women
Attacked

n of John R.
ur Identified
e Line-Up by
rl and Matron

Ford Would Replace Gold With Energy Currency and Stop Wars

Declares if Government Will Give Him Muscle Shoals Plant He Can Demonstrate Success of Plan to Substitute Natural Wealth as Basis of World's Money

FLORENCE, Ala., Dec. 3.—Henry Ford and Thomas A. Edison arrived here to-day to inspect the Muscle Shoals nitrate plant, which the Detroit bankers who to-day control the bulk of the world's gold supply. No matter to what country they as individuals claim allegiance, they all play the same game to keep the gold they have in their own

Craig U
$10,00
Educati

Slash Into Sch
Suggested to
to Obtain Re
$350,516,52

Figure 3.11: Intimate tie between energy and money, Henry Ford

hour and excluding hardware costs). This is not to say that all mining is, or should be, so concentrated. Anyone running the hashing algorithm can get lucky and claim the block reward. PoW ties the value of the 'money' component of Bitcoin directly to energy production. This is not a new idea. Henry Ford proposed an intimate tie between energy and money to create a separation of powers from government, as can be seen in Figure 3.11. The potential ecological footprint of the network has always been a concern; Hal Finney himself was thinking about this issue with a mature Bitcoin network as early as 2009, and a debate on the Bitcoin mailing lists called the mining process "thermodynamically perverse". The most cited negative analysis on the matter by Mora et al sees Bitcoin mining alone warming the planet above 2 degrees [49].

Proponents of the technology say that the balance shifted dramatically in 2021 with China outright banning the technology; this has forced the bulk of the energy use toward the USA, and away from 'dirty coal' as seen in Figure 3.12. Some adherents have proposed mitigations [50]. As a worked example of Cross and Bailey's proposal a retail investor owning 1 BTC would have to buy around 700 shares of 'CleanSpark' mining company (CLSK) to make their holding completely neutral. Some more strident voices suggest that 'ending financialisation' through use of Bitcoin may be net positive for the environment at a macro level [51]. Indeed it may provide a route to support electrifying everything through deployment of flexible demand load. This enables a kind of 'financial battery' that can soak up excess capacity from overbuilt renewables (something which needs to be done). Local subsidy initiatives may begin to drive this kind of adoption as may be happening in Texas[52, 53]. Brad Jones, interim CEO of the Texas grid said:

"As we get more renewable generation, in particular wind [which] is operating at night ... we have to find a home for it, otherwise we have to turn the wind down. It's such a great resource we shouldn't turn it down. Bitcoin mining or what some call crypto has found a way to come into our markets and take some of that wind in off-peak periods. Then when we get to peak period times they are very quick to remove themselves from the market

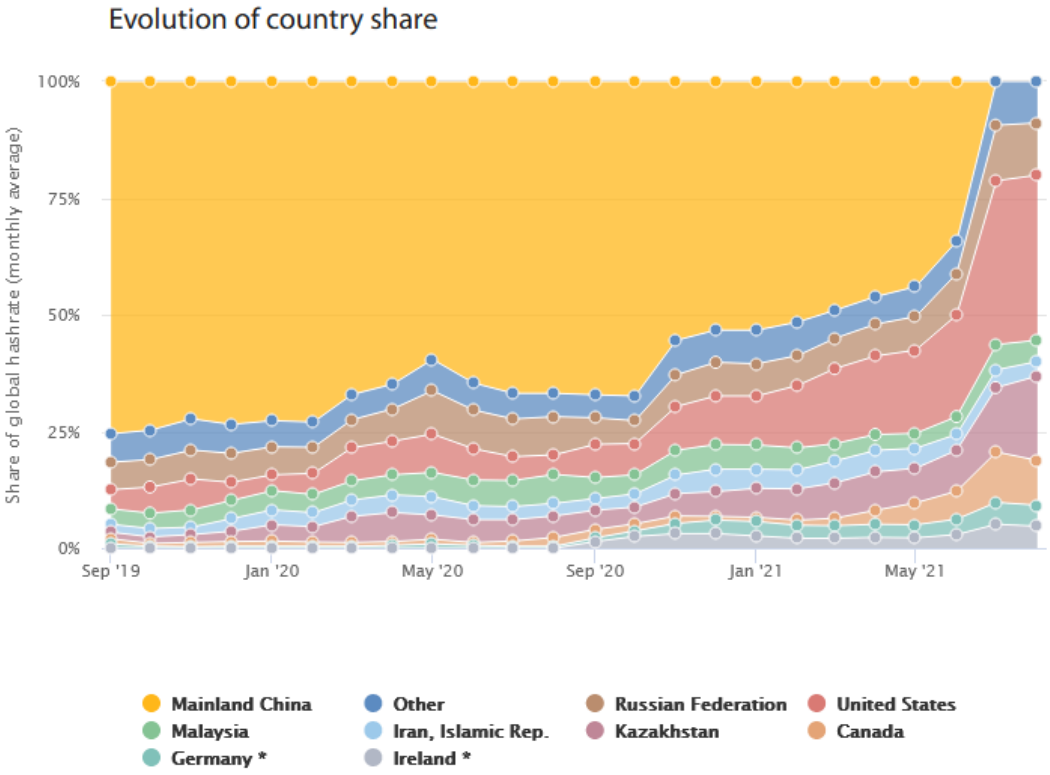


Figure 3.12: Hash rate suddenly migrates from China [Reuse rights requested]

as prices increases The fact that we can turn down whenever we need the power for other customers is fantastic. We can use that crypto currency to soak up that excess generation when there's a lot of that, and find a home for more solar and more wind to come to our grid. Then they reduce consumption when we need that power for other customers. So it's a great balancing act. Most other datacenters [such as] Microsoft or Amazon have other customers to serve every other day, so they can't just turn off. But these crypto customers can. If the cost of energy gets too high they can remove themselves from the market. They are also helpful if we lose a generator. They can quickly respond to that frequency disruption and allow us to balance our grid."
This "global energy market revolution" is explained by Tabatabai of Modo Energy.

There is growing interest and adoption of so called "stranded energy mining" which cannot be effectively transmitted to consumers, and is thereby sold at a huge discount while also developing power capacity, without the usual constraints [54], re-purposing historic infrastructure, and/or reducing the carbon (or more interestingly the methane) of existing infrastructure. Adam Wright of Vespene Energy says: *"You could either mine Bitcoin on one small landfill for a year, or you could plant 5 million trees and let them grow for 10 years - both of those are going to have the same environmental impact."*

Cheikosman, a policy analyst for the World Economic Forum (somewhat surprisingly) wrote *"Crypto is becoming an essential part of developing a carbon-neutral energy grid and has made it economically viable to invest in, develop and build renewable energy power generation."* The market economics of this are far from simple, but are well explained by Connell in a podcast.

The most cited example of building capacity before grid connection is El Salvador's

'volcano mining' proposal, which is supporting their national power infrastructure plans. Uzbekistan seems to be promoting a similar model with zero tax provided the Bitcoin mining companies build out their own solar infrastructure. A more poignant example is the Mechanicville hydro plant in the USA. The refurbishment of this 123 year old power plant is being funded by Bitcoin mining. This is the "buyer of last resort" model first advanced by Square Inc.

Conversely it might be that vertical integration of Bitcoin mining within legacy fossil fuel stations gives them a new lease of life. New York State has dealt with this kind of threat by imposing a moratorium on new, fossil fuel powered mining activity.

More pragmatically, Baur and Oll found that *"Bitcoin investments can be less carbon intensive than standard equity investments and thus reduce the total carbon footprint of a portfolio."*[55]. Perhaps of note for the near future is that KPMG whose investment was mentioned in the introduction also matched their position in the space with equivalent carbon offsets. This may provide an investment and growth model for others.

The power commitment to the network is variously projected to increase, or level off over time, but certainly not decrease. The industry now argues that economic pressures mean that most of the 'hashrate' is generated by renewable energy[56]. As a recent example of this trend Telsa (Elon Musk), Block (Twitters Jack Dorsey), and Blockstream (Adam Back) are teaming up to mine with solar energy in Texas.

The debate whether this consumption is 'worth' it is complex and rapidly evolving. Useful examples of this are:

- the online pushback to an academic article by PhD candidate de Vries et al. [57]
- the assertion that the widely cited Mora er al. paper in Nature [49] was based on an undergraduate class discussion, and has had an outsized effect on global policy.
- a paper from the Bitcoin Policy Institute,
- and the industry open letter to the EPA.
- this well considered Twitter thread by climate scientist Margot Paez.

It is somewhat confusing that positive views are coming only from diverse and non-specialist voices in the community, and never the academic community, but the shortcomings they point out in the supposedly considered articles such as Mora et al [49] are easily verified. Academia seems poorly positioned to pivot to this subject, as an ethical bar has to be established before research can commence, and the field is too new to make this an affordable task. This stuff is existentially important to the whole technology. Is a trillion dollar asset which potentially replaces the money utility of gold, but doesn't need to be stored under guard in vaults (Figure 3.13), worth the equivalent power consumption of clothes dryers in North America? Probably not with the current level of adoption, but this is an experiment in replacing global money. If that were to happen then Bitcoin would be around 50 times more efficient than the current system according to Khazzaka [58]. To be clear it's not the position of this book that replacing Fiat money is a good idea, but the experiment is being run regardless. This is explored in it's own chapter later.

It seems possible that three value propositions are therefore emerging:

- Bitcoin the speculative asset (or greater fool bubble [59]). Nations such as the USA, who own 30% of the asset have bid up the price of the tokens during a period of very cheap money, and this has led to a high valuation for the tokens, with a commensurately high network security through the hash rate (mining). This could be a speculative bubble, with the asset shifting to one of the other valuations below.
- Bitcoin the monetary network, and 'emerging market' value transfer mechanism.

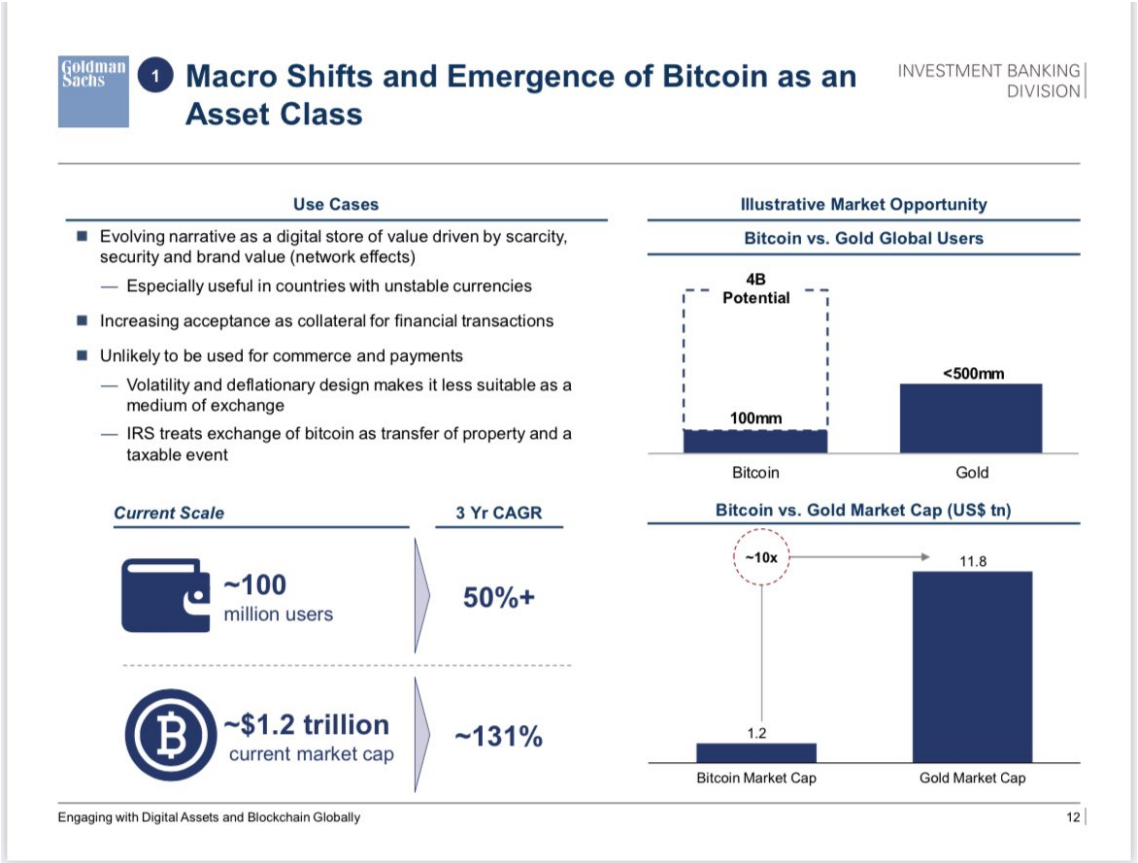


Figure 3.13: Goldman suggest growth opportunity and potential demonetisation of gold?

There is no sense of the "value" of this network at this time, but it's the aspect we need for our metaverse application. For this use the price must simply be high enough to ensure that mining viably secures the network. This security floor is unfortunately a 'known unknown'. If a global Bitcoin monetary axis evolves (as in the Money chapter later) the network would certainly require a higher rate than currently, suggestive of a higher price of token to ensure mining.

- Bitcoin as a flexible load in power distribution systems. Again there is no price against this, but we can perhaps grossly estimate it at around half the current hash rate if 50% of the network is currently green energy. This would imply a price for the asset roughly where it is now (ie, not orders of magnitude higher or lower).

Legislators globally, are starting to codify their positions on proof of work as a technology (including Bitcoin). The USA is variously supporting or constricting the technology, according to state legislatures. Notably New York has banned new carbon intensive mining facilities for 2 years, while rust and farm belt states with energy build-out problems are providing incentives.

The EU has just voted to add the whole of 'crypto', including PoW, to the EU taxonomy for sustainable activities. This EU wide classification system provides investors with guidance as to the sustainability of a given technology, and can have a meaningful impact on the flows of investment. With that said the report and addition of PoW is not slated until 2025, and it is by no means clear what the analysis will be by that point. Meanwhile they're tightening controls of transactions, on which there will be more detail later. For it's part the European Central Bank has come out in favour of strong constraints on crypto

mining. They use the widely discredited "digiconimist" estimates to assert that mining operations are disproportionately damaging to the environment.

We have seen that China has cracked down hard on the technology, banning mining and pressuring holders of the assets. They have unwound this somewhat, and based on past experience it seems that they will continue to nuance their position as they seek adoption of their own digital currency. As much as 20% of all mining activity is now suspected to take place within China.

In India there has been confusion for years as more "local" law vies with confusing central government signalling. It has variously been banned and unbanned, and is now subject to punitive tax. The central bank of India is strongly in favour of a complete ban. Ajay Seth, secretary of the Finance Ministry's Department of Economic Affairs recently said *"We have gone through a deep dive consulting with not just the domestic and institutional stakeholders but also organizations like IMF and World Bank.... Simultaneously we are also beginning our work for some sort of a global regulation (to determine) what role India can play... Whatever we do, even if we go to the extreme form, the countries that have chosen to prohibit, they can't succeed unless there is a global consensus"*

It feels like a global political response is just around the corner, but reputable voices in the community suggest that it always feels this way. There is more detail on this in Money chapter later in the book.

3.4.3 Technical overview

This section could be far more detailed, but this is pretty complex stuff. Instead, there's plenty of books and websites that do a more thorough job, if the reader is interested. Each subsection will include a good external link where more depth can be found. This whistle stop tour of the main components of the protocol should provide enough grounding, but it's not essential reading for non technical readers.

3.4.3.1 ECDSA / SHA256 / secp256k1

These technologies tend to use the same underpinning elliptic curve cryptography, and it makes sense to unpack this here just once, only in the context of Bitcoin, as this will be the main focus of our attention.

Public keys are a huge number used in conjunction with an algorithm to encrypt data. This allows a remote party to interact with an actor on the network whose private keys can decrypt that same data.

In Bitcoin the ECDSA algorithm is used on the secp256k1 elliptic function to create a trapdoor. This (essentially) one way mathematical operation was originally the "discrete log problem" and part of the research in cryptography by Diffie and Hellman [8]. This is what binds the public and private keys in a key pair (the foundation of the whole space).

In their mathematical construct a modulus operator creates an infinite number of possible variations on operations which multiply enormous exponential numbers together, in different orders, to create key pairs. In order to reverse back through the 'trapdoor' a probably impossible number of guesses would have to be applied.

Latterly, elliptic curves such as the secp256k1 curve used in Bitcoin have substantially simplified the computation problems. Rather than exponentials used by Diffie Helmman instead a repeated operation is applied to an elliptic curve function, and this itself creates a discrete log problem trapdoor in maths, far more efficiently. Figure 3.14 suggests how this works.

This makes it easier, faster, and cheaper to provide secure key pairs on basic computational resources. Elliptic curve solutions are not 'provably' secure in the same way as the Diffie-Hellman approach, and the security of this system is very sensitive to the randomness which is applied to the operation. Aficionados of Bitcoin use dice rolls or even more exotic means to add entropy (randomness) when creating keys. This really isn't necessary, the software does this well enough.

ECDSA has already been replaced by the more efficient Schnorr signature method [60] which uses the same mathematical curve so is backward compatible. This will take some time for organic adoption, and ECDSA will never be deprecated.

3.4.3.2 Addresses & UTXOs

Ethereum has addresses which transactions flow in and out of. This is synonymous to a bank account number and so makes intuitive sense to users of banks. This is not the case in Bitcoin.

Bitcoin is a UTXO model blockchain. UTXO stands for unspent transaction output, and these are 'portions' of Bitcoin created and destroyed as value changes hands (through the action of cryptographic keys). They are the basis of the evolving ledger. This process is described well by Rajarshi Maitra in this post.

"Every Transaction input consists of a pointer and an unlocking key. The pointer points back to a previous transaction output. And the key is used to unlock the previous output it points to. Every time an output is successfully unlocked by an input, it is marked inside the blockchain database as 'spent'. Thus you can think of a transaction as an abstract "action" that defines unlocking some previous outputs, and creating new outputs.
These new outputs can again be referred by a new transaction input. A UTXO or 'Unspent Transaction Output' is simply all those outputs, which are yet to be unlocked by an input. Once an output is unlocked, imagine they are removed from circulating supply and new outputs take their place. Thus the sum of the value of unlocked outputs will be always equal to the sum of values of newly created outputs (ignoring transaction fees for now) and the total circulating supply of bitcoins remains constant."

Fresh UTXOs are created as coinbase transactions, rewarded to miners who successfully mine a block. These can be spent to multiple output as normal. This is how the supply increases over time.

3.4.3.3 Bitcoin script

A Bitcoin script is a short chunk of code written into each transaction which gives conditions for the next UTXO transfer (spend). The limited scripting language and the features built into wallets on top, allow for some clever additional options beside receiving and spending. In fact, some of the more innovative features such as discrete log contracts (detailed later) are quite powerful, and can interact with the outside world. Scripts allow spends to be contingent on multiple sets of authorising keys, time locks into the future, or both.

3.4.3.4 Halving

As mentioned eariler, roughly every four year the 'block reward' given to miners halves. This gives the issuances schedule of Bitcoin; it's monetary inflation. This 'controlled supply' feature was added to emulate the growth of physical asset stocks through mining. It's exhaustively explained elsewhere and is somewhat immaterial to our transactional use case in metaverse applications.

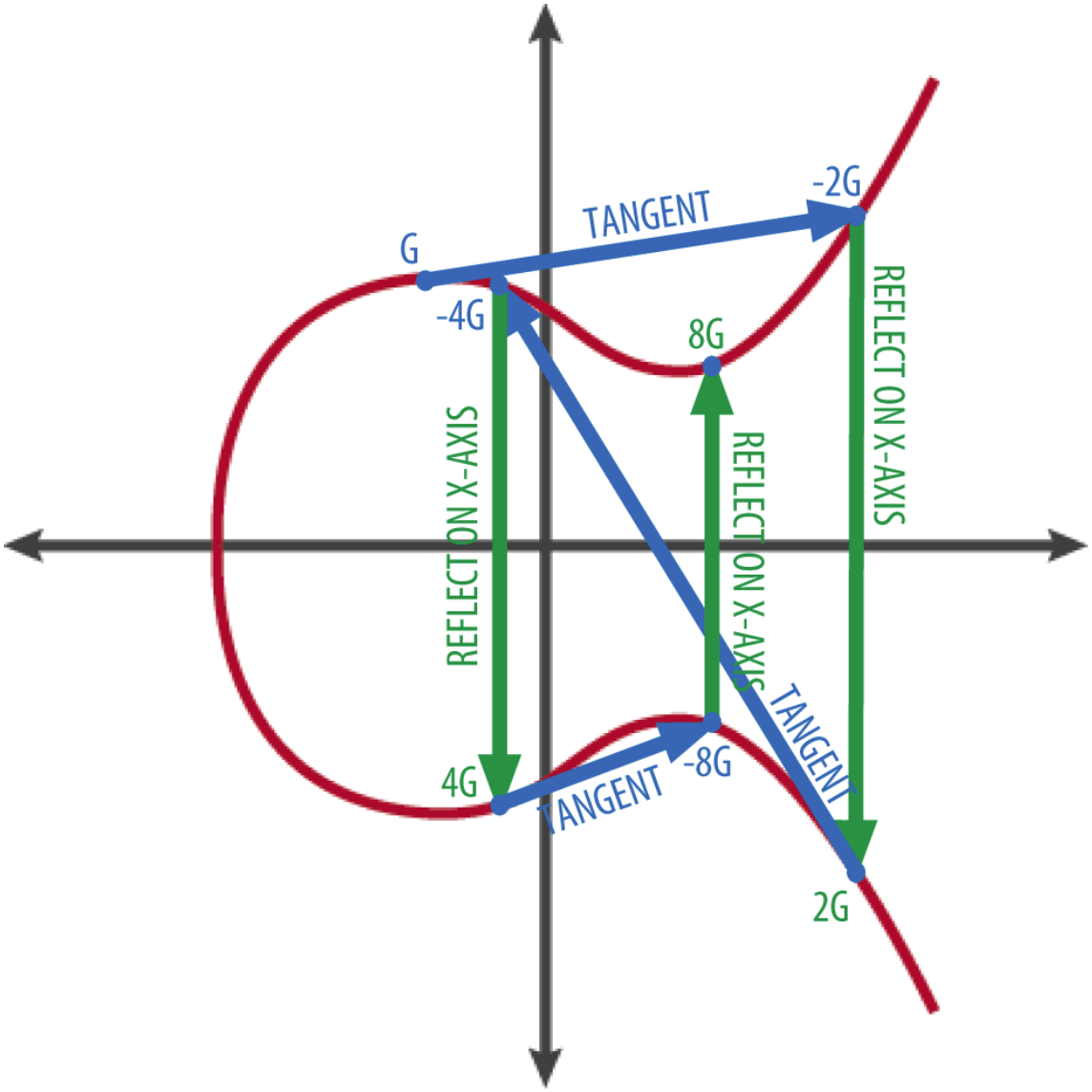


Figure 3.14: Given a start point on the curve and a number of reflection operations it's trivial to find a number at the end point, but impossible to find the number of hops from the two end points alone. (CC Mastering Bitcoin second edition)

3.4.3.5 Difficulty adjustment

The difficult adjustment (also mentioned earlier) shifts the difficulty of the mining algorithm globally to re-target one new block every 10 minutes. This means that adding a glut of new mining equipment will increase the issuance of Bitcoins, in favour of the new mining entity, for up to 2 weeks, at which point the difficulty increases, the schedule resets, and the advantage to the new miner is diffused. Equally this protects the network against significant loss of global mining hashrate, as happened when China comprehensively banned mining. Again, this is explained in more detail elsewhere.

3.4.3.6 Bitcoin nodes

The Bitcoin network can be considered a triumvirate of economic actors, each with different incentives. These are:

- Holders and users of the tokens, including exchanges and market makers, who make money speculating, arbitraging, and providing liquidity into the network. Increasingly this is also real 'money' users of BTC, earning and spending in pools of circular economic activity. Perversely Bitcoin as a money is the fringe use case at this time.
- Miners, who profit from creation of new UTXOs, and receive payments for adding transactions to the chain. In return they secure the network by validating the other miners blocks according the rules enforced by the node operators.
- Node operators, who enforce the consensus rule-set, which the miners must abide by in order to propagate new transaction into the network. In return node operators optimise their trust minimisation, and help protect the network from changes which might undermine their speculation and use of the tokens [61].

There are currently around 15,000 Bitcoin nodes distributed across the world. Since IT engineer Stadicus released his Raspibolt guide in 2017 there has been an explosion of small scale Bitcoin and Lightning node operators. Around thirty thousand Raspberry Pi Lightning nodes (which are also by definition Bitcoin nodes) run one of a big selection of open source distributions, with the most noteworthy explained alongside their stand-out feature-set:

- Raspiblitz offers fully opensource lightning focused functionality with a touchscreen display
- Mynode focuses on ease of use through a web interface and has many modules which users can try out.
- Umbrel is a more user friendly multi purpose node allowing access to a suite of Bitcoin and self sovereign individual tools.
- RoninDojo is designed for use alongside the privacy focused Samourai mobile wallet.
- nix-bitcoin focuses on security of the underlying operating system by building on NixOS.
- NODL is a premium prebuilt node focusing on security of the more performant hardware, and underlying operating system. It offers additional privacy tools.
- Start9 Embassy is a small form factor prebuilt unit at a lower price. It is a venture capital funded project with a more restrictive license but offers a suite of easy to use self sovereignty tools including Bitcoin.
- The CLBoss plugin can be combined with 'Core Lightning' to automate much of the management, and is a contender for our deployment too.

This is as good a time as any to start shaping a mission statement: **This book builds toward a new metaverse focused suite of tools, that utilises the nix-bitcoin distribution for the Bitcoin node**. There's a lot of components that haven't been covered yet, but nix-bitcoin is the first selected piece of open source software.

3.4.3.7 Wallets, seeds, keys and BIP39

In all the cryptographic systems described in this book everything is derived from a private key. This is an enormous number, and the input to the trapdoor function described earlier. As usual, it's beyond the scope of this book to 'rehash' the detail. Prof Bill Buchanan OBE has a great post on the basic version of this process.

In modern wallets, private keys (and so too their public keys), and addresses, are generated hierarchically. This is all part of BIP-0032. It starts with a single monstrously large number of up to 512 bits. From this are crafted Hierarchical Deterministic (HD) wallets, which use 'derivation paths' to make a tree of public/private key pairs, all seeded from this first number. This means that knowing the initial number, and the derivation path applied to it (just another number), wallets can search down the tree of derivations and find all the possible addresses. In this way a whole group of active addresses belonging to an entity can be held conveniently in one huge number (a concatenation of the input and path). This is the seed. Seeds are even more conveniently abstracted into a mnemonic called a seed phrase. Anyone interacting with these systems will see a 12 word (128 bits of entropy which is considered to be 'enough') or 24 word (256 bit) seed phrase. That phrase accesses the whole of the assets stored by that entity in the blockchain under it. A master key. These seeds can be generated by hand with dice, remember it's just a huge number and the onward cryptography at play here.

An address in Bitcoin is derived from the public/private key pair. Again this is a one way hash function. The public/private keys can't be found from the address. Addresses are really only a thing in wallets. They contain the element necessary to interact with the UTXOs. Many UTXOs can reside under an address, in that they just share the same keys. Wallets and nodes can monitor the blockchain to see transactions that 'belong' to addresses owned by the wallet, then they can perform unlocking of those funds to move them, through operations on the UTXOs via keys.

3.4.3.8 Custody

The topic of 'custody' of Bitcoin (addresses,UTXOs) can be confusing at first. This is another area where there's a lot of detail available, but not all of it is appropriate because increased complexity increases risk. Broadly though it's important to remember that ownership of a UTXO is passed around using signing keys, which are functions of wallets. Wallets themselves don't contain Bitcoin, they contain keys. The simplest approach is a software wallet. This is an application on a device, which stores the private keys, and manages signing of transactions which go onto the blockchain. It's beyond the scope of this book to review or suggest software in detail, but Bluewallet on mobile devices, and Sparrow Wallet on desktop devices provide rich basic functionality if a reader wishes to get started immediately. Note that these software wallets send your extended public key (the path of those keys) to the wallet providers server, for the monitoring of the blockchain to happen on it's behalf. They're updated by the software vendor, not the blockchain direct. To get this to 'privacy best practice' commensurate with the aim of this book it's necessary to run a full node as detailed above, and connect the wallet software to that on a secure or local connection.



Figure 3.15: Seedsigner is an inexpensive open source project which scans the master seed in from a QR code to enable signing. One device can run a quorum based wallet (multisig).

So called Hardware wallets like Coldcard should perhaps be termed signing devices. Rather than store Bitcoin they store the private key in a more secure way, in a device which interacts with a computer or phone, or else they scan in the seed each time themselves as is the case with opensource "seedsigner" (Figure 3.15).

For higher security it's possible to combine hardware and software wallets (signing devices) to provide a quorum of signatures required to move funds. More exotic still are proposals like "Fedimint" which allows groups such as families or villages to leverage their personal trust to co-manage Bitcoin. What is not/rarely secure is leaving Bitcoin with a custodian such as an exchange as they simply issue you with an IOU and may abscond. In building toward a proposal for a product in this book it would be simple for us to build a metaverse which users simply paid to use. This is the norm up to now. Representative money would flow around in the metaverse and be changed back like game money at some point. This is not what we wish to promote, so everything will be a variation on "self-custody", minimising third party trust for users.

3.4.4 Upgrade roadmap

3.4.4.1 Taproot

'Taproot' is the most recent upgrade to the Bitcoin network. It was first described in 2018 on bitcoin-dev mailing list, and become BIP-0341 in 2019. It brings improved scripting, smart contract capability, privacy, and Schnorr signatures [60], which are a maximally efficient signature verification method. The network will always support older address types. It is rare to get such a large update to the network, and deployment and upgrade was carefully managed over several months under BIP-0008. Uptake will be slow as wallet

manufacturers and exchanges add the feature. It can be considered an upgrade in progress (0.3%). Aaron van Wirdum, a journalist and educator in the space describes Taproot in detail in an article.

3.4.4.2 AnyPrevOut

BIP-0118, is a "soft-fork that allows a transaction to be signed without reference to any specific previous output". It enables "Eltoo, a protocol that fulfils Satoshi's vision for nSequence"

This is Lightning Network upgrade technology in the main. The Eltoo whitepaper or this more readable explanation from developer fiatjaf go into detail.

3.4.4.3 CheckTemplateVerify

BIP-0119 is "a simple proposal to power the next wave of Bitcoin adoption and applications. The underlying technology is carefully engineered to be simple to understand, easy to use, and safe to deploy". At it's most basic it is a constructed set of output hashes, creating a Bitcoin address, which if used, can only be spent under certain defined conditions. This is a feature called 'covenants'. It enables a feature called 'vaults' which provides additional safety features for custodians. There is currently some debate about the activation process, and the feeling is that it won't happen (soon).

3.4.4.4 Blind merge mining

BIP-0301 allows 'other' chains transactions to be mined into Bitcoin blocks, and for miners to take the fees for those different chains, without any additional work or thoughts by the miners. This is also a prerequisite for Drivechains (mentioned later), and improve Spacechains. In a way this can offer other chains the security model of the Bitcoin network, while increasing fees to miners, which might be increasingly important as the block subsidy falls. This is pretty fringe knowledge originally proposed by Satoshi, but has been refined since and is best explained by Paul Sztorc elsewhere. It is likely an important upgrade in light of the security budget of Bitcoin.

3.4.4.5 Simplicity scripting language

Simplicity is a proposed contract scripting language which is 'formally provable'. This would provide a radical upgrade to confidence in smart contract creation. It is work in progress, and looks to be incredibly difficult to develop in, despite the name. It is more akin to assembly language. Development has recently slowed, and the proposal requires a soft fork to Bitcoin. The main reason to think it stands a chance of completion vs other similar proposals is the powerful backing of Blockstream, one of the main drivers of the Bitcoin ecosystem, run by Adam Back (potential co-creator of Bitcoin).

3.4.4.6 Tail emission

It is conceivable though unlikely that Bitcoin will choose to remove the 21 million coin hard cap in the end. This would potentially result in a stable and predictable supply, compensating for lost coins, and reinvigorating the miner block reward. The Bitcoin narrative is **so** invested in the 'hard money' thesis that is seems such a hard fork would be contentious at least, and possibly existentially damaging. Peter Todd, long time Bitcoin Core contributor things the idea has merit and has described it in a blog post.

3.4.4.7 Ossification

The Bitcoin code is aiming toward so called "ossification". The complete cessation of development of the feature set. This would provide higher confidence in the protocol moving forward, as long term investors would be somewhat assured that the parameters of the technology would not change, and potentially pressure on the developers would reduce. There's a push to get some or all of the features described above in over the next few year before this happens. As ever this is a controversial topic within the development community. Notably Paul Sztorc, inventor of Drivechain feels strongly that cessation of innovation is a fundamental mistake, while also agreeing that ossification is necessary.

3.5 Extending the BTC ecosystem

The following section are by no means an exhaustive view of development on the Bitcoin network, but it does highlight some potentially useful ideas for supporting metaverse interactions in a useful timeframe.

3.5.1 Keet by holepunch

Tether and Bitfinex have released Keet messenger which allows peer to peer video calling and file sharing. It will be BTC and Tether enabled which allows transmission of value in a trust minimised fashion. It is built upon the same Hypercore "holepunch" technology used by Synonym.

3.5.2 Block & SpiralBTC

Block (formally the payment processor "Square" is now an umbrella company for several smaller 'building block' companies, all of which are major players in the space. Block itself is now part of the W3C web consortium, so they will be driving a new era of standards in distributed identity and value transfer.

SpiralBTC, formally 'Square Crypto' (a subsidiary of Square) is funding development in Bitcoin and Lightning. Their main internal product is the Lightning Development Kit (LDK). This promising open source library and API will allow developers to add lightning functionality to apps and wallets. It is a useful contender for our metaverse applications. They also fund external open source development.

3.5.3 BTCPayServer

BTCPayServer is one of the recipients of a Spiral grant. It is a self hosted Bitcoin and Lightning payment processor system which allows merchants, online, and physical stores and businesses to integrate Bitcoin into their accounting systems. It might seem that if one were to use Bitcoin then a simple address published on a website might be enough, but this is far from privacy best practice. Using a single address creates a data point which allows external observers to tie all interactions with a given point of sale to all of the customers, and onward to all of their other transactions through the public ledger. Since we seek to employ cyber security best practice will avoid the issues with address reuse. Each Bitcoin address should be used just once. This is fine as there's essentially an unlimited number of addresses.

In a metaverse application there is no website to interact with, but fortunately BTCPay-Server is completely open source and extensible, has a strong support community, and an

API which could be integrated with a virtual world application. BTCPayServer supports the main three distributions of Lightning but would potentially need extending in order to work with newer technology like RGB or Omnibolt.

3.6 Lightning (Layer 2)

Lightning was a 2016 proposal by Poon and Dryja [62], and is a method for networks of channels of Bitcoin between parties, which can transfer value. The main public network is a community driven liquidity pool which enables scaling and speed improvements for the Bitcoin network. It makes Bitcoin more like money [63]. As with Bitcoin base chain there are multiple standards and approaches, but within Lightning these are not necessarily cross compatible with one another, resulting in several Lightning networks. This is to our advantage as innovation is possible within these smaller networks. It is mainly 'powered' by thousands of volunteers who invest in hardware and lock up their Bitcoin in their nodes, to facilitate peer-to-peer transactions. Zebka et al. found that although the network is "fairly decentralised" it is more recently skewing to larger more established nodes [64]. Though this is a grassroots technology the nature of the design means it can likely be trusted for small scale commercial applications.

The following text is from John Cantrell, an engineer who works on Lightning.

"The Lightning Network is a p2p network of payment channels. A payment channel is a contract between two people where they commit funds using a single onchain tx. Once the funds are committed they can make an unlimited amount of instant & free payments over the channel. You can think of it as a tab where each person tracks how much money they are owed. Each time a payment is made over the channel both parties update their record of how much money each person has. These updates all happen off-chain and only the parties involved know about them. When it's time to settle up the two parties can take the final balances of the channel and create a channel closing transaction that will be broadcast on chain. This closing transaction sends each party the final amounts they are owed. This means for the cost of two on-chain transactions (the opening and closing of the channel) two parties can transact an unlimited number of times and the overall cost of each transaction approaches zero with every additional transaction they make over the channel. Payment channels are a great solution for two parties to transact quickly and cheaply but what if we want to be able to send money to anyone in the world quickly and cheaply? This is where the Lightning Network comes into play, it's a p2p network of these payment channels. This means if Alice has a payment channel with Bob and Bob has a channel with Charlie that Alice can send a payment to Charlie with Bob's help. This idea can be extended such that you can route a payment over an arbitrary number of channels until you can reach the entire world. Routing a payment over multiple channels uses a specific contract called a Hash Time Locked Contract (HTLC). It introduces the ability for Bob and any other nodes you route through to charge a small fee. These fees are typically orders of magnitude smaller than onchain fees. This all sounds great but what if someone tries to cheat? I thought the whole point of Bitcoin was that we no longer had to trust anyone and it sure sounds like there must be some trust in our channel partners to use the Lightning Network? The contracts used in Lightning are built to prevent fraud while requiring no trust. There is a built-in penalty mechanism where if someone tries to cheat and is caught then they lose all of their money. This does mean you need to be monitoring the chain for fraud attempts."

Lightning is a key scaling innovation in the bitcoin network at this time. It is seeing rapid development and adoption (Figure 3.16). The popular payment app "Cash App" integrates the technology, and 'Lightning Strike' services the USA, El Salvador, and Argentina with zero exchange and transmission fees. It allows for unbound scaling of transactions (millions of transations per second compared for instance to around 45,000 TPS in the VISA settlement network). Transaction costs are incredibly low, and the transaction speed virtually instantaneous.

The most popular lightning software is LND from Lightning Labs or C-Lightning from Blockstream. The software can be run on top of any Bitcoin full node, in a browser extension with a limited node, in a mobile app as a client or a server, or a hybrid such as the Greenlight server used by Breez wallet. Different trust implications flow from these choices.

3.6.1 Micropayments

Possibly the most important affordance of the Lightning network is the concept of micro-payments, and streaming micropayments. It is very simple to transfer even one satoshi on Lightning, which is one hundred millionth of a bitcoin, and a small fraction of a penny. This can be a single payment, for a very small goods or service, or a recurring payment on any cadence. This enables streaming payments for any service, or for remittance, or remuneration. These use cases likely have enormous consequences which are just beginning to be explored. Integration of this capability into metaverse applications will be explored later.

3.6.2 BOLT12 and recurring payments

BOLT12 is a new and developing 'standard' which simplifies and extends the capability of the network for recurring payments, but can negotiate single payments too. The example keyring QR code seen in Figure 3.17 can be scanned to send single or recurring payments securely and anonymously to the holder.

3.6.3 Fedimint and Fedi app

From the blog post on the Fedi App website; Fedimint is:

- a form of community Bitcoin custody,
- utilising federations (a byzantine fault tolerant multi-sig wallet technology similar to Blockstream's Liquid network),
- run collectively by groups of trusted community members we call "guardians",
- for and on behalf of their communities,
- with privacy through Chaumian e-cash,
- and with close integration with the Lightning Network

Obi Nwosu sees Fedimint as the third vital pillar of the Bitcoin ecosystem. If Bitcoin is secure decentralised money, and Lightning is decentralised payments, then he says Fedimint is decentralised custody of the Bitcoin asset. The excitement in the community is such that this protocol is included in our metaverse stack later. With Fediment a clade of users within the metaverse would have near perfect transactional privacy within their group inside the metaverse [11]. This could be a potentially huge group of users, and could include AI actors in the scene. Transactions with the outside world could be through lightning as already planned.

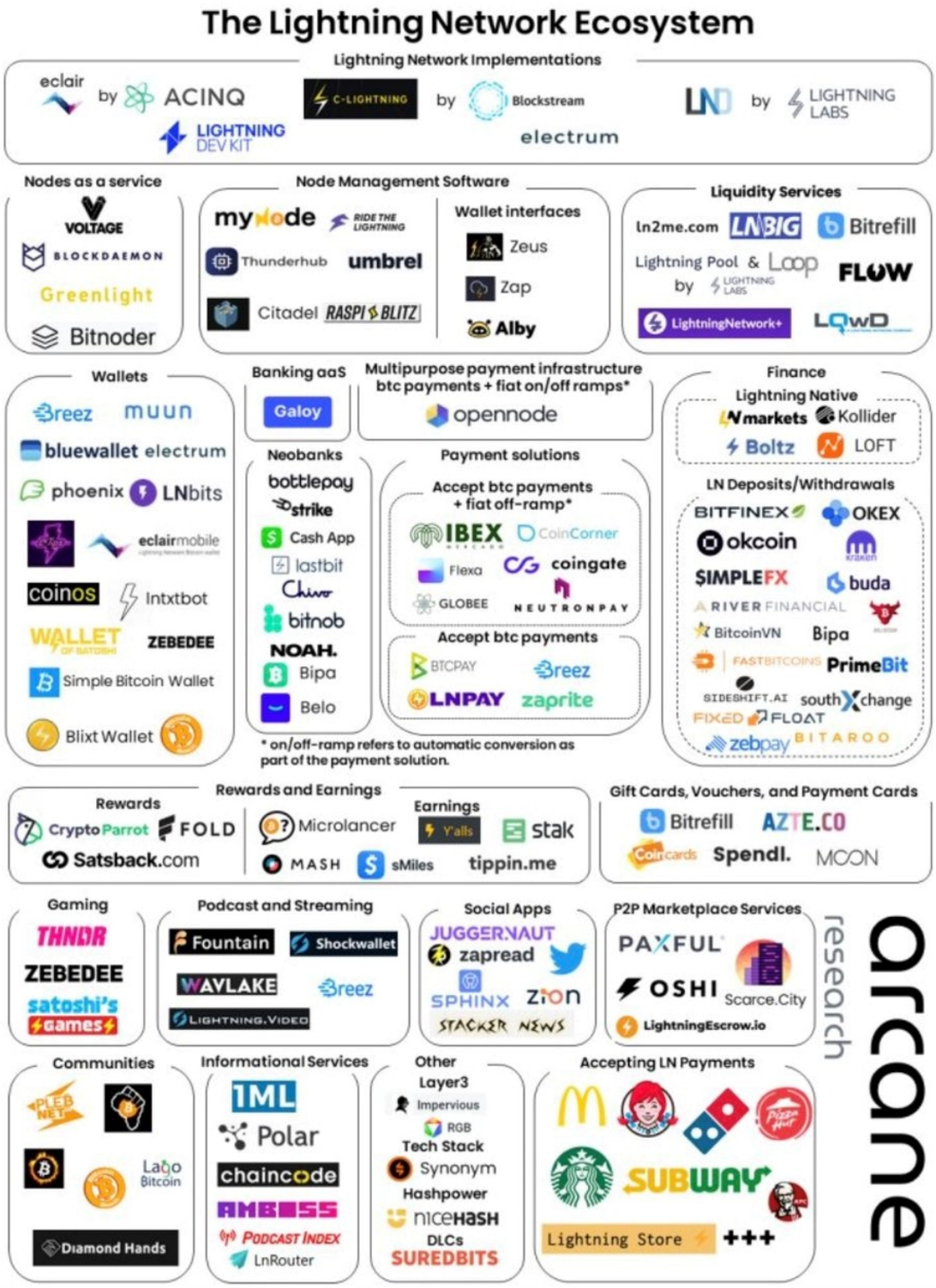


Figure 3.16: Arcane research lightning adoption overview.



Figure 3.17: A key fob with a Bolt12 QR code

3.6.4 LNURL-auth

What is LNURL-auth? *"LNURL-auth is a generic authentication protocol. It authenticates the user using digital signatures, which means that the user needs to have a public-private key pair. Thanks to the rising popularity of lightning wallets, more and more users are in possession of and have easy access to such keys. Consequently, users are identified by their public keys, nothing else. The protocol does not require any other identifying information such as passwords, emails, usernames, or similar."*

LNURL-auth may be able to service all of our user management via LNBits.

3.6.5 LNBits

LNBits is an open source, extensible, Lightning 'source' management suite. It is self hosted, and can connect to a variety of Lightning wallets, further abstracting the liquidity to provide additional functionality to network users. Remember that all of these tools run without a third party, on a £200 setup, hosted at home or within a business. The best way to explore this is to describe *some* of the plugins.

- "Accounts System; Create multiple accounts/wallets. Run for yourself, friends/family, or the whole world!"
- Events plugin allows QR code tickets to be created for an event, and for payments to be taken for the tickets.
- Jukebox creates a Spotify based jukebox which can be deployed online or in physical locations.
- Livestream provides an interface for online live DJ sets to receive real-time Lightning tips, which can be split automatically in real-time with the music producer.
- TPoS, LNURLPoS & OfflineShop support online and offline point of sale (Figure

3.18).
- Paywall creates web access control for content.
- LightningTipBot is a custodial Lightning wallet and tip handling bot within the popular on Telegram instant messenger service.

Together these plugins are incredibly useful primitives which are likely to be translatable to a multi party metaverse application. A proposal for building a more specific plugin along these lines is detailed later.

LnBits is capable of backing every object in a metaverse scene as an economic actor, with a key which is compatible with Nostr. This makes it the best choice and it will likely form the core of the proposed metaverse stack.

3.6.6 Etleneum

Etleneum is a centralised smart contract platform built around Lightning invoices. It is most notable as a sign of things to come. There are many small contracts available to try on the site, such as a simple market for moving value between lightning and Bitcoin layer 1, or this simple auction. Contracts are able to operate on data drawn from the wider web, and automatically send and receive lightning payments based on conditional states. It should be viewed as an experiment which allows tinkering in smart contracts, and therefore potentially useful for the software proposed in the final section. There are suggestions that this approach might (with some work) allow layer 3 computation more like Ethereum etc.

3.6.7 Message passing

It is possible to pass data alongside lightning payments, routing messages between parties across the global network. This means that a host of other applications can inherit the privacy and censorship resistance of the Lightning network. First amongst these has been simple message passing and group messenger clients such as Sphinx, Juggernaut, Impervious messenger, and RGB Lightning chat. To be clear, this is considered by some to be a misappropriation of the function of the network, and pretty silly given the number of end to end encrypted chat clients available. One more developed use case has been demonstrated by the Impervious development team; they use the message passing capability to negotiate a virtual private network between two parties, using open source software. This allows a secure side channel between internet IP addresses to be opened without a trusted third party. This in itself is a much sought after function of privacy minded networking, and the basis for much of their Impervious browser feature set.

3.7 Liquid federation (layer 2)

Liquid is an implementation on Blockstream Elements, and is itself part of the open source development contribution of Blockstream, the company started by Adam Back (of hashcash fame) and nearly a dozen other early cypherpunks and luminaries.

The Liquid side chain network, and it's own attendant Lightning layer 2, is a fork of Bitcoin with different network parameters. In liquid the user of the network 'pegs' into the Bitcoin network, swapping tokens out from BTC to L-BTC (this can of course mean very small subunits of 1 Bitcoin). Once tokens have been 'locked' and swapped to Liquid the different network parameters used in the fork allow a different trust/performance trade-off. Liquid is fast on the L1 chain, cheaper to use at this time, and more private. The consensus achieved on this side chain network is faster because it is a far smaller group of node



Figure 3.18: Two of the many prebuilt and kit options for Lightning 'point of sale'

operators. The next block to be written to the side chain is chosen by a node operated by a member of a federation of dozens of major contributors to the Bitcoin technology space. These 'trusted' nodes all check one another's security and network operations, meaning that the network is as secure as the aggregate of the trust placed in half of the membership at any one time. There are still dozens of major companies, development teams, and individual actors, with significant reputational investment.

"Federation members contribute to the Liquid Network's security, gain voting rights in the board election and membership process, and provide valuable input on the development of new features. Members also benefit from the ability to perform a peg-out without a third party, allowing their users to convert between L-BTC and BTC seamlessly within their platform."

Crucially for our purposes here Liquid allows tokenised asset transfer. Anyone can issue an asset on Liquid. Such transfers of assets may be orders of magnitude cheaper than on chain Bitcoin transactions, but still potentially orders of magnitude more expensive than a simple Lightning transaction of value on the Bitcoin network.

Blockstream plan to add arbitrary (user generated) token support to their 'Core Lightning' implementation at some point. This would be a very strong choice for specific use cases within an economically enabled metaverse application. When participants wish to 'cash out' of the Liquid network they must do this through one of the federation members who activate the other side of the 'two-way peg', dispensing the equivalent amount of Bitcoin. This is transparently handled through Blockstream's "green wallet".

All of this has the advantage of a far lower energy footprint compared to the main chain, but it's not quite ready with a full suite of affordances.

The Liquid network is being used as the underlying asset for a novel new global financial product. El Salvador are working with Blockstream to issue a nation state backed bond.

3.8 Bitcoin Layer 3

Increasingly important features of modern blockchain implementations are programmability through smart contracts, and issuance of arbitrary tokens. Assigning a transaction to represent another thing like an economic unit, energy unit, or real world object, and operating on those abstractions within the chain logic. Chief among these use cases are stablecoins such as Tether, which are pegged to national currencies and described in the next section. Bitcoin has always supported very limited contracts called scripts, and stablecoin issuance has existed in Bitcoin since Omni Layer. Omni was the first issuer of Tether, but more recently these important features have passed to other layer one chains. This year is likely to see the resurgence of this capability on Bitcoin, which of course benefits from a better security model. Once again, there is a stong assertion by some that this isn't even possible. The debate is complex and unresolved.

In order to properly understand the use of Bitcoin based technologies in metaverse applications it is necessary to examine what these newer 'layer 3' ideas might bring.

3.8.1 LNP/BP and RGB

LNP/BP is a non profit standards organisation in Switzerland which contributes to open source development of Bitcoin layer 3 solutions into the Lightning protocol, and Bitcoin protocol (LNP/BP). One of the core product developments within their work is the 'RGB'

protocol, which is somewhat of a meaningless name, evolved from "coloured coins" which were an early tokenised asset system on the Bitcoin network. RGB represents red, green, and blue. The proposal is built upon research by Todd and Zucco. RGB is regarded as arcane Bitcoin technology, even within the already rarefied Bitcoin developer communities. Zucco provides the following explanation:

"When I want to send you a bitcoin, I will sign the transaction, I will give the transaction only to you, you will be the only one verifying, and then we'll take a commitment to this transaction and that I will give only the commitment to miners. Miners will basically build a blockchain of commitments, but without the actual validation part. That will be only left to you. And when you want to send the assets to somebody else, you will pass your signature, plus my signature, plus the previous signature, and so on."

This is non-intuitive explanation of Todds 'single-use-seals', applied to Bitcoin, with the purpose of underpinning arbitrary asset transfer secured by the Bitcoin network. In this model the transacting parties are the exclusive holders of the information about what the object they are transferring actually represents. This primitive can (and has) been expanded by the LNP/BP group into a concept called 'client side validation'. It's appropriate to explain this concept several times from different perspectives, because this is potentially a profoundly useful technology for metaverse applications.

- A promise is made to spend a multi output transaction in the future. This establishes the RGB relationships between the parties.
- One of the pubkeys to be spent to is known by both parties.
- The second output is unknown and is a combination of the hash of the state, and schema, from the operation which has been performed.
- When the UTXO is spent the second spends pubkey can be processed against the shared data blob to validate the shared state in a two party consensus (sort this out, it's nonsense).
- This is now tethered to the main chain. Some tokens from the issuance have gone to the recipiant, and the remainder have gone back to the issuer. More tokens can be issued in the same way from this pool.
- A token schema in the blob will show the agreed issuance and the history back to the genesis for the token holder.
- The data blob contains the schema which is the key to RGB functions and the bulk of the work and innovation.
- Each issuance must be verified on chain by the receiving party.

This leverages the single-use-seal concept to add in smart contracts, and more advanced concepts to Bitcoin. Crucially, this is not conceptually the same as the highly expressive 'layer one' chains which offer this functionality within their chain logic. In those systems there is a globally available shared consensus of 'state'. In the LNP/BP technologies the state data is owned, controlled, and stored by the transacting parties. Bitcoin provides the crytographic external proof of a state change in the event of a proof being required. This is an elegant solution in that it takes up virtually no space on the blockchain, is private by design, and is extensible to layer 2 protocols like Lightning.

This expanding ecosystem of client side verified proposals is as follows:

- RGB smart contracts
- RGB assets are fungible tokens on Bitcoin L1 and L2, and non fungible Bitcoin L1 (and somewhat on L2).
- Bifrost is an extension to the Lightning protocol, with it's own Rust based node

implementation, and backwards compatibility with other nodes in the network. This means it can transparently participate in normal Lightning routing behaviour with other peers. Crucially however it can also negotiate passing the additional data for token transfer between two or more contiguous Bifrost enabled parties. This can be considered an additional network liquidity problem on top of Lightning, and is the essence of the "Layer 3" moniker associated with LNP/BP. It will require a great number of such nodes to successfully launch token transfer on Lightning. As a byproduct of it's more 'protocol' minded design decisions Bifrost can also act as a generic peer-to-peer data network, enabling features like Storm file storage and Prometheus.

- AluVM is a RISC based virtual machine (programmable strictly in assembly) which can execute Turing complete complex logic, but only outputs a boolean result which is compliant with the rest of the client side validation system. In this way a true or false can be returned into Bitcoin based logic, but be arbitrarily complex within the execution by the contract parties.
- Contractum is the proposed smart contract language which will compile the RGB20 contracts within AluVM (or other client side VMs) to provide accessible layer 3 smart contracts on Bitcoin. It is a very early proposal at this stage.
- Internet2: "Tor/noise-protocol Internet apps based on Lightning secure messaging
- Storm is a lightly specified escrow-based bitcoin data storage layer compliant with Lightning through Bifrost.
- Prometheus is a lightly specified multiparty high-load computing framework.

Really, any compute problem can be considered applicable to client side validation. In simplest terms a conventional computational problem is solved, and the cryptographically verifiable proof of this action, is made available to the stakeholders, on the Bitcoin ledger.

Less prosaically, at this stage of the project the more imminent proposed affordances of LNP/BP are described in 'schema' on the project github. The most interesting to the technically minded layperson are:

- RGB20 fungible assets. This could be stablecoins like dollar or pounds representation. This is a huge application area for Bitcoin, and similar to Omni, which will also be covered next.
- RGB21 for nonfungible tokens and ownership rights. In principle BiFrost allows these to be transferred over a the Lightning network, significantly lowering the barrier to entry for this whole technology. DIBA have this technology working on testnet.
- RGB22 may provide a route to identity proofs. This is covered in detail later.

Federico Tenga is CEO of 'Chainside' and an educator and consultant in the space. He has written an up-to-date "primer", which is still extremely complex for the uninitiated, but does capture how the RGB token transfer system works. That medium article also touches on Taro, which is next.

3.8.2 Taro

Taro is an very new initiative by Lightning Labs to allow assets to transmit on the Lightning network. It is more similar to RGB above than Omnibolt below. They say: *"Taro enables bitcoin to serve as a protocol of value by allowing app developers to integrate assets alongside BTC in apps both on-chain and over Lightning. This expands the reach of Lightning Network as a whole, bringing more users to the network who will drive more*

volume and liquidity in bitcoin, and allowing people to easily transfer fiat for bitcoin in their apps. More network volume means more routing fees for node operators, who will see the benefits of a multi-asset Lightning Network without needing to support any additional assets."

The project has clearly been under development by the lead developer at Lightning Labs for some years and seems both capable and mature, though they are obviously following the model of 'co-opting' open source ideas (from RGB) to garner venture capital funding. They credit RGB in the github. More will doubtless be added to this section and it seems a contender for our metaverse purposes, being less broadly ambitious than RGB upon which it's based, but perhaps more focused and implemented. The key feature of Taro seems to be that only the first and last hop in a multi-hop lightning transaction need to support Taro, because of external data validation databases called "universes". This is an advance on the RGB proposal. The technical specs are now on the lightning labs web pages.

3.8.3 Slashpay

Slashpay is a very promising and recent product, and part of a suite of interlinked (Bitcoin compatible) layer 3 ideas. It is *not* a blockchain technology, but it is highly intersectional with Bitcoin. The Synonym suite is advocating what they call the 'Atomic Economy', an overarching abstraction of any of the technologies in the space into a single cryptographic key pair, with all the other products nested under it. The suite will be selected and unpacked for metaverse purposes later, but for this section the Slashpay product integrates as a layer three idea, building upon lightning.

Slashpay gathers all of the available Lightning invoice and QR code 'standards' under an abstracted metastandard with it's own key pair. This allows a negotiation between party and counterparty in code, which settles on agreeable standards for the value transfer. The Slashpay mediation metadata is embedded in the top level Slashtag QR code. Within the Slashpay element of the data is a priority list for the exchange, which can be changed by the user according to their capability and preferences.

The code to support this is in a early stage. There is a minimum viable product which can negotiate between online Lightning nodes. The advantage of the Slashpay method, and the thing that puts it in the layer 3 section, is that in the event of a failed Lightning payment (for whatever reason), the software can then default to the next payment method in it's negotiated list. This would most likely be another (different) Lightning attempt, or a Bitcoin main chain transaction.

This technical ecosystem uses a 'distributed hash table' to hold and negotiate keys, stored using Hypercore, another external project based on Bittorrent. This is the 'Hyperswarm DHT', which has potential uses elsewhere in the metaverse use cases.

There is clearly additional complexity in setting this system up, but once in place it might provide a unified way to scale capability under the evolving standard.

3.8.4 Spacechains

Spacechains is a proposal by Ruben Somsen. It is a way to provide the functionality of any conceivable blockchain, by making it a sidechain to Bitcoin.

Like RGB described earlier it's a single use seal, but which can be closed by the highest bidder.

In a spacechain the Bitcoin tokens are destroyed in order to provably create the new

spacechains tokens at a 1:1 value. These new tokens only have worth moving forward within the new chain ecosystem they represent, as they cannot be changed back. They nontheless have the same security guarantees as the bticoin main chain, though with a radically reduced ecological footprint (x1000?), and higher performance. Each 'block' in the new chain is a single bitcoin transaction. The high level features are:

- Outsource mining to BTC with only a single tx per block on the main chain.
- One way peg, Bitcoin is burnt to create spacechain tokens.
- Allows permissionless chain creation, without a speculative asset.
- Fee bidding BMM is space efficient and incentive compatible. Miners just take the highest fees as normal.
- Paul Sztorc raised the idea
- It's best with a soft fork but possible without

The concept is explained fully in a recent presentation at Advancing Bitcoin conference.

3.8.5 Statechains, drivechain, softchains

There are many proposals for layer 2 scaling solutions for the bitcoin network. Ruben Somsen describes Softchains, Stateschains, and Spacechains, while Drivechain is described by the author Paul Sztorc on the project web pages and is split across BIP-0300 for drivechain and BIP-0301 for a "blind merge mining", a soft fork which it's unlikely to get. They are all hypothetical with the exception of sidechains.

3.9 Other chains and networks

It's useful to make some 'honourable mentions' of other options as this technology is moving so fast. These chains are viewed by some as a kind of triage for ideas which might one day find their way into Bitcoin. This is potentially most true of zk rollups which might eventually migrate from privacy and scaling experiments on other chains [65]. This list simply isn't very useful in terms of judging other chains, as they rise and fall so fast. To be clear, there is a fundamental *legal* difference between all of the 15,000 or so attempts at layer 1 chains after Bitcoin, in that they are controlled by a subset of people who have an incentive to lie about the usefulness of the technologies they are invested in. This lack of useful decentralisation has been touched on but is dealt with in detail by Microstrategy CEO Michael Saylor in a four hour podcast with Ai researcher Lex Fridman. It's interesting that Saylor (who is a significant educator in the space) views custodial companies holding Bitcoin on behalf of their clients as Bitcoin layer 3. All of this is new enough that virtually all of it is contested by someone. To demonstrate the difference between Bitcoin as a property vs alt coins as 'securities in law' it's useful to see the allocations of tokens to seed investors in some of the newer chains in Figure 3.19.

3.9.1 Layer 1 chains

As the market wanes in 2022 the fragility of tokens other than Bitcoin is being exposed. They are suffering brutal losses. Historically tokens spend around 19 weeks in the top tier of tokens before falling away. Each cycle brings and new crop during the bull market and these invariably don't make it through to the next cycle. There are a few which have longevity and name recognition, but mainly because they amassed enough capital during the early days to play a very long, if somewhat pointless game.

- Monero is a privacy focused coin with a great deal of credible and competent

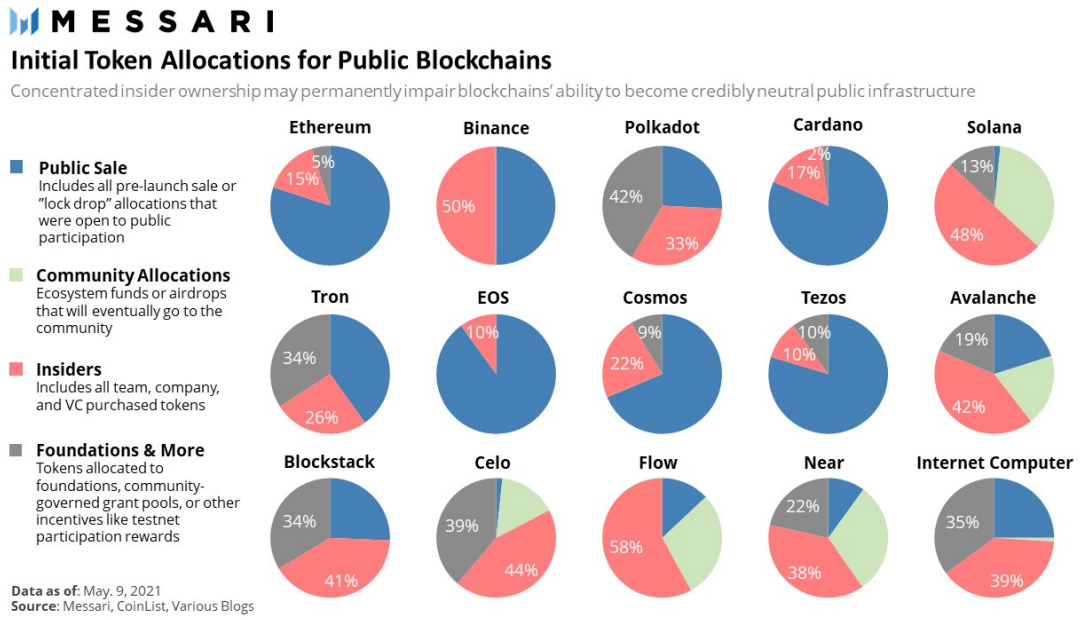


Figure 3.19: Allocations given at the beginning of public blockchain, by Messari.

developer attention. It attracts a lot of criticism precisely because it's anonymity by design makes it perfect for nefarious activity such as drugs markets. Privacy advocates in the space say that total unaccountability of money is a 'must have' feature and that critiques of the chain are in bad faith. It's actually arguably the best of the alternatives, having a valid use case in privacy.

- Solana is a far more centralised layer 1 proposition which uses a few hundred highly performant nodes to achieve high transaction throughput. The consensus algorithm is the novel "proof of history" system. Development of the technology has been funded and supported by huge venture capital investment, and even though the chain is quite unreliable it seems that the vested interests of the investors can keep interest going. It is cheaper, and more useful than Bitcoin and Ethereum, but lacks longevity and reliability. It could probably be a database. With that said it is well funded, and fun to use. They have announced a mobile stack and a first foray into making an android mobile phone to leverage it. This would, they say, allow a whole new model of mobile Web3 interaction.
- Polkadot is much hyped within the "crosschain" protocol community. These chains connect the logic of a smart contract on one chain to that of another. In practice, while it is possible that this is useful for distributed finance products, it seems that chains such as DOT might be promising more than the markets actually want or need. Governance of the token is a DAO like model where staking (locking up) the tokens theoretically controls the direction of the product. Crosschain products like this are a cybersecurity nightmare.
- TRON TRX draws extensive criticism for being founded by Justin Sun. A huge amount of value transacts on TRON, mainly thanks to the Tether stablecoin, and it could be argued that this gives it a genuine use case. It's more likely another house of cards.
- Tezos is a well established player with an early and somewhat battle tested proof

of stake mechanism and distributed governance model. It has attracted many high profile partnerships and sponsors, but is primarily seeking to be a store of value token like bitcoin, which exposes the chain to the "winner takes all" landscape of digital money. There are some compelling NFT advocates of the technology, which is certainly 'greener' and cheaper to use, but the longevity in such an irrational market is uncertain, because it does not seem to have the network effect and growth velocity.

- Algorand's ALGO token purports to be a more modern and useful proof of stake value transfer chain. It is fundamentally similar to Tezos.
- IOTA is noteworthy, interesting, and established concept, with an edge use case. It is a 'distributed ledger of the internet of things', the much hyped and clearly extant ecosystem of edge compute, sensors, smart devices etc. The marketing around IOTA correctly identifies it's positioning and potential within this developing technology ecosystem, but it's primary use case is too nascent and too niche, and the implementation itself has drawn (valid) criticism for amateurish cryptography and a fundamentally centralised model. The concept remains interesting.
- VeChain is a long established platform with 'significant' industry adoption which still doesn't represent it's market capitalisation, usefulness, or future success. It is the most exposed of all the chains to the untruth that immutable global ledgers, of real world assets, somehow protect from fraudulent behaviour. It's perhaps useful, but mainly in a highly automated industry 4.0 environment, with minimal human interaction.
- Cardano foundation ADA is one of the more established players and has been developing methodically and slowly. They have made great strides in successfully enabling a provable proof of stake consensus structure. Proof of stake non-the-less has significant problems in that tokens and therefore control inevitably concentrates over time. There is no proposed solution to this. They have working products and partnerships, but perhaps not as many as the market cap of the ecosystem would suggest.
- HBAR claims "third generation" blockchain technology, with carbon positive, high speed, distributed applications. There are always tradeoffs bound by physical constraints within distributed computing, and Hedera HBAR has been accused of a cryptographic model which is inherently insecure.
- EOS is one of the early major successes of the ICO funding model in 2017, and they amassed an enormous war chest of bitcoin which they still hold. The onus is on them to deliver some kind of product, and they have the funds to do so, but they probably won't.

3.10 Risks and mitigations

Looking across the whole sector, this paragraph from the Bank of International Settlement (BIS) sums everything up:

"...it is now becoming clear that crypto and DeFi have deeper structural limitations that prevent them from achieving the levels of efficiency, stability or integrity required for an adequate monetary system. In particular, the crypto universe lacks a nominal anchor, which it tries to import, imperfectly, through stablecoins. It is also prone to fragmentation, and its applications cannot scale without compromising security, as shown by their congestion

and exorbitant fees. Activity in this parallel system is, instead, sustained by the influx of speculative coin holders. Finally, there are serious concerns about the role of unregulated intermediaries in the system. As they are deep-seated, these structural shortcomings are unlikely to be amenable to technical fixes alone. This is because they reflect the inherent limitations of a decentralised system built on permissionless blockchains."

This might seem like reason enough to stop here and wait for proper digital currency (expanded later), but Bitcoin is here now, is likely unstoppable in, and with mitigations in place might have uses if developed properly. Perhaps surprising the same BIS is allowing up to 1% of bank reserves to be held in crypto assets, including Bitcoin, according to their June 2022 Basel Committee on Banking Supervision report.

Lightning is still considered to be experimental and not completely battle tested. There have been various attacks and a major double spend attack may be possible [66].

3.10.1 Digital assets

For digital assets more generally it is useful to look at the recent "whole government executive order" signed by President Biden. It is mainly framed in terms of "responsible innovation, and leadership" in the new space, is a product of multi agency collaboration, and has been long anticipated. It identifies high level risks, aspirations, and challenges, and strongly hints toward development of a "digital dollar" (CBDC, expanded later). The risks sections show how legislators are framing this, so it's useful to break down here.

- Consumer and business protections. This is likely to pertain to custodians and is much needed. Misselling is rife. Security presents a challenge.
- Systemic risk, and market integrity are a concern. The legislators clearly worry about contagion risks from the sector.
- Illicit finance (criminality and sanction busting etc) are a concern, but not particularly front and centre[67]. Criminality in 2021 was a mere 0.15% of transactions according to Chainalysis, but this number varies year to year. There are claims that Iran have begun official overseas buying with cryptocurrencies, but again, the numbers are small. The US treasury department has recently published a National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing. This is a comprehensive report and speaks to careful research across the space. It is broken into three parts. Perhaps surprisingly, while they do see activity in these areas, they do not rate the risk as very significant. Cash remains the main problem for illicit funding. There is some talk that the nature of public blockchain analysis allows greater oversight of these tools and that this is to the advantage of government and civil enforcement agencies.
- Highlighting the need for international coordination suggests they are mindful of jurisdictional arbitrage. The partial regulatory capture of these technologies, where activity flows to globally more lenient legislative regimes, continues to be a concern. Many of the centralised exchanges for instance are located in tax havens such as Malta. As the world catches up with these products it is likely that this will be smoothed out.
- Climate goals, diversity, equality and inclusion are mentioned. It seems that the "environment" aspect of ESG is more important then "social" and "governance" at this time.
- Privacy and human rights are mentioned.
- Energy policy is highlighted, including grid management and reliability, energy

efficiency incentives and standards, and sources of energy supply.

A recent proposed bi-partisan bill in the USA will likely lead global law in digital assets if it is passed in the next year or two. It encourages the use of Bitcoin as a medium of exchange by applying a tax exemption on transactions of less than $200. The issue of whether an asset is a commodity (a raw material thing) or a security (a promise) is left to a couple of major government agencies to unpick, with corresponding reporting requirements. Crucially for this book these nascent bills all regard both Bitcoin and Ethereum as sufficiently decentralised to qualify as commodities, meaning they would enjoy more lenient oversight. In this line of policy, exchanges will be required to do far more reporting, and would be penalised for trading against their customers. DOAs and DeFi are the big potential losers. In a maddening twist the Office of Government Ethics in the USA has banned anyone who owns digital assets from working on the legislation. This is an exceptional move and likely to result in poorly crafted laws in the first instance.

The most recent and troubling example is the US ban on any Ethereum assets which have been through a "mixer service" that obfuscates history. This is a huge constraint on the code and smart contract itself, not just sanctions against individuals. It has 'free speech' and constitutional implications [68]. More such actions and arrests of developers are feared. It has led to Circle (who issue the USDC stablecoin) blacklisting every address sanctioned by the US government. Centrally issued digital assets are obviously neither uncensorable nor permissionless. This intersects (again) with the whole question of what decentralisation means and how effective it can be in it's stated goal of circumventing global policies.

3.10.2 Bitcoin specifically

In addition it's useful for this document to focus more on the technical challenges to the Bitcoin network.

- The block reward is reduced every 4 years (epochs). This means a portion of the mining reward is trending to zero, and nobody knows what effect this will have on the incentives for securing the network through proof of work [69]. It is increasingly being discussed as the major eventual problem for the network.
- Stablecoins are a vital transitional technology (described later) but do not meaningfully exist yet on the Bitcoin network. This may change.
- Bitcoin lacks privacy by design. All transactions are publicly viewable. This is a major drag to the concept of BTC as a money. Upgrade of the network is possible, and has indeed been achieved for a Bitcoin fork called Litecoin [70].
- The Lightning network (described later) has terrible UX design at this time.
- The basic 'usability' of the network is still poor in the main. Any problems which users experience demand a steep learning curve and risk loss of funds. There is obviously no technical support number people can call.
- Only around one billion unspent transactions can be generated a year on the network. This means that it might become impossible for everyone on the planet to have their own Bitcoin address (with it's associated underpinning UTXO).
- Chip manufacture is concentrated in only a few companies and countries, as identified by Matthew Pines.
- Potential constraints on monetary policy flexibility.
- Future protocol changes.
- Unanticipated effects on the domestic and international energy system.

- Vulnerability to adversary attacks are widely studied, and still pretty much completely speculative because of the complex nature of the attack surface.
- Mining tends toward economy of scale concentration. Many are already on their own specialised network to connect to one another.
- Future hard forks. There will doubtless be pressure to fork the code to add inflation, or ESG mitigations, or to fix the UNIX clock issue in 2106. Each fork is a risk.
- Other unknown, unanticipated risks given Bitcoin's limited 13-year history.



4. Money in the real world

It is necessary here to briefly examine what money actually is in the world outside of metaverses, so we can understand it in the context of a virtual global space. In the previous section Bitcoin can be viewed in a couple of different lights. As a self custody digital bearer asset it can be viewed as 'property', like gold, i.e. not a liability on someone else's asset sheet. Indeed this has long been one of the assertions of the community and it finds favour in law, possible most ironically in China which of course banned mining. 'Money' though is a far more slippery concept to grasp. It seems very likely that Bitcoin is evolving as a "base money", and it's important to define that, but there are many other kinds of money within the online world which can potentially transfer value within virtual social spaces.

4.1 Defining money

Money is an economic good, that is generally accepted as a medium of exchange. This simple and specific description doesn't do justice to the complexity of everything that humans consider to be money. Even the Encyclopaedia Britannica strays from this immediately in their definition:

"money, a commodity accepted by general consent as a medium of economic exchange. It is the medium in which prices and values are expressed; as currency, it circulates anonymously from person to person and country to country, thus facilitating trade, and it is the principal measure of wealth.".

In which it can be seen that the principle measure of wealth might not be money at all, but rather property, credit, etc. So are these things money? Is a promise on a ledger money? The assertion at the top of this section is challenged by different schools of economic thinking. Global debt is around an order of magnitude larger than base money, and most wealth is stored in illiquid land/built environment (some $300T), and yet the system seems to work fine. The debt theory of money offered by anthropologist David Graeber suggests that money is an abstraction of barter, and thereby 'credit', but credit clearly pre-dates money, and needs no barter, commodity, intermediary nor underlying asset [71]. This suggests that money is something slightly different.

Money seems to have evolved for two principle purposes; trade outside of a village

context, and inheritance [72]. In doing this it somewhat replaced and augmenting 'credit', which as said above, was a promise between parties based on future actions, and likely as old as rudimentary language itself.

Money can be divided into two categories, which are fungible (interchangeable) from the point of view of the users. Base money is 'commodity' money which is backed by assets, or tangible physical (or digital) goods through the actions of a central bank ledger, and is around $30-$40T. Everything else is 'fiduciary media' [73].

All fiduciary money is credit but not all credit is fiduciary money. Nobody knows the extent of the global supply of fiduciary media. It encapsulates all the new digital money platforms like PayPal, gift cards, offshore accounts and all manner of other vehicles, and is thought to be many tens of trillions of pounds. This somewhat muddies the waters since money that is backed by 'something' blends away into money which cannot reasonably be assayed. This in turn undermines the assertion that money is backed. It seems that a combination of available raw materials and labour, central banks and their associated political structures [74], and global markets drive the value of money up and down relative to "stuff" in the shops. This manifests as 'inflation', which is 'possibly' the effect of not pegging money to an asset such as silver, or gold as in the past [75]. While the gross drivers of inflation seems to be accepted and understood, nobody seems very sure how the various aspects interact.

All this makes it hard to find a universally accepted and explicable definition of money. The best approach may be to look at the properties of a thing which is asserted to be a money. In his book 'A history of money', Glyn Davies identifies "cognisability, utility, portability, divisibility, indestructibility, stability of value, and homogeneity" [76].

Stroukal examines Bitcoins' likely value as a money from an Austrian economics perspective and identifies "portability, storability, divisibility, recognizability, homogeneity and scarcity" [77].

A helpfully brief and useful web page by Desjardins from 2015 describes some properties and explains them in layman's terms below:

- Divisible: Can be divided into smaller units of value.
- Fungible: One unit is viewed as interchangeable with another.
- Portable: Individuals can carry money with them and transfer it to others.
- Durable: An item must be able to withstand being used repeatedly.
- Acceptable: Everyone must be able to use the money for transactions.
- Uniform: All versions of the same denomination must have the same purchasing power.
- Limited in Supply: The supply of money in circulation ensures values remain relatively constant.

4.1.1 Global currency interactions

The legacy moniker "third world" came from a division of the world along economic lines [78]. At the time this was the petrodollar / neo-institutional hegemony [79, 80], vs the economic superpower of the soviet block, and then 'the rest'; unaligned economic powers.

This old framework has fallen away with the associated terminology, but it's useful to look at what money 'is' from a global viewpoint, because all money is effectively trust in the liability held by some defined counter party.

Right now the dollar system is still predominant, but it seems likely that there are new axes forming, especially around the Chinese Yuan. It's clear that central banks have been

aware of this potential transition away from a global dollar / energy system. The Dollar has potentially suffered from the radical expansion of the money supply over the last 70 years or so under the private "Eurodollar" system [81]. Some policy makers have been looking back to the great economist John Maynard Keynes' ideas for a neutral basket of assets as a global synthetic hedgemonic currency [82, 83] which would almost certainly consist partly of gold [84].

Use of the dollar system has recently been shown more and more to be contingent on adherence to US defined political principles. This is evidenced most starkly by the seizure of Russian central bank foreign reserves, a new and untried projection of monetary power.

The Chinese Yuan/Renminbi is potentially stepping in where the petrodollar is now waning [85]. The effects of this expansion of economic influence by China, through a potential petro-Yuan, and the belt and road initiative [86], are not yet felt, but the lines are fairly clearly defined. The Euro system is potentially more stable, and less 'weaponised' but comes with it's own restrictions for use, especially through the International Monetary Fund (IMF). It is notable for instance that the IMF have included a clause in their negotiations with Argentina to 'discourage' the use of crypto based money, leading to a complete ban on banks offering the products only days after they began. This is likely a response to the adoption of Bitcoin by El Salvador, something with which the IMF is very uncomfortable. They are also wary of the ability of nation states to monetise their energy reserves without the need for export markets. They do however concede that CBDCs and 'some' crypto assets may be more energy efficient than traditional systems. It seems to industry insiders that they are learning in public.

The new 'third world' who are excluded from the Dollar and/or Yuan poles of the global economy might drift toward the 'basket of assets' discussed by Keynes and Carney above. As mentioned this will certainly have a component of gold, and likely other commodity assets such as rare metals. For our purposes here it's also possible that there would be a small 'hedge' allocation of Bitcoin or even a global axis of 'unaligned' nations using the asset [87]. Block and Wakefield research found that in developed nations Bitcoin is treated as in investment, while in less wealthy demographics there is interest in the utility. This is evidenced in the early nation state adoption seen and described to date, and the game theory incentive explained by Fidelity in the introduction. It's too early to tell if this 'unaligned money' could constitute a global economic pole, but it's interesting that some commentators are now even discussing this, and that carbon neutrality research is being undertaken specifically for this application.

4.2 International money transfer networks

Transferring money from one financial jurisdiction to another is itself a global marketplace which has accreted over the entire course of human history. It's far less useful here to discuss the mythos of salt and seashells as a mechanisms of international remittance and taxation [88, 89]. Suffice it to say that there are dozens, if not hundreds, of cross border payment companies who make their business from taking a percentage cut of an international money transfer. There are also hundreds if not thousands of banks who offer this service as part of their core business portfolio. This section looks at some of the major players, and their mechanism, to contextualise the more recent shifts brought about by technology.

4.2.1 Swift, ISO 20022, and correspondence banking

Society for Worldwide Interbank Financial Communiactions (SWIFT) was initially formed in 1973 between 239 banks across 15 countries. They needed a way to improve handling of cross border payments. It is now the global standard for financial message exchange in over 200 countries, and has recently found itself under a fresh spotlight, during the invasion of Ukraine. The system handles around 40 million short, secure, code transmissions a day, which represent crucial data about a transaction and the parties involved. It is used by both banks and major financial institutions to speed up settlement between themselves, on behalf of the clients and customers. It replaced the Telex (wire transfer) system. The new proposed and incoming standard to replace SWIFT is ISO20022 which is a complex and data rich arrangement. To be clear the SWIFT consortium are promoting this new standard to their 11,000 plus global user base, and there is significant investment and hype from major financial players, but it seems unclear what the actual take-up will or even should be. A group of 'crytocurrencies' are heavily involved in the ISO20022 standard, and there's been experimentation with private permissioned distributed ledger technologies. It's actually somewhat unclear what value they bring, and possible that the relationship of these public ledgers to international bank to bank messaging is a marketing distraction. Note that SWIFT, ISO20022, and the associated tokens within crypto are all themselves products which have a business model. They are all intermediaries which will demand a mediating fee somewhere. All of this proposed functionality could be replaced by central bank digital currencies, which will be discussed later in the section.

4.2.2 VISA etc

VISA have announced a "crypto business to business support unit".

4.2.3 Money transfer operators

International Money Transfer Operators analysis

western union etc, moneygram, transferwise,

4.2.4 Digital disruptive fintech

It seems that the neobank providers of digital banking apps are likely to converge with native digital asset "wallets". This is also the thesis advanced by the Ark intestments Big Ideas paper.

CNN have a useful primer of the most prevalent mobile digital payment methods. This can be seen in Figure 4.1. This comparison makes it pretty clear that Bitcoin is not ready as a personal mobile payment system. That's not to say that there isn't a place for the underlying technology in global payment processing. The most interesting example of this is Strike, a product in the international fintech arena. It is a 'global' money transmitter which uses bank connections in local currencies, but a private version of the Lightning network with settlement on the Bitcoin main chain. In practice users connect the app to their bank and can send money to the bank connected Strike app of another user instantly, and without a fee. This is a far better product than those previously available. In principle it's open API allows many more applications to be integrated into the Strike back end. Twitter already uses this for international tipping (and remittance). It seems that this is a perfect contender for supporting transactions in open metaverse applications, and that may be true, but Strike is currently only available in three countries (USA, El Salvador,



Figure 4.1: Comparison of mobile based payment systems

Argentina).

Paypal, xoom, Strike, servicing smaller payments, cashapp, venmo, revulot,

4.2.5 Stablecoins

Stablecoins are 'crypto like' instruments which are 'pegged' at a 1:1 ratio with nationally issued Fiat currencies. In fact they usually correspond to units of privately issued debt underwritten by a variety of different assets. This is (depending on the issuing company's model) a far more risky unit of money than the nominal currency that they represent, but they offer significant utility. They allow the user to self custody the cryptographic bearer instrument representing the money themselves, as with blockchain. This may afford the user less friction in that they can transmit the instrument through the newer financial rails which are emerging. Once again, this is likely a product most useful to emerging markets, those living under oppressive regimes, currencies suffering from high inflation, and countries who rely on the dollar as their currency, and within digitally native metaverse applications. These are *enormous* global uses though. The use in the west is prominently for 'traders' on exchanges at this time. /par The caveat of such products is that such 'units' of money can be frozen by the issuer, and they are subject to the third party risk of the issuer defaulting on the underlying instrument, instantly wiping out the value.

Klages-Mundt et al. wrote a paper in 2020, which explains the details of the different mechanisms and risks.

The following text paraphrases Spencer noon of on-chain analytics company "Our-Network", who provides an useful summary of the paper. *There are two major classes of stablecoins:*

- *Custodial: entrusted by off-chain collateral assets like fiat dollars that sit in a bank. Requires trust in third party.*
- *Non-custodial (aka decentralized): fully on-chain and backed by smart contracts & economics. No trusted parties.*

In custodial stablecoins, custodians hold a combination of assets (currencies, bonds, commodities, etc.) off-chain, allowing issuers (possibly the same entity) to offer digital tokens of an reserve asset. The top 2 custodial stablecoins today are USDT and USDC. There are 3 types of custodial stablecoins.

- *Reserve Fund: 100% reserve ratio. Each stablecoin is backed by a unit of the reserve asset held by the custodian. A useful example of this the USDF banking consortium.*
- *Fractional Reserve Fund: The stablecoin is backed by a mix of both reserve assets and other capital assets.*
- *Central Bank Digital Currency (CBDC): A digital form of central bank money that is widely available to the general public. CBDCs are in their nascency as today only 9 countries/territories have launched them, many of them small.*

Custodial stablecoins have three major risks:

- *Counterparty Risk (fraud, theft, govt seizure, etc.)*
- *Censorship Risk (operations blocked by regulators, etc.)*
- *Economic Risk (off-chain assets go down in value)*

Each can result in the stablecoin value going to zero.

It's worth taking a look at these tokens individually, to get a feel for the trade-offs, and figure out how they might be useful for us in our proposed metaverse applications. It's important to know that these tokenised dollars and/or other currencies are issued on top of the public blockchains we have been detailing throughout. Which tokens are on

what blockchains is constantly evolving, so it's not really worth enumerating specifics. In a metaverse application it would be necessary to manage both the underlying public blockchain and the stablecoin issued on top of it, making the interaction with the global financial system perversely more not less complex. In the following list of a few of the major coins, the first hyperlink is the whitepaper if it's available.

- Tether is the largest of the stablecoins, with some $70B in circulation, and the third largest 'crypto'. This has been a meteoric rise, attracting the ire and scrutiny of regulators and investigators. There is considerable doubt that Tether has sufficient assets backing their synthetic dollars, but the market seems not to mind. It's resilience against 'bank runs' was tested in May 2022 when $9B was redeemed directly for dollars in a few days following the UST crash (more on this later), and they have been shoring up their position since by reducing exposure and size. It might be that the market comes to see this event as a validation of the asset. They are shortly to launch a GBP version for the UK. It's an important technology for this metaverse conversation because of intersections with Bitcoin through the Lightning network. Tether might actually provide everything needed. It's only as safe as the trust invested in the central issuer though.
- Binance USD is the dollar equivalent token from global crypto exchange behemoth Binance. It's released in partnership with Paxos, who have a strong record for compliance, and transparency. Paxos also offer USDP. Both these stablecoins claim to be 100% backed by dollars, or US treasuries. They are regulated under the more restrictive New York state financial services and have a monthly attestation report.
- MakerDAO Dai is an Ethereum based stablecoin and one of the older offerings. It's been 'governed' by a DAO since 2014. 'Excess collateral', above the value of the dai-dollars to be minted, is voted upon before being committed to the systems' cryptographic 'vaults' as a backing for the currency. These dai can then be used across the Ethereum network. Despite the problems with DAOs, and the problems with Ethereum, DAI is well liked by its community of users and has a healthy billion dollars of issuance. They may be dangerously exposed to the new crackdown in the USA, and there is internal talk of pro-actively abandoning DAI altogether.
- TrueUSD claims to be fully backed by US dollars, held in escrow. It runs on the Ethereum blockchain. They have attestation reports available on demand and claim fully insured deposits. It's not quite that simple in that a portion of the backing is 'cash equivalents'.
- Gemini GUSD claim reserves are "held and maintained at State Street Bank and Trust Company and within a money market fund managed by Goldman Sachs Asset Management, invested only in U.S. Treasury obligations." which seems pretty clear.
- TerraUSD (UST) **was** a newer and more experimental stablecoin, and one of a set of currency representations within the network. It worked in concert with the LUNA token on the Cosmos blockchain in order to keep it's dollar stability. It was not backed in the same way as the other tokens, instead relying on an arbitrage mechanism using LUNA. In essence the protocol paid users to destroy LUNA and mint UST when the price was above one dollar, and vice versa. This theoretically maintained the dollar peg. There was much concern that this model of 'algorithmic stable coin' is unstable [90]. The developers of the Terra tried to address this concern by buying enormous amounts of Bitcoin, which they quickly had to employ to address UST drifting downward from $1. This failed to address the 'great depegging', with

LUNA crashing to essentially zero, destroying some $50B of capital. It will now likely act as a cautionary tale to other institutions considering Bitcoin as a 'reserve asset'. An earlier version of this book highlighted the specific variation of the risk which quickly manifested.

- USDC is a dollar backed coin issued by a consortium of major players in the space, most notably Circle, and Coinbase. It's has a better transparency record than tether but is still not backed 1:1 by actual dollars in reserve. It may or may not be a fractional reserve asset. It's well positioned to take advantage of regulatory changes in the USA, and seems to be quietly lobbying to be the choice of a government endorsed digital dollar, at least a significant part of a central bank digital currency initiative. It's too early to tell how this will work out, but it has substantial 'legacy finance backing'. It is the only stablecoin to increase slightly in value (depegging upward) in the wake of the UST implosion. This 'flight to quality' shows the advantage of the work that CENTRE put into regulatory compliance. If our metaverse were to pick a stablecoin to work with it would be USDC. It runs on Ethereum, Algorand, Solana, Stellar, Tron, Hedera, Avalanche and Flow blockchains.

.

4.2.5.1 The evolving US position

In most regards the legislative front line is happening in the USA. Treasury Secretary Yellen responded to the collapse of Terra/UST saying that: *"A comprehensive regulatory framework for US dollar stablecoins is needed"*. She also said that the stablecoin market is too small to pose systemic risk at this time. This is clearly an evolving situation, but the incredible consumer exposure to these risky products is likely to elicit a swift and significant response, and the timing seems right for intervention. The markets suggest that USDC will be the eventual winner.

Koning meanwhile has looked into the different regulatory approaches used by various stablecoins.

- The highly regulated New York state financial framework (Paxos, Gemini)
- Piggyback off of a (Nevada) state-chartered trust [TrueUSD, HUSD]
- Get dozens of money transmitter licenses [USDC]
- Stay offshore [Tether]

New legislation specific to the concept of stablecoins is now entering the system under Sen Toomey. There are many provisions in the bill, mostly pertaining to convertibility and the ever present problem of attestation of the 'backing' of these products. Mention has already been made of the major bill advanced by Sen. Lummis and Gillibrand. This bill also includes significant provision around stablecoins. Lummis said *"Stablecoins will have to be either FDIC insured or more than 100% backed by hard assets."*. This is good news for this section of the digital asssets space.

Crucially there is also more clarity on privacy. This is a huge threat from digital money systems, and the USA is likely to lead. Remember though that none of this is yet law.

Valkenburg, the lead researcher of a US think tank in digital assets says the following: *"Stablecoin TRUST Act, is a discussion draft mostly about stablecoins, but it also has important privacy protections for crypto users broadly: it puts real limits on warrantless surveillance by narrowing what info can be collected from third parties. Last summer we fought a provision in the infrastructure bill that damaged the privacy of crypto users by expanding the broker definition (who needs to report information about transactions to*

22 Digital settlement assets: power to make regulations

(1) The Treasury may by regulations make such provision as they consider appropriate for the purpose of, or in connection with—

(a) the regulation of payments that include digital settlement assets,

(b) the regulation of—

(i) recognised payment systems that include arrangements using digital settlement assets,

(ii) recognised DSA service providers, and

(iii) service providers connected with, or in relation to, the systems and providers mentioned in sub-paragraphs (i) and (ii),

as those terms are for the time being defined in Part 5 of the Banking Act 2009, and

(c) making insolvency arrangements (including administration, restructuring and any similar procedure) in respect of the systems and providers mentioned in paragraph (b).

(2) In this section, "digital settlement asset" means a digital representation of value or rights, whether or not cryptographically secured, that—

(a) can be used for the settlement of payment obligations,

(b) can be transferred, stored or traded electronically, and

(c) uses technology supporting the recording or storage of data (which may include distributed ledger technology).

Figure 4.2: The UK signs into law regulation of digital representatives of value

the IRS) & crypto 6050I reporting (reports on business transactions over $10,000). The winter before we fought and successfully delayed a rushed proposal from the outgoing Trump administration to mandate that exchanges collect information about persons who are not their customers, who hold crypto at addresses in wallets they control directly. the Stablecoin TRUST Act would stop these encroachments, constrain the treasury from collecting any nonpublic information unless they get a search warrant or collect only information voluntarily provided to an exchange by a customer and for a legitimate business purpose. If "voluntarily provided for a legitimate business purpose" sounds familiar to you, that's b/c it's the constitutional standard articulated by the Court in Carpenter describing LIMITED circumstances where warrantless searches of customer data are ok.It's the standard we've advocated must also limit warrantless data collection at crypto exchanges. If exchanges must collect information about non-customers, that information is, by definition, not voluntarily provided for a legitimate business purpose."

4.2.5.2 The evolving UK position

As mentioned briefly in the introduction the UK has recently signalled an enthusiasm for stablecoins as "means of payment". This is a stark reversal of their previous legislative momentum is possibly a response to the tightening of rhetoric in Europe around such assets. The Financial Services and Markets Bill. became law in July 2022. An excerpt pertaining to stablecoins can be seen in Figure 4.2.

The U.K. Financial Conduct Authority's chief executive, Nikhil Rathi, outlined the FCA's regulatory goals at the Peterson Institute for International Economics: *"The U.S. and U.K. will deepen ties on crypto-asset regulation and market developments — including in relation to stablecoins and the exploration of central bank digital currencies."*

The timing seems right to explore the use of stablecoins in metaverse applications up the list of choices.

4.2.5.3 Stables in metaverse applications

It makes a **lot** of sense to consider stablecoin transfer as the money in metaverses. USDC is furthest along this possible adoption curve. Their partnership with global payment provider Stripe has enabled global dollar transfer within Twitter for users of their 'Connect' platform. This leverages the Polygon chain (mentioned in the blockchain chapter). Many digital wallets can be connected from the user end, with Metamask potentially being the easiest to integrate. This has also been mentioned in the book. The downside of this for our open platform is that none of these elements are particularly open, or distributed, and the users of the platform will still need to use an exchange to get the USDC to spend. This approach makes it easier for the vendors and product providers in the metaverse applications to accept USDC, but everything else is actually harder.

4.3 Central bank digital currencies

If 2021 was the year of the stablecoin then 2022 is likely to be the year of the central bank digital currency (CBDC). CBDCs would likely not exist without the 2019 catalyst of Facebook Libre crypto currency project, which is now cancelled and defunct, pressure exerted on central banks by the concept of Bitcoin, and the stablecoins which emerged from the technology.

It now seems plausible that the world is moving toward a plurality of national and private digital currencies. Figure 4.3 from the Bank for International Settlement, shows the growing acceptance within central banks. Their 2022 annual economic report dedicates a 42 page chapter to the subject. Hyun Song Shin, head of research at BIS said *"Our broad conclusion is captured in the motto, 'Anything that crypto can do, CBDCs can do better."*

This text from the thinktank VoxEU highlights the pressure on not to be 'left behind':
"Given the rapid pace of innovations in payments technology and the proliferation of virtual currencies such as bitcoin and ethereum, it might not be prudent for central banks to be passive in their approach to CBDC. If the central bank does not produce any form of digital currency, there is a risk that it loses monetary control, with greater potential for severe economic downturns. With this in mind, central banks are moving expeditiously when they consider the adoption of CBDC."

CBDCs are wholly digital representations of national currencies, and as such are centralised database entries, endorsed and potentially issued by national governments. The USA's whitepaper shows the approach. Curiously only The Bahamas seem to have a successful implementation, but it is a rapidly evolving space, and many nations are now scrambling to catch up.

The following text is taken from the March 2021 Biden government "executive order" on digital assets, and defines the current global legislative position well.
"Sec. 4. Policy and Actions Related to United States Central Bank Digital Currencies. (a) The policy of my Administration on a United States CBDC is as follows:
(i) Sovereign money is at the core of a well-functioning financial system, macroeconomic stabilization policies, and economic growth. My Administration places the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC. These efforts should include assessments of possible benefits and risks for consumers, investors, and businesses; financial stability and systemic risk; payment systems; national security; the ability to exercise human rights; financial inclusion and equity; and the actions required to launch a United States CBDC if doing so is deemed

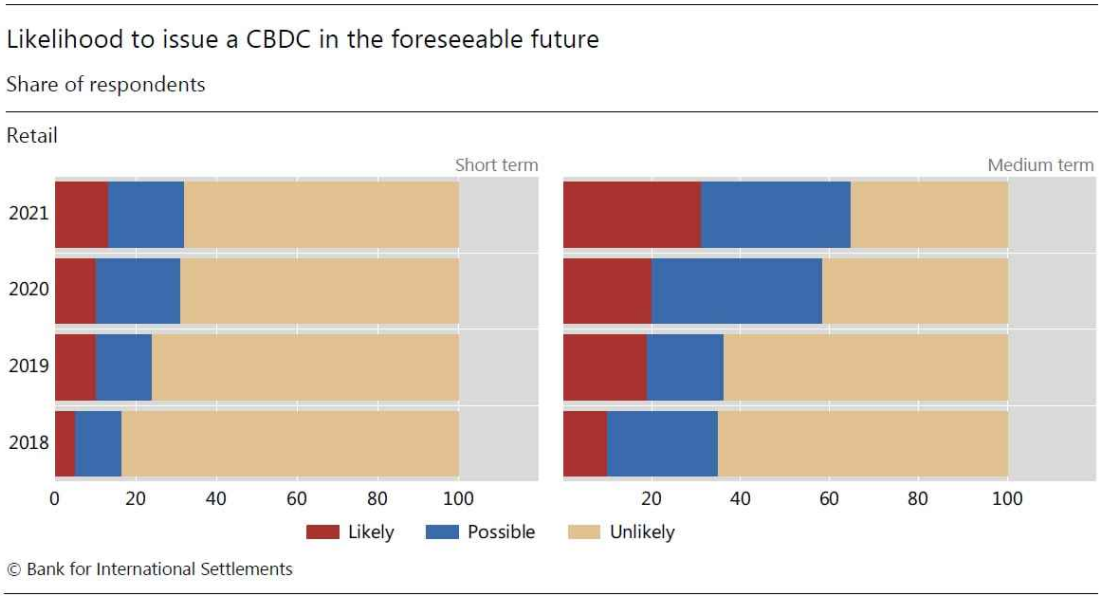


Figure 4.3: More than half of central banks surveyed by the BIS said they saw issuance of a CBDC as possible.

to be in the national interest.
(ii) My Administration sees merit in showcasing United States leadership and participation in international fora related to CBDCs and in multi-country conversations and pilot projects involving CBDCs. Any future dollar payment system should be designed in a way that is consistent with United States priorities (as outlined in section 4(a)(i) of this order) and democratic values, including privacy protections, and that ensures the global financial system has appropriate transparency, connectivity, and platform and architecture interoperability or transferability, as appropriate.
(iii) A United States CBDC may have the potential to support efficient and low-cost transactions, particularly for cross-border funds transfers and payments, and to foster greater access to the financial system, with fewer of the risks posed by private sector-administered digital assets. A United States CBDC that is interoperable with CBDCs issued by other monetary authorities could facilitate faster and lower-cost cross-border payments and potentially boost economic growth, support the continued centrality of the United States within the international financial system, and help to protect the unique role that the dollar plays in global finance. There are also, however, potential risks and downsides to consider. We should prioritize timely assessments of potential benefits and risks under various designs to ensure that the United States remains a leader in the international financial system."

In traditional nation state currencies the central banks control the amount of currency in circulation by issuing debt to private banks, which is then loaned out to individuals [91]. The debt is 'destroyed' on the balance sheet to remove currency through the reverse mechanism. They also facilitate government debt [92], and work (theoretically) outside of political control to adjust interest rates, in order to manage growth and flows of money.

It is somewhat surprising that Powell, chair of the US Federal Reserve has recently said *"Rapid changes are taking place in the global monetary system that may affect the international role of the dollar. A US central bank digital currency is being examined to*

help the US dollar's international standing.". This is a rapid evolution of the narrative, with implications. It seems unlikely that the world would sacrifice the traditional banking system in favour of centrally controlled money, but many things which cannot be done with traditional nation state money systems are possible with CBDCs, because they remove the middleman of private banking between the end user and the policy makers.

- Negative interest rates are possible, such that all of the money can lose purchasing power over time, and at a rate dictated by policy. This "removal of the lower bound" has been discussed by economists over the last couple of decades as interest rate mechanisms have waned in efficacy. It is not possible in the current system, and instead money must be added through quantitative easing, which disproportionately benefits some though Cantillon effects [93, 94].
- Ubiquitous basic income is possible in that money can be issued directly from government to all approved citizens, transferring spending power directly from the government to the people. This also implies efficiency savings for social support mechanisms.
- Asset freezing and confiscation are trivial if CBDCs can replace paper cash money completely, as a bearer asset. Criminals and global 'bad actors' could have their assets temporarily or permanently removed, centrally, by suspending the transferability of the digital tokens.
- Targeted bailouts for vital institutions and industries are possible directly from central government policy makers. Currently private banks must be incentivised to make cheap loans available to sectors which require targeted assistance.
- Financial surveillance of every user is possible. In this way a 'panopticon of money' can be enacted, and spending rulesets can be applied. For instance, social support money might only be spendable on food, and child support only on goods and services to support childcare. This is a very dystopian set of ideas. Eswar Prasad says "In authoritarian societies, central bank money in digital form could become an additional instrument of government control over citizens rather than just a convenient, safe, and stable medium of exchange." [95]
- It's a virtually cost free medium of exchange, since there is no physical instrument which must be shipped, guarded, counted, assayed, and securely destroyed.
- The counterfeiting risk is significantly reduced because of secure cryptographic underpinnings rather than paper or plastic anti counterfeiting technologies.
- Global reach and control is instantly possible for the issuer. This is a big problem especially for a reserve currency such as the dollar. Two thirds of $100 bills are thought to reside outside of the USA.
- System level quantitative easing and credit subsidies are made far simpler and less wasteful when centrally dictated.
- Transfer of liability and risk to the holder globally reduces the management costs for global deposits of a currency.
- It may be possible to automate the stability of a currency through continuous adjustment of the 'peg' through algorithms or AI.

The UK has signalled that it is not interested in developing a CBDC at this time. It is viewed as a solution in search of a problem, with the Lords economic affairs committee saying:*"The introduction of a UK CBDC would have far-reaching consequences for households, businesses, and the monetary system for decades to come and may pose significant risks depending on how it is designed. These risks include state surveillance of*

people's spending choices, financial instability as people convert bank deposits to CBDC during periods of economic stress, an increase in central bank power without sufficient scrutiny, and the creation of a centralised point of failure that would be a target for hostile nation state or criminal actors."

Meanwhile in Europe, ECB President Christine Legarde said: *"On your question concerning CBDC, you know my views on CBDC and you know that I have pushed that project. Fabio Panetta is working hard on that together with members in the entire Eurosystem with the high-level taskforce that is working really hard on moving forward. But in a way, I am really pleased that attention is now focussed on the role that cryptos can play and the role that Central Bank Digital Currency can have when they are implemented. We have a schedule, as you know. The Governing Council decided back in October '21 to launch a two-year investigation phase, and it is at the end of that investigation phase that the decision will definitely be made to launch the CBDCs and to make it a reality. We can't go wrong with that project. I am confident that we will move ahead, but that's going to be a decision of the Governing Council. I think it's an imperative to respond to what the Europeans expect, and I think we have to be a little bit ahead of the curve if we can on that front. If we can accelerate the work, I hope we can accelerate the work. I will certainly support that and I was delighted to see that in the United States there was an executive order by President Biden to actually expect similar effort and focus and progress on CBDC, cryptos. I think that it will take all the goodwill of those who want to support sovereignty, who want to make sure that monetary policy can be transmitted properly using our currency, will endeavour."*

In the USA this text from Congressman Tom Emmer shows how complex and interesting this debate is becoming.*"Today, I introduced a bill prohibiting the Fed from issuing a central bank digital currency directly to individuals. Here's why it matters: As other countries, like China, develop CBDCs that fundamentally omit the benefits and protections of cash, it is more important than ever to ensure the United States' digital currency policy protects financial privacy, maintains the dollar's dominance, and cultivates innovation.*
CBDCs that fail to adhere to these three basic principles could enable an entity like the Federal Reserve to mobilize itself into a retail bank, collect personally identifiable information on users, and track their transactions indefinitely.
Not only does this CBDC model raise "single point of failure" issues, leaving Americans' financial information vulnerable to attack, but it could be used as a surveillance tool that Americans should never be forced to tolerate from their own government.
Requiring users to open an account at the Fed to access a United States CBDC would put the Fed on an insidious path akin to China's digital authoritarianism.
Any CBDC implemented by the Fed must be open, permissionless, and private. This means that any digital dollar must be accessible to all, transact on a blockchain that is transparent to all, and maintain the privacy elements of cash.
In order to maintain the dollar's status as the world's reserve currency in a digital age, it is important that the United States lead with a posture that prioritizes innovation and does not aim to compete with the private sector.
Simply put, we must prioritize blockchain technology with American characteristics, rather than mimic China's digital authoritarianism out of fear."

Most analysts now seem to think that there is little appetite to replace all of a given currency with a CBDC. Most significantly such products would need the support of retail banks, and it is not in their interest to service such a product. Their business model relies on

using retail deposits for yield generation, and it is these deposits, not cash itself that would be the most addressable market for a CDBC. Banks don't want people to self custody money. It is far more likely that a blend of stablecoins, private bank issued digital currency (with a yield incentive) and some limited CBDC, alongside the new contender Bitcoin, will present a new landscape of user choice. Different models of trust, insurance, yields, acceptability, and potentially privacy, will emerge.

Clearly a global, stable, wholly digital bearer asset in a native currency would be the ideal integration for money in a metaverse application, but it is likely that a transition to such a technology would be complex and painful. It is certainly not ready for consideration now.

4.4 Bitcoin as a money

Nwosu, cofounder of Coinfloor exchange in the UK, and cofounder of the aforementioned Fedimint and says that a digital money needs the following four characteristics:

- that it be technically mature. Nwosu does not see Ethereum as demonstrating this for instance due to it's change to proof of stake. This is the same reasoning outlined in the blockchain section of this book.
- it should have strong community support and network effect. We have seen that this is more simply a feature of money itself.
- that there should be regulatory clarity around the asset, a feature which even Bitcoin currently struggles with.
- it should demonstrate a core use case of 'store of value' which sounds simple enough, but again is contestable because of the volatility of Bitcoin.

4.4.1 Spending it

Since this book seeks to examine transfer of value within a purely digital environment it is necessary to ask the question of whether Bitcoin is money. This short 'story', purportedly written by Nakamoto, is a fabulous look at the money values of the technology, irrespective if it's provenance. In it is the following text: *"Here, for once, was this idea that you could generate your own form of money. That's the primary and sole reason, is because it was related to this thing called money. It wasn't about the proficiency of the code or the novelty, it was because it had to do with money. It centered around money. That is something people cared about. After all, plenty of projects on Sourceforge at the time were just as well coded, well maintained, if not better, by teams, and even if someone else had created the blockchain before me, had it been used for something else beyond currency, it probably would not have had much of an outcome.*

Again, irrespective of the author here, this point seems to ring true. The memetic power of Bitcoin is in it's proximity to 'money', and the potential of the separation of money from the state.

It is beyond argument that the Bitcoin network is a rugged message passing protocol which achieves a high degree of consensus about the entries on it's distributed database.

Ascribing monetary value to those database entries is a social consensus problem, and this itself is a contested topic. The most useful 'hot take' here is that Bitcoin behaves most like a 'property', while it's network behaves far more like a monetary network which is created and supported by the value of the Bitcoin tokens.

Jack Mallers, of Strike presentation to the IMF identified the following challenges

which he claims are solved by the bitcoin monetary network.

- Speed
- Limited transparency and dependability
- High cost
- Lack of interoperability
- Limited Coverage
- Limited accessibility

He further identifies the attributes of the ideal global money.

- Uncensorable
- Unfreezable
- Permissionless
- Borderless
- Liquid
- Digital

Mallers has recently announced USA focused partnerships which leverage his Strike product to enable spending Bitcoin, through Lightning, as Dollars in much of the point of sale infrastructure in the USA. This is a huge advance as it immediately enables the vendors both online and at physical locations to either save 3% costs for card processors, or else pass this on as a discount. Crucially for 'Bitcoin as a money' it also allows the vendors to receive the payment **as** Bitcoin, not Dollars. A possible further and highly significant feature is that it might now be possible to divest of Bitcoin in the USA, buying goods, without a capital gains tax implication. Mallers claims to have legislative backing for this product, but the devil will likely be in the detail. The likely mechanism for this product is that the EPOS partner sends a Lighting request to Strike, which liquidates some of their Bitcoin holding to a dollar denominated stablecoin, but in a tax free jurisdiction such as El Salvador. This stablecoin will then be sent to the EPOS handing partner such as NCR. Stablecoin to Dollar transactions in the USA are much murkier and likely don't cost anything for these companies. This agent will then authorise the Dollar denominated sale to the American digital till. Crucially nobody has a US capital gains tax exposure in this chain, and all of the settlements were near free, and instantaneous, with 'cash finality' for everyone except the EPOS company. They are likely actually exposed to a small risk here because uptake will be very low level. The novelty opportunity will likely cover any potential exposure to stablecoin collapse. This is a radical upgrade on the normal flow of divesting Bitcoin for American users.

Using this open product to spend Bitcoin as Bitcoin to vendors might be available through Shopify globally. Again, it's too new to be sure. Promisingly a Deloitte study has found that 93% of businesses accepting Bitcoin have seen revenue and brand perception improve, and 75% of USA sales execs plan to accept digital assets at some point in the next 2 years. This ambition in the US markets is likely to benefit from the proposed $200 tax exempt law for purchasing goods and services with Bitcoin.

Of these recent developments in Lightning Lyn Alden says: *Some people naturally dismiss [strike] because they don't want to spend their BTC; they want to save it. However, the more places that accepted BTC at point of sale (on-chain or Lightning or otherwise), the more permissionless the whole network is. This is because, if all you can do with BTC is convert it back into fiat on a major exchange, then it's easy to isolate it, effectively blacklist addresses, etc. But if you can directly spend it on goods and services across companies and jurisdictions, it's harder to isolate. There are now plenty of vendors that*

make this easy for merchants to implement, and the merchant can still receive dollars if they want (rather than BTC), or can decide their % split. Since it's an open network, anyone can build on it, globally. And then when you add fiat-to-BTC-to-fiat payments over Lightning, it gets even more interesting because it doesn't necessarily need to be a taxable event. Lightning wallets with a BTC balance and a USD/stablecoin balance. Lower fees than Visa and others.

More interestingly for metaverse applications Mallers has opened this section of the company to interact with the public Lightning network, allowing people with a self hosted wallet or node to pay directly for goods across America, settling immediately in Dollars, using their Bitcoin, at zero cost. **This opens the possibility to buy from US based (Dollar denominated) metaverse stores, using the capabilities of the stack assembled at the end of the book**. The implications globally are unclear at this time.

4.4.2 Saving with it

The Bitcoin community believes that Bitcoin is the ultimate money, a 'store of value', chance to separate money from state, increase equality of opportunity and ubiquity of access, while others view it as 'rat poison', or a fraudulent Ponzi scheme [96]. A notable exclusion from the negative rhetoric is Fidelity, the global investment manager, who have always been positive and have recently said: *"Bitcoin is best understood as a monetary good, and one of the primary investment theses for bitcoin is as the store of value asset in an increasingly digital world."*

The following paraphrases Eric Yakes, author of 'The 7th Property'. Again, this is an Austrian economics perspective, and like much economic theory the underlying premise is contested[97]: *"Paper became money because it was superior to gold in terms of divisibility and portability BUT it lacked scarcity. People reasoned that we could benefit from the greater divisibility/portability of paper money as long as it was redeemable in a form of money that was scarce. This is when money needed to be "backed" by something.*
Since we changed money to paper money that wasn't scarce, it needed to be backed by something that was. Since the repeal of the gold standard, politicians have retarded the meaning of the word because our money is no longer backed by something scarce.
So, what is bitcoin backed by? Nothing.
Sound money, like gold, isn't "backed". Only money that lacks inherent monetary properties must be backed by another money that maintains those properties. The idea that our base layer money needs to be backed by something is thinking from the era of paper money. Bitcoin does not require backing, it has inherent monetary properties superior to any other form of money that has ever existed."

The 2022 ARK Big Ideas report again provides some useful market insight. They posit that demand for the money features of Bitcoin could drive the price of the capped supply tokens to around 1M pounds per Bitcoin as in Figure 4.4. Take this with the usual pinch of salt, as Ark have been performing notably badly lately with their predictions. Perhaps more than any of these takes, it is worth considering the current public perception of the technology as a money and store of value. This twitter thread from professional sportsman Saquon Barkley, to his half million followers on the platform, captures the mood. He is one of a handful of athletes now being paid directly in Bitcoin.

"I want my career earnings to last generations. The average NFL career is 3 years and inflation is real. Saving and preserving money over time is hard, no matter who you are. In today's world: How do we save? This is why I believe in bitcoin. Almost all professional

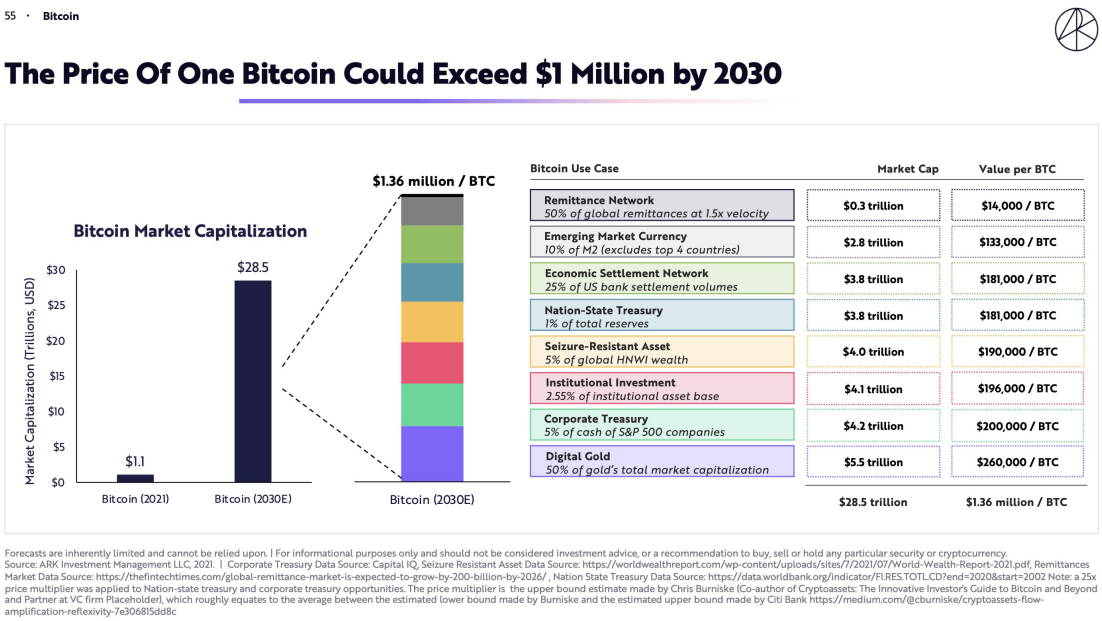


Figure 4.4: Potential market exposure to Bitcoin as a money

athletes make the majority of their career earnings in their 20s. With a lack of education, inaccessible tools, and inflation, a sad yet common reality is many enter bankruptcy later on. We can do better. We need to improve financial literacy. Bitcoin is a proven, safe, global, and open system that allows anyone to save money. It is the most accessible asset we've ever seen."

This ubiquity of access is what probably most distinguishes Bitcoin. Previously it could be argued that only the most wealthy could access the 'means' to store their labour without loss of value over time (through inflation). To be clear, inflation is an important part of the money system, somewhat within the control of the central banks, and approximate to taxation. It applies equally to all holders of the money supply. Asserting that money should be replaced by a 'hard asset' such as Bitcoin, in the place of the more controllable utility of money, is likely both a fantasy, and wrong minded. This conflation of money and property is a confusion caused by Bitcoin's proximity to money, and it's 'money like' network, and is extremely commonplace.

These narrative takes are all rooted in the popular idea that Bitcoin is a 'hedge against inflation'; an increasingly fragile take, as the price plummets with global markets. The Bitcoin community seems somewhat confused about the nature of money, which is predictable because we can see in these sections that money is pretty confusing. Money is the fluid thin 'working' layer on top of historical human production, which provides transaction convenience, and tools for credit. Value is effectively swapped in and out of this layer through the actions of central banks, controlling inflation into acceptable margins. Simplistically this is done through manipulation of interest rates (the easiness of credit), quantitative easing (buying of assets) and quantitative tightening (selling of assets). It is primarily *not* a long term store of value, as Austrian economists perhaps believe it should be. This function is left to assets.

Fundamentally, Bitcoin isn't money (in the traditional sense) because it's not an IOU, which money certainly is. It's a bearer instrument, novel asset class, with money like properties, as identified above. As said again and again it functions most like a 'property'

which can be invested in by anyone, with all the attendant risks of that property class to the holder. Lyn Alden says it sits somewhere between a saving tool, and an investment, acting as "programmable commodity money".

Andrew M. Bailey says *"in an ideal world where governments honour the rights of citizens, they don't spy, they don't prohibit transactions, they manage a sound money supply, and they make sound decisions, the value of bitcoin is very low; we're just not in an ideal world"*

Another potentially important differentiating affordance is censorship resistance. There's really nothing else like it for that one feature. With that said Bitcoin is only a viable 'money like thing' when viewed in the layers described in this book, and elsewhere[98]. The base chain layer is an apex secure store of value. Whatever layer 2 ultimately emerges is the transactional layer which could replace day to day cash money, while the hypothetical layer 3 might be useful for complex financial mechanisms and contracts operating automatically, and also provides the opportunity for using the security model of the chain to support other digital assets, including government currencies through stablecoins. All these things have a natural home in borderless social spaces.

4.5 Risks (money, not technical)

Special thanks to economist Tim Millar for help with this section.

4.5.1 Risks to Bitcoin the money

4.5.1.1 Geopolitics

It can be seen that following the invasion of Ukraine by Russia, that sanctions of various kinds were applied to the Russian economy. One of these was the previously dicussed Swift international settlement network. Another whole catagory was the removal of support by private businesses domiciled outside of Russia and Ukraine, and pertinent here is that VISA, Mastercard, Paypal, and Western Union all removed support for their product rails. This means that while some cards and services still work, and will likely work again through Chinese proxies in the coming months, considerable disruption will be felt by Russian companies and individuals. This is not to say that this disruption is necessarily wrong, but it is clear now that all of these global financial transfer products and services are contingent on political factors. The same might be true of CBDC products if they gain traction globally. There is certainly no reason why all money within a physically delineated border could not be blocked or cancelled. This is not as true for Bitcoin at this time.

However, with enough political will it is technically plausible to incentivise miners with additional payments to exclude transactions from geolocated wallets. This would be mitigated by Tor, and in a global anonymous network it is very likely that a miner could be found at a higher price for inclusion in the next block.

We have already seen much negative political positioning related to the energy concerns in an earlier chapter. There are similar noises coming from policy makers with regard to the money utility of the technology. The United Nations have made the following recommendations: *"Developing countries may have less room to manoeuvre, yet the regulation of cryptocurrencies is possible. The following policies, among others, have the potential to curb the further spread of the risks of cryptocurrencies and stablecoins:*

- *Ensuring comprehensive financial regulation, through the following actions:*
  - *Require the mandatory registration of crypto-exchanges and digital wallets*

and make the use of cryptocurrencies less attractive, for example by charging entry fees for crypto-exchanges and digital wallets and/or imposing financial transaction taxes on cryptocurrency trading;
  - *Ban regulated financial institutions from holding stablecoins and cryptocurrencies or offering related products to clients;*
  - *Regulate decentralized finance (such finance may, in fact, not be fully decentralized, given its central management and ownership, which form an entry point for regulation);*
- *Restricting or prohibiting the advertisement of crypto-exchanges and digital wallets in public spaces and on social media. This new type of virtual, and often disguised, advertisement requires policymakers to expand the scope of regulation beyond traditional media. This is an urgent need in terms of consumer protection in countries with low levels of financial literacy, as even limited exposure to cryptocurrencies may lead to significant losses;*
- *Creating a public payment system to serve as a public good, such as a central bank digital currency. In the light of the regulatory and technological complexity of central bank digital currencies and the urgent need to provide safe, reliable and affordable payment systems, authorities could also examine other possibilities, including fast retail payment systems.*

This is tough talk. We have seen that the IMF is willing to make their loans contingent on such regulation. This global response to the technology is a significant headwind, but like the internet itself, it's very hard to actually stop these products being used.

4.5.1.2 Liquidity Lottery

Because holders of BTC are disincentived to sell the asset (assuming future gains) it is likely vulnerable to something Kao called the 'liquidity lottery'. This is a supply/demand mismatch which he thinks could spell the end of the asset class in time.

4.5.1.3 Manipulation of price or the network

Bitcoin is still young and illiquid enough to be highly manipulable. Imagine for instance if a major organisation or nation state wished to accumulate a significant amount of the asset, but would prefer a lower price.

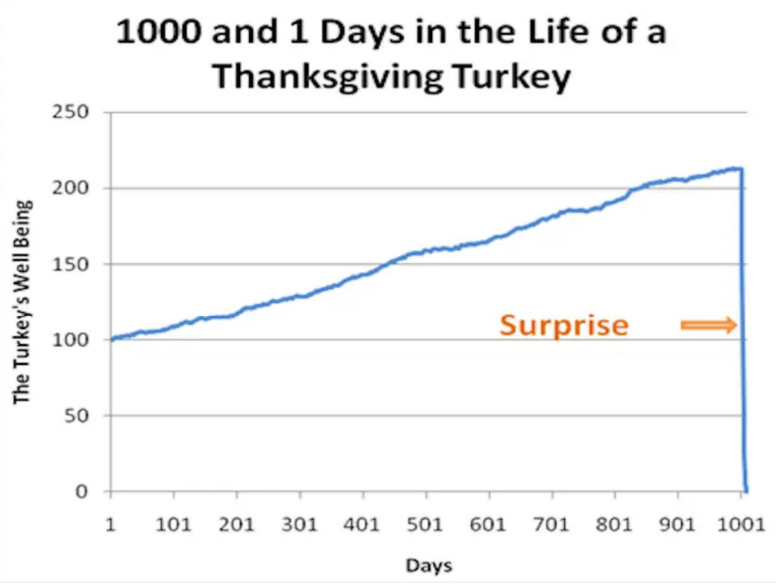
There is an unknown level of exposure to risk from centralised mining. If a few of the major mining pools were simultaneously infiltrated by a nation state actor then it might be possible to engineer a 'deep re-org' of a large transaction. This would be dealt with quickly and almost certainly be a transient attack, but the damage to the narrative might be substantial. A similar vulnerability exists in the centralisation at the level of internet service providers [99]. This or some other flaw might lead to a selling cascade. Nobody knows just how vulnerable to selling cascades Bitcoin might be against a really serious challenge by an empowered actor, but it's already high volatility is suggestive of risk.

4.5.1.4 Rehypothecation

It's vulnerable to rehypothecation (paper bitcoin managed by centralised entities running a fractional reserve). It seems that Figure 4.5 by Nassim Taleb is a cautionary tale [100].

4.5.1.5 Scale

Scalability is always going to be a problem for Bitcoin, for all the reasons discussed in the blockchain chapter. There is no "ready to go" solution (except perhaps federations)



Wikimedia Commons

Figure 4.5: Nassim Taleb's Turkey Problem

that could onboard the whole world at this time because of the limited number of available UTXOs.

Finally, a lack of fungibility, and privacy by default in Bitcoin, trends towards blacklists and over time this could seriously compromise the use of the asset.

4.5.1.6 Centralisation of the money over time

In a medium term future it's possible to imagine a smart enough autonomous AI or ML actor managing to accrue Bitcoin through fast and smart 'decisions'. This could unreasonably centralise the asset, and it would be impossible to claw this situation back. These constructs would last for the lifetime of the chain unless constrained by timelock multisigs for instance.

4.5.2 Bitcoin externalities

This section is the risks that Bitcoin poses to external money systems, but it's worth pointing out that a risk to wider society is clearly *also* a risk to Bitcoin itself.

4.5.2.1 Inherent volatility

One of the better public analysts of the asset, sees the price eventually fluctuating somewhere between $700k and $300k. Figure 4.6. This is not how a money is supposed to work.

Neither though is it the endless "number go up" that speculators have been promised. The aims of the project have a cognitive dissonance right at the core. The volatility trends toward:

4.5.2.2 Unfair distribution

By design the distribution of Bitcoin is likely 'fair', in that everyone has been able to access and secure the asset long term without prejudice. Figure 4.7 from Twitter user @Geertjancap shows the distribution in 2021. Whether this is judged to be fair if the asset



Figure 4.6: Cycle theory revisited blog post [Image used with permission]

jumps to 10 times it's current value, minting a new class of hyper rich holders, is another matter. This pressure to emulate the early winners leads to:

4.5.2.3 Endless HODL

It's possible that there's a problem with people not wanting to sell the asset, because they are predisposed to a particular fervour promoted within the community. This can be seen in the glassnode data, where the black line in Figure 4.8 shows that the asset held for more than a year (illiquid) has increased over the years. There's real recalcitrance about using the asset as a money, which leads to:

4.5.2.4 Reduction of funding source / liquidity in legacy finance

In the current financial system remuneration for labour performed in the workforce is loaned into the money system, where it's put to work providing liquidity for creation of more opportunity. This system actually works pretty well. The more of this deferred labour that's taken out of the legacy system, the less work can be done with what remains. This isn't to say that Bitcoin will cause a liquidity crisis, but there is possibly a cost if the current trend continues. This isn't as bad as:

4.5.2.5 Bitcoin collapse system shock

In the event of an existential collapse of the Bitcoin network the erasure of so much capital would certainly have a contagion effect on the whole global financial system. It's hard to imagine what such an event could be, this being the nature of "black swans". One cited example is the unravelling of cryptography by quantum computing. Some conspiracy theorists in the past have even speculated that Bitcoin is itself a canary in the coal mine, engineered by the NSA to warn about emergent quantum computing somewhere in the world. It's all pretty silly because without cryptography Bitcoin would be the least of humanities problems. The risk of 'something' does exist though. The same anti-fragile feature can't be said about the technologies around Bitcoin, which gives us:

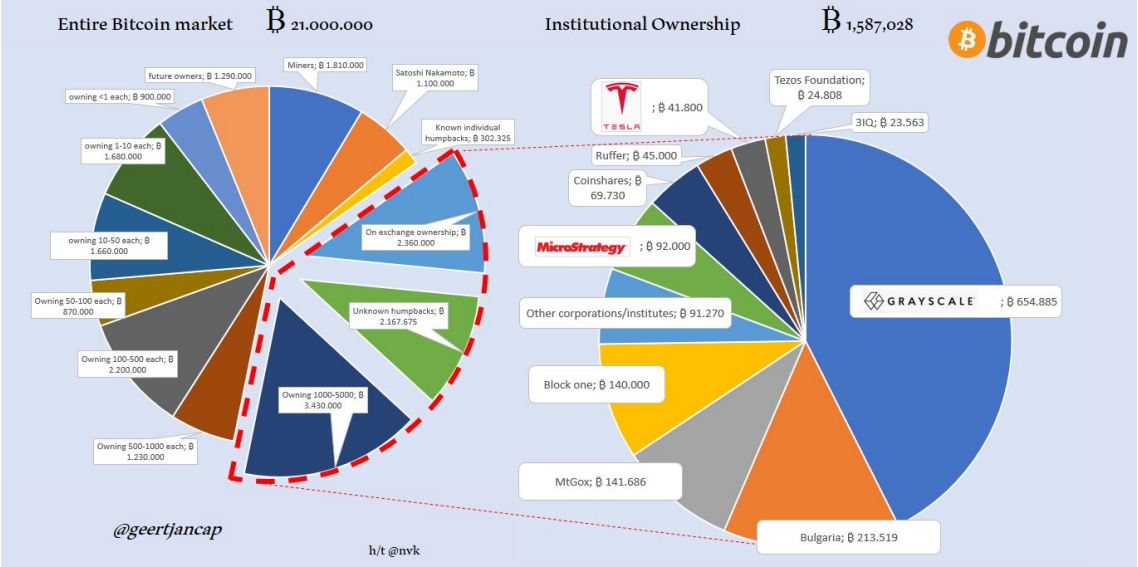


Figure 4.7: Bitcoin distribution is skewed to s few early holders, but it likely is fair. [Image used with permission]

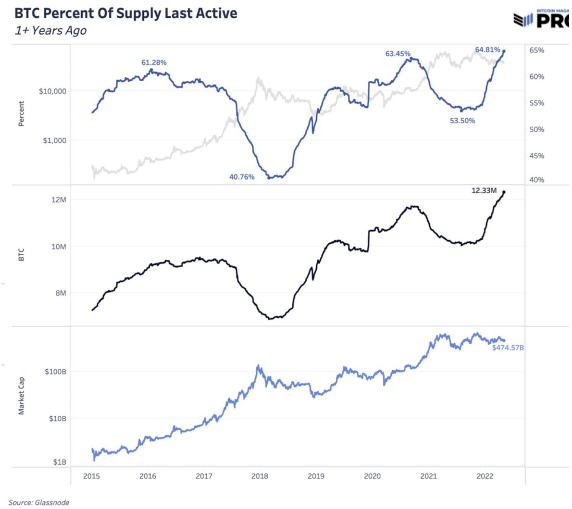


Figure 4.8: Supply of bitcoin that hasn't moved for over 1 year

4.5.2.6 Stablecoin collapse system shock

This is much more likely. Stablecoins are under regulated, centralised, under collateralised, ponzo like structures, which could quite clearly fall apart at any point. The contagion effects of this are unclear as they're not yet too significant. They're a risk nontheless, and may be an indicator of:

4.5.2.7 Tech for techs sake yielding unexpected outcomes

The whole question of what Bitcoin addresses, whether it's been properly thought about, what the end goals are, and what the risks are is significant. It's a computer science and engineering solutions gone completely wild. It's clearly got benefits and there's clearly human appetite for this technology, but it's probably running ahead of the knowledge base around it. This is most exemplified in:

4.5.2.8 No agreed measurable end goal

Bitcoin is a game theoretic juggernaut, where success of the network breeds more success for the network. The was obviously a great design choice for the computer scientists trying to solve the problem of a secure, and scalable, electronic cash, which couldn't be confiscated. Ironically for a global consensus mechanism it seems that nobody wants to discuss what constitutes a successful end point to this, and especially not what 'successful' endpoints for the game theory which have calamitous negative repercussions for wider society look like. This might have implications for:

4.5.2.9 National security / actual warfare

There's some national security implications for Bitcoin which are discussed both in the fringes and the sector media. Essentially, the industrial mining complexes which are more commonplace now, are easily identifiable targets, and provide nations with both some leverage over the global network, and a considerable source of income. The IMF correctly identifies these facilities as a way for nation states to monetise their energy reserves without the need for foreign markets, opening the door to sanction avoidance. In the case of smaller and developing nation states who are perhaps subject to financial penalties on the global stage for whatever reason, these facilities start to look like legitimate targets for cyber and conventional warfare. This 'weaponisation' of a neutral technology is already manifest in:

4.5.2.10 Bitcoin as a culture war foil

Bitcoin's online community skews very hard toward right wing libertarianism. This isn't to say there are no other voices, but they are certainly outnumbered. This imbalance is almost certainly a product of the ESG concerns around the technology. There has been a notable increase in diversity of thought since the evolution of the energy narrative, but it persists. This leads to a paucity of voices in policy making circles, and in the USA a strong delineation between policy makers along party lines. This kind of thing tends to be self reinforcing, and it seems very possible that the global liberal left will swing mainly against the technology, while the neoliberal right will be attracted more to it. As tensions increase so it seems does the online rhetoric. Even scientists now seem to agree that Bitcoin investors are calculating psychopaths [101]. This leads to:

4.5.2.11 Self reinforcing monocultures

There are some powerful 'pockets' of fringe thinking within the vocal, online, Bitcoin communities. The most palatable of these are figures like Michael Saylor, Elon Musk and

Jack Dorsey, but there's whole subcultural intersections around antivax, anti-woke, anti cancel culture, and fad diets. It might seem that this isn't terribly important, but Bitcoin viewed though the lens of these of these communities looks pretty strange to the newcomer. The early adopters are just using their wealth to leave the battlefield behind using:

4.5.2.12 Jurisdictional / legislative arbitrage

The reach of Bitcoin and it's ability to undercut the global money systems, delivering savings for those with a first mover advantage, and the current paucity of agreed legislation has set up an interesting and rare condition. Bitcoin encourages something called jurisdictional arbitrage; the race to take advantage of the variance in national approaches to the asset class. This section could perhaps be explored as a list of opportunities, but from the viewpoint of our SME business use case it's far more likely that these destabilising 'features' are risks:

- **Difference in 'crypto' profit models**. Countries and jurisdictions can apply different charges for use of trading platforms and capital gains tax enjoys huge variance. Some countries are now competing to offer zero tax as a way to attract valuable tech mind share.
- **Income tax** is harder to monitor in a truly international context. This is variously pitched around the world. It's hard to monitor this stuff and tax at source like with company employees wages, because it's basically designed to be hard to monitor. This results in:
- **Passport perks**. Countries are already selling residence and company rights against Bitcoin marketing. There's a lot of new ways to buy passports and citizenship based on 'inclusion' in this community now. It's a terrible look. The early adopters can live international jetsetter lifestyles and ca benefit from:
- **Business subsidies** such as those appearing in Switzerland, Hondoras, El Salvador, Africa etc. This means a new divide is emerging since some countries are in instead applying:
- **KYC/AML** rules which make onboarding into this technology harder. Currently there's a trend toward globally capturing information about people buying these assets, but it's effectively tech warfare now with engineers, rapidly producing tools to circumvent slow and varied legislation. The best example of this remains El Salvador, where Bitcoin is legal tender, and has perhaps kickstarted:
- **Bond issuances**. El Salvador are having a faltering start to their promised bond issuance. It might be that all of this is a harbinger of the rise of:
- **The Network State** is a proposal by Srinivasan [102]. His is a transhumanist thesis which he describes: *"The fundamental concept behind the network state is to assemble a digital community and organize it to crowdfund physical territory. But that territory is not in one place — it's spread around the world, fully decentralized, hooked together by the internet for a common cause, much like Google's offices or Bitcoin's miners. And because every citizen has opted in, it's a model for 100% democracy rather than the minimum threshold of consent modeled by 51% democracies."*

4.5.2.13 Hyperbitcoinization

All of the above starts to look like convergence on something the crypto community regularly describes to itself within it's internal media. Hyperbitcoinization is a term coined in 2014 by Daniel Krawisz [103]. It is the hypothetical rise of Bitcoin to become the global

reserve currency, and the demonetisation of all other store of value assets. This seems unlikely but is hinted at in a game theoretic analysis of both Bitcoin and current macro economics. Again, Bitcoin is a likely very poor replacement for money. The ability to monetise assets through banks, backed by law and contracts (the debt based system), is a highly refined human concept, while Bitcoin is a fusion of Austrian economics, and a computer science project. The hyperbitcoinization idea finds it's ultimate expression in Svalholm's "Everything Divided by 21 Million", a hypothetical re-accounting of all human production into the Bitcoin ledger [104].

Nobody is sure what a regular deflationary cycle might do to global supply chains. Malherbe et al. point out the inherent unsuitability of a deflationary asset such as Bitcoin as the global reserve currency [105] and feel that perhaps other cryptocurrencies might be more suitable for adoption by governments. Interestingly this is the only paper to reference 'Duality' (the only thing purportedly written by Satoshi Nakamoto after they left the project).

Writer and activist Cory Doctorow is not a fan of Bitcoin. He provides an excellent summary of what he sees as the basic societal mistake of the libertarian ideals around strong property rights and hard money. In a hyperbitcoinised world where debt law would be enforced by distributed code, it might be far harder to prevent the "fall of Rome" scenario he describes.

Fulgur Ventures (a venture capital firm) provide a blog post series about the route this might take. It's important to note that Budish suggested that the usefulness of Bitcoin (and blockchain) cannot exceed the cost to attack it. The is highly suggestive that hyperbitcoinisation is impossible [106]. It's beyond the scope of this book to look at the implications of all this.

4.6 Does DeFi matter to SMEs

DeFi is decentralised finance, and might only exist because of partial regulatory capture of Bitcoin. If peer-to-peer Bitcoin secured yield and loans etc were allowed then it seems unlikely that the less secure and more convoluted DeFi products would have found a footing. DeFi has been commonplace over the last couple years, growing from essentially zero to $100B over the last two or three. It enables trading of value, loans, and interest (yield) without onerous KYC. If Bitcoin's ethos is to develop at a slow and well checked rate, and Ethereum's ethos is to move fast and break things, then DeFi could best be described as throwing mud and hoping some sticks. A counter to this comes from Ross Stevens, head of NYDig who says *"The concept of decentralized finance is powerful, noble, and worthy of a lifetime of focused effort."*. This may be true in principle, but certainly isn't the case as things stand.

According to a recent JPMorgan industry insider report, around 40% of the locked value on the Ethereum network is DeFi products. It is characterised by rapid innovation, huge yields for early adopters, incredibly high risk, and a culture of speculation which leads to products being discarded and/or forked into something else in the pursuit of returns. Ethereum also allows miners of the blockchain to cheat the system [107].

Much of the space is now using arcane gamification of traditional financial tools, combined with memes, to promote what are essentially pyramid schemes. Scams are very commonplace. Loss of funds though code errors are perhaps even more prevalent.

The Bank for International Settlements have the stated aim of supporting central banks

monetary and financial stability. Their 2021 report on DeFi noted the following key problems.

- ..a "decentralisation illusion" in DeFi due to the inescapable need for centralised governance and the tendency of blockchain consensus mechanisms to concentrate power. DeFi's inherent governance structures are the natural entry points for public policy.
- DeFi's vulnerabilities are severe because of high leverage, liquidity mismatches, built-in interconnectedness and the lack of shock-absorbing capacity.

These are two excellent and likely true points. European Parliament Vice President Eva Kaili made this same point at the World Economic Forum, so clearly regulators are aware of the lack of meaningful distribution in DeFi. In addition access to DeFi is 'usually' through Web2.0 centralised portals (websites) which are just as vulnerable to legal takedown orders as any other centralised technology. Given who the major investment players seem to be in this 'new' financial landscape it seems very likely that regulatory capture is coming. The seemingly unironic trend towards CeDeFi (centralised decentralised finance) illustrates this; it's is all likely a fad.

There are more recent DeFi on Bitcoin contenders, but these are vulnerable to the same attacks and problems in the main.

There is likely no use for this technology for small and medium sized companies on the international stage. It is far more likely that reputation would be damaged. The 'best' of the portfolio of DeFi offerings is perhaps high yield stablecoin accounts, where dollars equivalent tokens are locked up providing very high return rates of up to 20 percent. It's also possible to get loans (by extension business loans) out of such systems at relatively low risks. The best 'distributed' example of this is probably Lend, at HODLHODL, which is a peer-to-peer loan marketplace. Atomic Finance leverages discrete log contracts amongst other more edge uses of Bitcoin, to provide financial services without custody of the users' Bitcoin. It is possible to make the argument that between hodlhodl loans, taro asset issuance, boltz exchange, and lightning escrow that all of the "classes" of DeFi smart contract can be serviced already by Bitcoin alone.

Many more custodial options exist for loans (CASA, BlockFi, Nexo, Ledn, Abra etc). These might not really fit the definition of DeFi at all. Many of these centralised DeFi companies (CeDeFi) have imploded in the wake of the Terra/Luna collapse since they were generating yield from one another and ultimately Terra. The maxim seems to be that if you don't know how the system is monetised then you are likely the product. DeFi itself weathered the recent market turmoil comparatively well and it's possible that as these products evolve they may be useful to companies who have Bitcoin and stablecoins on their balance sheet long term. Dan Held maintains an online spreadsheet which compares these products.

4.7 Do DAOs matter to SMEs

A distributed autonomous organisation, or DAO is a governance structure which is built in distributed code on a blockchain smart contract system. Token holders have voting rights proportional to their holding. The first decentalised autonomous organisation was simply called "The DAO" and was launched on the Ethereum network in 2016 after raising around $100M. It quickly succumbed to a hack and the money was drained. This event was an important moment in the development of Ethereum and resulted in a code fork

which preserves two separate versions of the network to this day, though one is falling into obsolescence. Again, this is covered in Shin's book on the period in extreme detail, but it seems this stuff is falling into dusty history now, leaving only a somewhat tarnished and technically shaky legacy [30].
In practice DAOs have very few committed 'stakeholders' and the same names seem to crop up across multiple projects. Some crucial community decisions within large projects only poll a couple of dozen eligible participants. Its might be that the experiment of distributed governance is failing at this stage.

Perhaps more interesting is the use of the DAO concept to crowd fund global projects, currently especially for the acquisition of important art or cultural items. DAOs are also emerging as a way to fund promising technology projects, though this is reminiscent of the 2017 ICO craze which ended badly and is likely to fall foul of regulations.

Within the NFT and digital art space PleaserDAO has quickly established a strong following. "PleasrDAO is a collective of DeFi leaders, early NFT collectors and digital artists who have built a formidable yet benevolent reputation for acquiring culturally significant pieces with a charitable twist.

Opensea wrangle between IPO and governance token.

ConstitutionDAO, Once upon a time in Shaolin etc

4.7.1 Bisq DAO

One of the better designed DAOs is Bisq DAO. It's slightly different design trys to address the issue of overly rigid software intersecting with more intangible and fluid human governance needs. From their website:

"Revenue distribution and decision-making cannot be decentralized with traditional organization structures—they require legal entities, jurisdictions, bank accounts, and more—all of which are central points of failure. The Bisq DAO replaces such legacy infrastructure with cryptographic infrastructure to handle project decision-making and revenue distribution without such central points of failure."

4.7.2 Risks

The most interesting thing about DAOs is that they belong more in this money chapter than they do in blockchain. As we have seen they're finding most success as loosely regulated crowd funding platforms. If a small company did find itself wishing to explore this fringe mechanism for raising capital, then we would certainly recommend keeping a global eye on evolving regulation and the onward legal exposure of the company.



5. Distributed Identity & Trust

For distributed Web3, and by extension metaverse applications to flourish it is necessary to solve the identification problem [108]. Without a solution to this bots, scammers, and AI actors will reduce usefulness and usability of and already quite arcane user experience.

This chapter is an oddity because most of traditional DID/SSI isn't really fit for purpose. Distributed self sovereign identity has a great elevator pitch though. Individuals should be empowered through technology to manage their own data, without manipulation or exploitation by centralised corporate behemoths. In practice it's a staggeringly complex proposition which increases risk to the individual, decreases convenience, and despite much work, does not even make much sense in it's own terms. Webs of trust are viable so this means Nostr, Marking, or Slashtags which will be discussed, but are early products. Thanks to Melvin Carvalho for advice with this section.

5.1 Applications of DID/SSI

Some of the likely, and discussed applications for DID/SSI are the more inherently private and personally valuable sets of data an individual might generate throughout their life. The theory is that subsets of such data could then be digitally revealed by the individual when required, and that cryptographic verification built into the system would guarantee the veracity of the data to the receiving party. It is also possible to make use of "zero-knowledge proof" such that assertions can be made about about the contents of the data without revealing the data itself. A good example of this an age verification challenge, where a threshold age could be asserted without necessarily revealing the date of birth. Other keystone uses of the technology are:

- health documents history
- qualifications and certifications
- financial record and relationships with those of others
- contacts, connections to other people and their appropriate data, including things like shared and personal calendars

It's also possible to extend this key management ethos to all login credentials, and all data currently stored on centralised servers. This is the tension discussed in the chapter about Web3. Proponents think that using something like a DID/SSI stack to manage encryption,

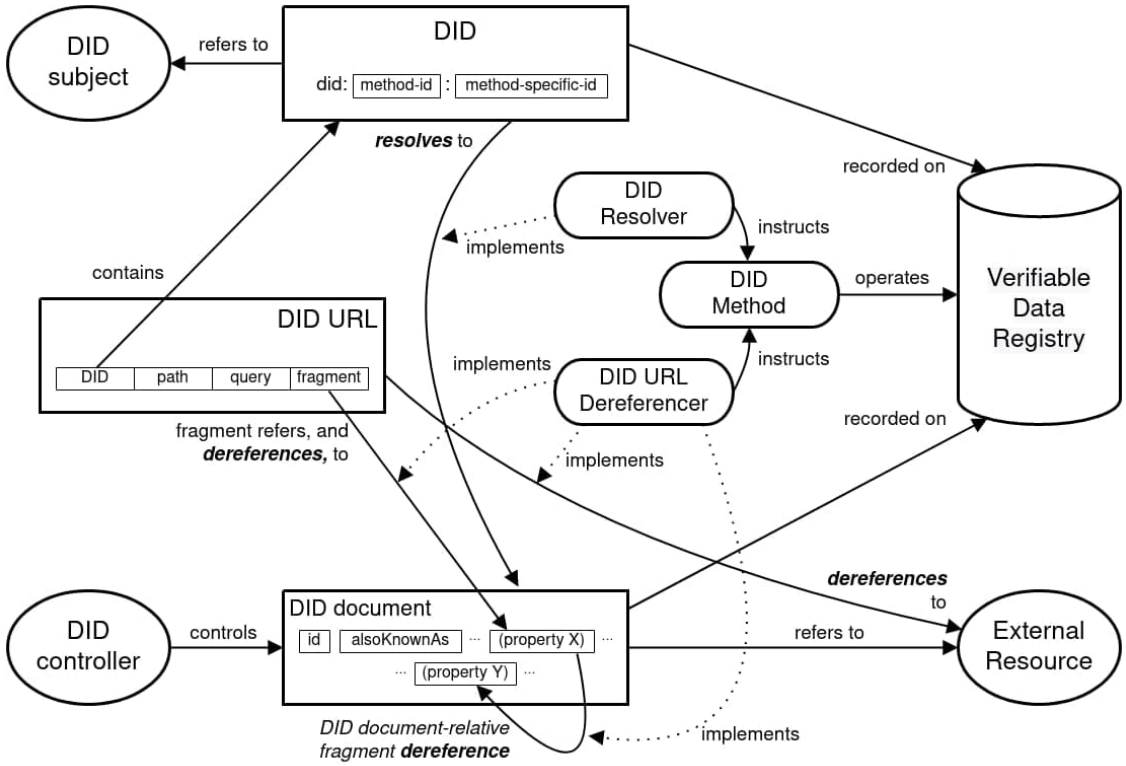


Figure 5.1: Part of the DID SSI specs

decryption and access to data within cloud services gives the user the best of all worlds. They see simply logging in with a cryptographic wallet, and using that same public/private key pair to manage the data beyond as some kind of panacea. This is very complex stuff though, and it seems very likely they just haven't thought this through enough.

5.2 Classic DID/SSI

Distributed identity / self sovereign identity has been extensively researched for decades, with hundreds of peer reviewed papers, and extensive support from the world wide web consortium. The academic field now seems quite ossified and has settled on a couple of hundred 'schema' which they feel underpin the next layer of development. It is a complex field, and the language and diagrams are arcane and self referential as seen in Figure 5.1. . Moreover the minimal implementation of such proposed systems hints at a federated model of centralised 'truth' to enable persistence of identifiers over time.

The major failing of the DID/SSI work to date is a lack of meaningful use cases with incentives for adoption. This is clearly explained by Lockwood [109] who proposes that the pathway to adoption of 'classic' DID/SSI requires an incentive over and above the current identity management on the web. Being distributed is not enough. Especially in the light of questionable assurances of this even being true.

Perhaps most concerning is this recent exchange on the mailing lists. Here, the two inventors of DID say the following:

"Not a single entity I know that's doing production deployments has actually vetted did:ion and found it to be production capable. This goes for every DLT-based DID Method out there - even the one we're working on. I am highly sceptical of anyone that says that any

DID Method is ready for production usage at present.
Agreed — as one of the proponents of DLTs (in particular permissionless public ones) none are mature enough yet for production.". It seems then that we can rule out use of these technologies?

5.2.0.1 DID principles

The core principles of distributed identity are that there should be persistent identifiers, like real world documents which assert identity, but with extended use cases. These should be permanent, and resolvable everywhere, forever. Underpinning this is cryptographically verifiable and decentralised data, managed by the user, or their trusted proxy. As primitives this makes them lifetime digital assets, that are portable, and unconfiscatable, with no required reliance on a trusted third party. By this stage in the book you should be familiar with these concepts, but application of this fundamental mindset to all personal data and digital interactions is a bigger reach even than money and value.

5.2.0.2 What's in a DID document?

All classic DID is underpinned by a DID document what bootstrap the services it's connected to. It is made up of one or more public keys. The documents can make use of services such as timestamps, cryptographic signatures, proofs, delegations, and authorisations. They should contain the minimum amount of information to accomplish the specific task required of them.

5.3 Newer Technologies

5.3.1 Lightning

It is possible to log into a website using only Lighting, as in Stacker News.

5.3.2 Slashtags

Slashtags is a new distributed identity open method being developed by Bitfinex and Tether under the Synonym suite. It uses Bitcoin keys for authentication, but communicates a schema through a metadata exchange.

5.3.3 Microsoft ION

While working at Microsoft on ION Daniel Buchner (now working at Square) or Henry Tsai said the following, which is worth quoting verbatim:

"While ledger-based consensus systems, on the surface, would seem to provide the same general features as one another, there are a few key differences that make some more suitable for critical applications, like the decentralized identifiers of human beings. Some of these considerations and features are:

- The system must be open and permissionless, not a cabal of authorities who can exclude and remove participants.
- The system must be well-tested, and proven secure against attack over a long enough duration to be confident in.
- The system must produce a singular, independently verifiable record that is as immutable as possible, so that reversing the record the system produces is infeasible.
- The system must be widely deployed, with nodes that span the globe, to ensure the

record is persisted.
- The system must be self-incentivized, so that nodes continue to operate, process, and secure the record over time. The value from operation must come from the system directly, because outside incentive reliance is itself a vector for attack.
- The cost to attack the system through any game theoretically available means must be high enough that it is infeasible to attempt, and even if an ultra-capitalized attacker did, it would require a weaponized mobilization of force and resources that would be obvious, with options for mitigation.

The outcome:
- Number 1 eliminates private and permissioned ledgers
- Number 2 eliminates just about all other ledgers and blockchains, simply because they are inadequately tested
- For the metrics detailed in 3-6, Bitcoin is so far beyond all other options, it isn't even close - Bitcoin is the most secure option by an absurdly large margin."

On the surface then it might seem that the choice is Bitcoin again, and indeed that the open source Microsoft ION stack is a natural choice, but it's complex to run, the interactions with the blockchain have a cost implication which can't be surmounted without every user owning some Bitcoin, and as we have seen, there is no formal validation of this system. In addition (in the current implementation) an identity proof does not need to be published to be valid, just timestamped. In this way an identity can be stolen and used years later to claim later chains of proof. It seems that it might be somewhat useful 'at scale' and is worth additional monitoring and investigation, especially given it's integration into TBD - Web5.

5.3.4 Nostr

Nostr is "The simplest open protocol that is able to create a censorship-resistant global "social" network once and for all." according to it's github page. More than that it's a client side validated proof of who a user is interacting with, hence being in this identity section. To be clear, it's not a completely peer to peer system in that it uses relay servers, but this gives it some of the best characteristics of both paradigms. This has the following advantages for our metaverse application;
- it's lightweight, with minimal network overhead and complexity
- it's real-time using websockets
- anyone can run a relay server, so one can be run in the deployment in the final section of the book.
- Each of the client peers connecting to the metaverse can be a relay and able to pass messages and proofs to the other clients without the metaverse server seeing the data or being online
- it's opensource
- there are multiple usable libraries and tools
- it's under active development with an excellent team. The lead, 'Fiatjaf' is one of the most prolific developers in the lightning space.
- it's based on the same underlying cryptographic technology we are using elsewhere, indeed with it's use of Bitcoin keys the identity system is global
- it provides the identity proof that we need to validate users and objects into a virtual space
- it enables message passing

- it scales to be a social network as required
- it need not rely on anything outside of a relay hosted on the metaverse server
- it can likely be scaled to provide one to many bulletin board style applications within the metaverse
- it can easily operate outside of the walled garden of the metaverse, extending the reach of the messages

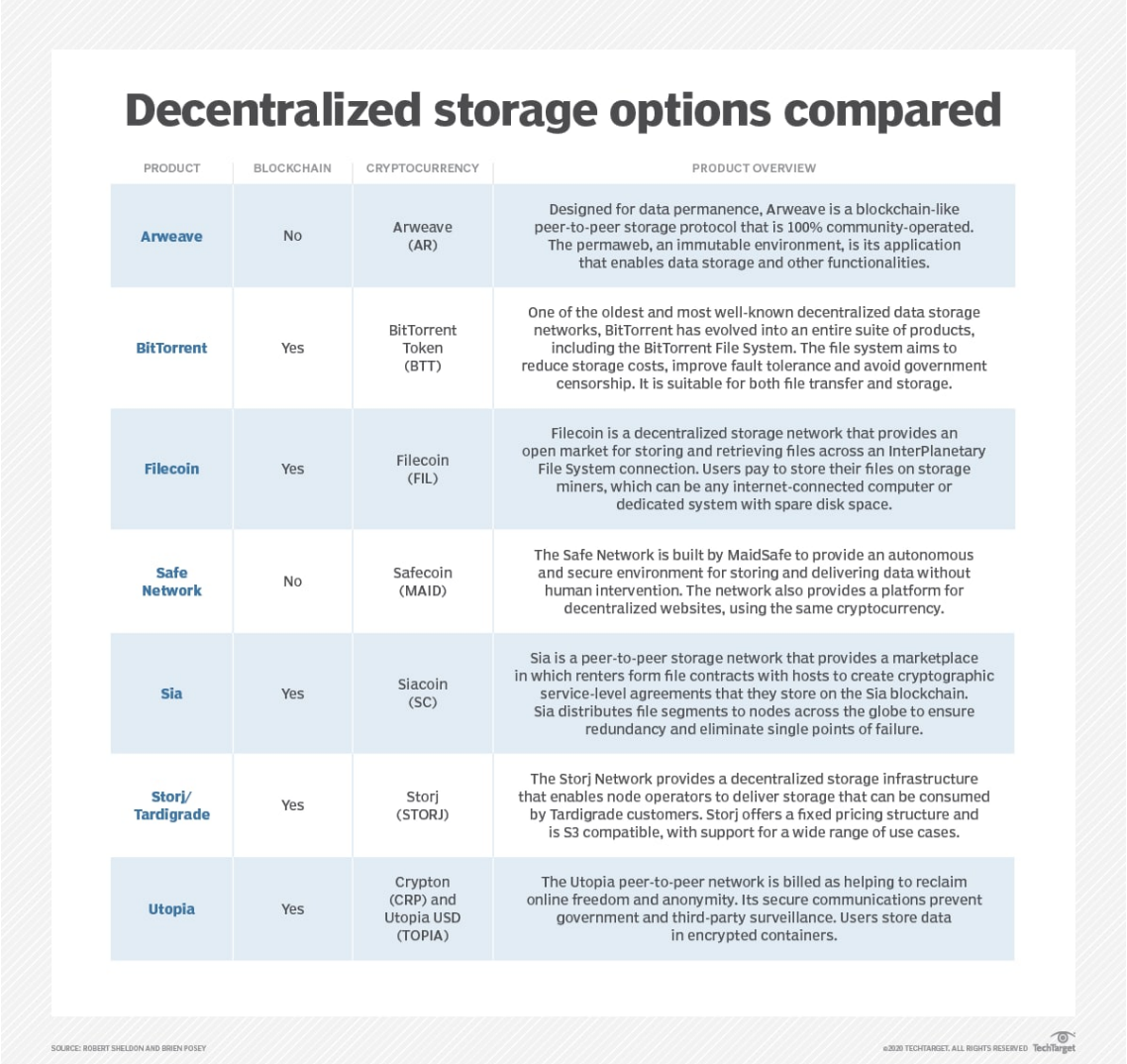
Nostr is incredibly promising, and integrating these relays in the metaverse servers and clients of the proposed technology stack in this book might allow us globally provable identity, with privacy by design. It can provide message passing. If all entities in the metaverse scenegraphs are also Nostr key pairs then schema can be applied consistently with the economic layer using the same key system as Bitcoin. A curated list of projects and libraries is available on github.

5.4 Micropayment based web

It seems the war against disinformation is now being lost. Much is written in the media about Deepfake technology creating plausible fake videos, but probably more pernicious is the use of toolkits to create entire plausible fake news sites using natural language AI such as GPT3. This makes it cheap to publish potentially market moving news which is then rehypothecated by online news vendors who are hungry for clicks. As these pipelines become more mature it will be difficult to keep fake news for financial or political gain out of the system. One interesting way to do this that *isn't* webs of trust or true cryptographic identity is to charge micropayments for "one to many" publication models. This would imply a tiny instant payment for clicks, especially on social media sites such as twitter. This kind of model has been discussed but is only possible in the context of systems such as Lightning where instant micropayment can be realised. It seems possible that this would price out speculative 'noise' spam from the information space. It's interesting and ironic that the origin of proof of work was to underpin just such a spam defeating system [16], and that Nakamoto mentioned this application for Bitcoin back in 2009. There is now much chatter about the integration of Bitcoin with Twitter in light of Musks buyout of the social network. .

5.5 Risks & Challenges?

Classic DID/SSI risks fragmentations. In all DID applications, scaling to a world where the user is managing potentially thousands of these critical cryptographic data files is daunting. Abstracting the guts of this away to make the use simple, and only mindful of thet right level of information, turns out to be huge problem that nobody has solved It's not clear that users want this. In the case of web of trust like Slashtags it's a big piece of work for the users to rate all of their digital interactions with a trust metric.



Decentralized storage options compared

PRODUCT	BLOCKCHAIN	CRYPTOCURRENCY	PRODUCT OVERVIEW
Arweave	No	Arweave (AR)	Designed for data permanence, Arweave is a blockchain-like peer-to-peer storage protocol that is 100% community-operated. The permaweb, an immutable environment, is its application that enables data storage and other functionalities.
BitTorrent	Yes	BitTorrent Token (BTT)	One of the oldest and most well-known decentralized data storage networks, BitTorrent has evolved into an entire suite of products, including the BitTorrent File System. The file system aims to reduce storage costs, improve fault tolerance and avoid government censorship. It is suitable for both file transfer and storage.
Filecoin	Yes	Filecoin (FIL)	Filecoin is a decentralized storage network that provides an open market for storing and retrieving files across an InterPlanetary File System connection. Users pay to store their files on storage miners, which can be any internet-connected computer or dedicated system with spare disk space.
Safe Network	No	Safecoin (MAID)	The Safe Network is built by MaidSafe to provide an autonomous and secure environment for storing and delivering data without human intervention. The network also provides a platform for decentralized websites, using the same cryptocurrency.
Sia	Yes	Siacoin (SC)	Sia is a peer-to-peer storage network that provides a marketplace in which renters form file contracts with hosts to create cryptographic service-level agreements that they store on the Sia blockchain. Sia distributes file segments to nodes across the globe to ensure redundancy and eliminate single points of failure.
Storj/ Tardigrade	Yes	Storj (STORJ)	The Storj Network provides a decentralized storage infrastructure that enables node operators to deliver storage that can be consumed by Tardigrade customers. Storj offers a fixed pricing structure and is S3 compatible, with support for a wide range of use cases.
Utopia	Yes	Crypton (CRP) and Utopia USD (TOPIA)	The Utopia peer-to-peer network is billed as helping to reclaim online freedom and anonymity. Its secure communications prevent government and third-party surveillance. Users store data in encrypted containers.

SOURCE: ROBERT SHELDON AND BRIEN POSEY

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Figure 5.2: Comparison of distributed file stores



6. Non Fungible Tokens

Nonfungible tokens are a whole 'class' of digital token, separate and distinct from everything discussed to this point. They are generally recognised in law as property in their own right [110, 111]. In the Initial Coin Offering (ICO) and project tokens detailed earlier, and limiting this description to the Ethereum network for now, a project launching an ERC-20 token commits contract code to the blockchain, and this contract then mediates the issuance and management of millions or billions of tokens associated with that project, and it's use case. ERC-20 is a fungible token issuance. Each of the projects' tokens is interchangeable with any other token. They're all the same from the point of view of the user.

Rather than the ERC-20 contract type used for fungible token issuance NTFs predominantly use ERC-721 protocol on Ethereum (just different instructions). It's the case that most NFTs in the 2021/2 hype bubble are algorithmically generated sets of themed art (so called PFP-NFT). Tens of thousands of distinct tokens are 'minted', each one being a complex transaction commitment to the Ethereum blockchain, along with it's associated gas fee. These minting events were much hyped social occasions (before the 2022 market crash), and happened very quickly, with users clamouring to create art with randomly allocated features from the art schema associated with the project. Lucky winners could find themselves with an NFT art piece with more than an average number of 'rare' features. If the overall mint becomes more popular, then the secondary market for all of those mints goes up, and because of the liquidity premium they can go up a lot. The perceived rarer mints go up a lot more. This whole process is very energy intensive on the chain, and the vast majority of these project simply trend to zero value. In response to this appalling cost benefit analysis the Ethereum foundation have proposed EIP-2309 to make minting NFTs more efficient. They say "This standard lets you mint as many as you like in one transaction!"

The Ethereum foundation give their somewhat constrained view of NFTs on their website and it's a useful primer. On that page they detail some of the use cases, as listed below, with a critique added:

- Digital content; this is the dominant use case right now. Much more on this later.
- Gaming items; again more on this later, it's an obvious enough use case but complex politics in the intersection of games and crypto have stalled the adoption curve.

- Domain names; this is just starting to reach for applications now, why not a database with the ISP/host?
- Physical items; seemed like a clear over-reach as transfer of the NFT does not imply transfer of the object, but this is emerging as the growth use case.
- Investments and collateral; while this was an emergent option in the space, it's likely been a bubble, as owners of the tokens cast around for additional liquidity, and loan businesses chased yield with higher risk. The recent implosion of lenders and funds in the crypto space was partly a function of supposedly world class risk managers accepting jpegs as collateral.

Moving away from Ethereum, NFTs can be minted on most of the other level one chains. Solana is a great newcomer example. Sol is a terrible chain with regards to decentralisation, but thanks to that it's far cheaper and faster to mint NFTs on it, and it's become a troubling competitor for Eth (Figure 6.1).

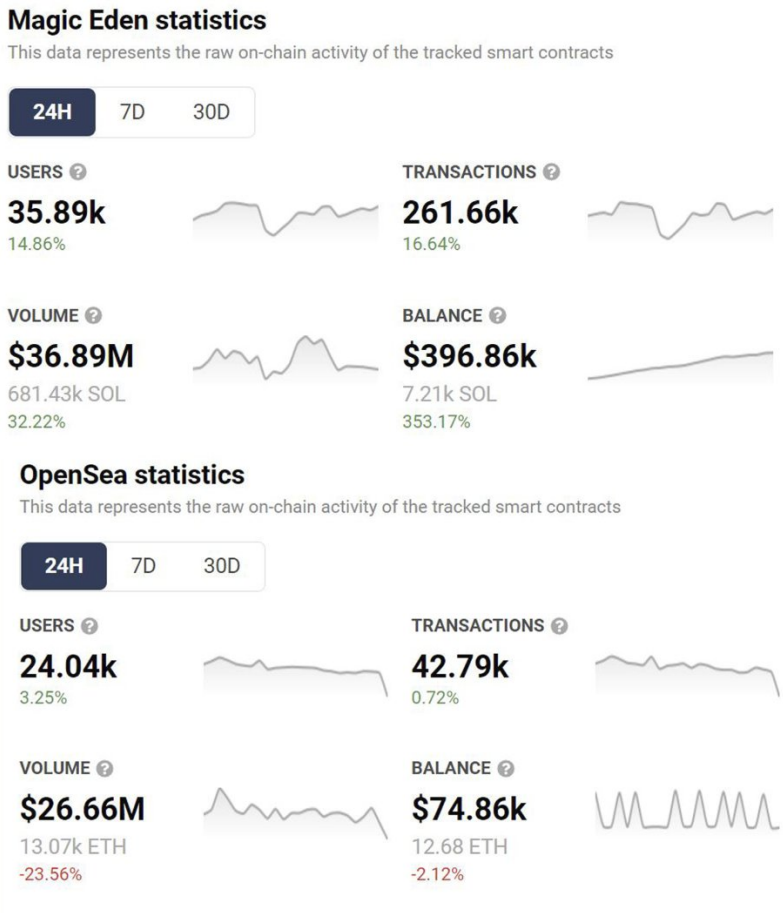


Figure 6.1: Solana NFT markets are enjoying growth compared to Opensea on Ethereum, even in the downturn.

The same might be true for Cardano's ADA, though ADA is struggling to hold onto it's market position despite some technical advances. It's worth reiterating here that the nature of these digital tools likely makes for a 'winner take all' market dynamic over time. With fees being central to this generative NFT use case it's possible to see that highly centralised, fast, and cheap chains will capture and eventually dominate the space. Remember that this likely (game theoretic) outcome might as well be a database running without the stark

inefficiencies of blockchain. The whole NFT space is a gamble on consumer enthusiasm for spending money continuing to outpace logic.

Astonishingly, according to a JPMorgan insider market report (reported on in a podcast), only around 2 million people have ever actually interacted with NFTs. One analysis suggests that a single entity accounts for 3 of the top 4 holders, having made 32,000 ETH from the NFT boom. This suggests heavy market manipulation and is far from the egalitarian landscape claimed in the hype. Tellingly it's thought around 10% of the trading volume on market leading platform 'Super Rare' was by the now bankrupt venture capital firm 'Three Arrows'.

With that said NFTs have clearly allowed digital and new media artists to connect with audiences without gatekeepers. Established mediators and curators of art have been caught totally wrongfooted, and NFTs seem to give a way for them to be cut out completely. There are suggestions of applications beyond this initial digital art scope. This is a compounding, and disrupting paradigm change.

6.1 NFT key use cases

6.1.1 Art

The recent surge of interest in NFT's during early 2021 has largely been driven by digital art NFT's, despite the origins of digital art NFT's started much earlier in 2014. New York artist Kevin McCoy's *Quantum* is widely recognised as the first piece of art created as an NFT. However it was during early 2021 that art NFT's started to gain significant attention; by the end of 2021, nearly £31b had been spent on NFT purchases, a considerable and exponential growth given 2020 sales of ~£71m High profile digital artists such as *Beeple* whose recent recording break sale of his NFT *"The first 5000 days"* (Figure 6.2) at Christies (a long established British auction house, specialising in high profile precious work of art) for £52.9m helped bring NFT's into the public spotlight and wider give them global attention.

Art as NFT's offer the following advantages:

6.1.1.1 Immutable Nominal Authenticity

Art fraud such as false representation, forgeries, plagiarism have been a reoccurring blight since art has existed; artists and works of art have been open to abuse by forgers, black market profiteers and even fellow artists laying claim to works of art of others. Unless a work of art is sold, exhibited or listed, documenting when and who created it, the *nominal authenticity,* which Dutton states as the *"correct identification of the origins, authorship, or provenance of an object"* [112] can be increasingly mutable over a period of time, dependent on a multitude of factors, including; the artists existing profile, how widely and where the work of art is exhibited, if the work of art is commissioned by a patron, if it's sold, and profile of the buyer/collector. At its most basic level, once a work of art is 'minted' as an NFT (publishing the art work as a unique token on the blockchain) this functions as an immutable publicly accessible proof of ownership and by extension proof of creation. The act of minting is not purely limited to digital art; all an artist requires is a digital representation of any physical art (sculpture, physical painting, installation etc..) which can be used as a proxy allowing artists to record the date of creation/origin of a physical piece of art on the blockchain, a buyer purchasing the NFT can be provided the actual physical artwork as part of the NFT. Nominal authenticity becomes secure and

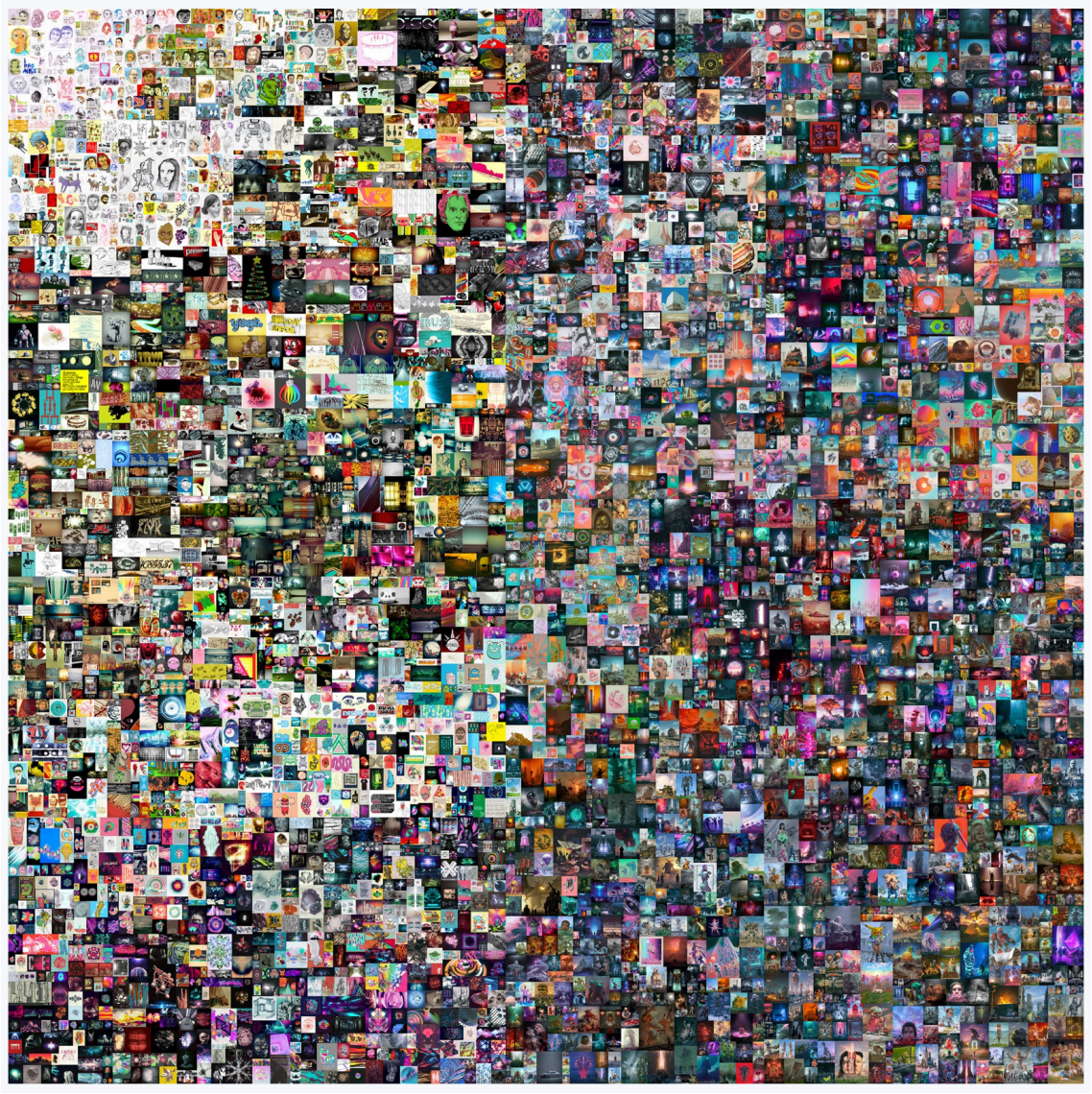


Figure 6.2: Beeple: First 5000 days, taken from the Christies website, assumed fair use.

immutable for the lifetime of the blockchain (by no means assured).

6.1.1.2 Secure Digital Provenance

Provenance (or the chain of custody) is an important aspect in works of art, antiques and antiquities. Provenance not only helps assign work to an artist but also documents ownership history. Digital provenance, an inherent feature of NFT's means provenance now no longer becomes what has historically sometime been a contentious detective's game at the best of times; one that is open to fraud, misinterpretation and entirely reliant on good record keeping.

Since provenance can contribute to the value of a piece of art (benefiting both the creator and collector) the use of the blockchain as an open, secure ledger is a far more trustworthy system than traditional methods of artistic provenance that were cobbled together; often consisting of a mix of physical and digital documents spanning private & public sale receipts, art/museum gallery exhibitions and private record keeping). Digital provenance provided when an artist 'mints' a piece of art into an NFT allows artists and

collectors to record a secure, permanent unalterable history of transactions for a specific piece of art, providing future collector complete trust in the origin and custody of a piece of art.

6.1.1.3 Decentralised automated royalty payments

Traditionally if a piece of art is sold, the first sale may (but not always) benefit the artist financially, however secondary and any subsequent sales would only ever financially benefit the buyer/collector; the original artist would rarely benefit. However If a work of art is minted into an NFT, royalty payments can be predetermined and automated in perpetuity directly by the use of a 'smart contract'. Smart contracts are small, automated scripts/programs that run automatically and independently of a buyer/seller; pre-determined conditions are set by the buyer; these trigger when certain conditions are met i.e

6.1.1.4 On sale transfer

20% of total sale amount into digital wallet of the creator. 80% of total sale amount into digital wallet of the seller.

Once the royalty payment rate is set by the artist/creator, future royalties of all sales can be paid directly to the artist/creator account (via a digital wallet) without the need of a third party (traditionally a gallery/agent etc..).

Smart contract driven NFT's means that even if piece of art is resold 5, 10 or even a 100,000 times moving through 5, 10 or even a 100,000 different collectors; a pre-determined royalty payment rate set by the creator would still guarantee the artist/creator is paid directly from each and every future sale.

Historically provenance for works of art may span across generations, for instance Gabriël Metsu's oil on canvas painting *The Lace Maker's* provenance, first recorded in 1722, now spans 300 years of ownership, including from a British Baron in the 19th century to an American philanthropist in the 20th century.) Metsu died young at the age of 38, leaving a widow; neither his/her relatives/descendants benefit from his original work, 300 years later this would be near impossible to facilitate with traditional systems, as even legal contracts are open and prone to the ravages of time.

NFT smart contracts hold an incredibly potential; an artists descendants financially benefiting directly from the resale of a piece of work long after the artist/museum's/gallery or even state have turned to dust as long as the original creator's digital wallet is accessible, *the blockhain becomes an everlasting digital patron* ensuring

NFT art currently suffers from the same failure of decentralisation already discussed in the Ethererum technology stack, but this is compounded by the normalisation of intermediate art brokers continuing to custody the NFTs even after sale. They are usually selling a pointer to their own servers. The market is nascent and evolving, but it's currently not delivering on it's core promise.

Proof of ownership is intuitively a pretty obvious application for the technology, but again it's hard to justify the expense when the benefits are so slim. Bulldogs on the blockchain is a clear gimmick, and might even incentivise poor behaviours as there are two products here which are not necessarily aligned. Much has been written over the years about deeds to property being passed through blockchains, cutting out the middle man, but in the event that a house deed NFT was hacked and stolen it's obviously not the case that the property would then pass to the hacker.

One of the most interesting companies is Yuga Labs, who launched the incredibly popular Bored Ape Yacht club set of 10,000 algorithmically generated NFTs. These

Ethereum based NFTs were based loosely on the 'Crypto Punks' model of PFP-NFT (variously profile picture project, picture for proof, and picture for profile - no definition remains uncontested for long). Yuga launched with a better commercialisation model for the holders, and a strong marketing drive into celebrity circles. They now regularly change hands for hundreds of thousands of pounds. Even this 'blue chip' NFT is not without serious criticism: *"I'd put it at 99.99% the project is in fact a deliberate troll, intentionally replete with Nazi symbols and esoteric racist dog whistles"*

Yuga recently bought the artistic rights to the commercial reuse of similarly popular (and preceding) Punks set. This is interesting because they have again handed the commercial re-use rights to the owners of the individual NFTs. This raises the same confusing problem with attaching commercial rights to an easily stolen token as NFTs for real estate does. This has been demonstrated recently when Seth Green had a Bored Ape stolen after creating an animated show around it's IP. Many more contradictions and ambiguities in NFT licenses are emerging. Galaxy Digital have surveyed the landscape: *"Contrary to the ethos of Web3, NFTs today convey exactly zero ownership rights for the underlying artwork to their token holders. Instead, the arrangements between NFT issuers and token holders resemble a distinctly Web2 maze of opaque, misleading, complex, and restrictive licensing agreements, and popular secondary markets like OpenSea provide no material disclosures regarding these arrangements to purchasers. Something more is required, and that 'something' is a legal agreement between the owner of the image—known as the 'copyright holder' and the NFT holder specifying what rights the NFT holder has with respect to the image. To the extent an NFT purchaser has any rights to the image associated with his or her NFT at all, those rights flow not from his or her ownership of the token, but from the terms and conditions contained in the license issued by the NFT Project governing the NFT holder's purchase and use of the image. Accordingly, for the vast majority of NFT projects, owning the NFT does not mean you own the corresponding digital content that is displayed when you sync your wallet to OpenSea. That content, as it turns out, is owned and retained by the owner of the copyright associated with that digital content, typically the NFT project. After reviewing the most used license agreements for NFT projects, it becomes apparent that NFT standards and smart contracts do not recognize off-chain law."*

Even so, the community around these collections is incredibly strong, mixing developers, artists, the rich and famous, and the fortunate and early, into a cohesive community who communicate online. The developer 'good will' is enormous, and it seems possible that this will lead to faster and broader innovation around the collections, and out into metaverse applications. The brand is strong, and the individual NFT items both benefit from, and reinforce that brand, while adding personal narratives and human interest.

As a gauge of how frothy this market still is it's interesting to look at the APE token which Yuga just launched. They airdropped 10,000 of the tokens free to each of the 10,000 NFT holders. This instantly created a multi-billion dollar market cap, and a top 50 'crypto' out of thin air, based purely on their brand. It's clear that there is both brand, and a market here.

A recent report from "Base Layer" tries to capture the community 'feature' of big brand NFTs. "Crypto culture decoded" explains that is is these online communities which are the attraction not necessarily the art. This is a powerful 'in group' argument, though speculation remains the most likely underpinning.

While it is likely that this is currently a speculative bubble, that is waning already

(Figure 6.3), it seems certain that the technology is here to stay in some form.

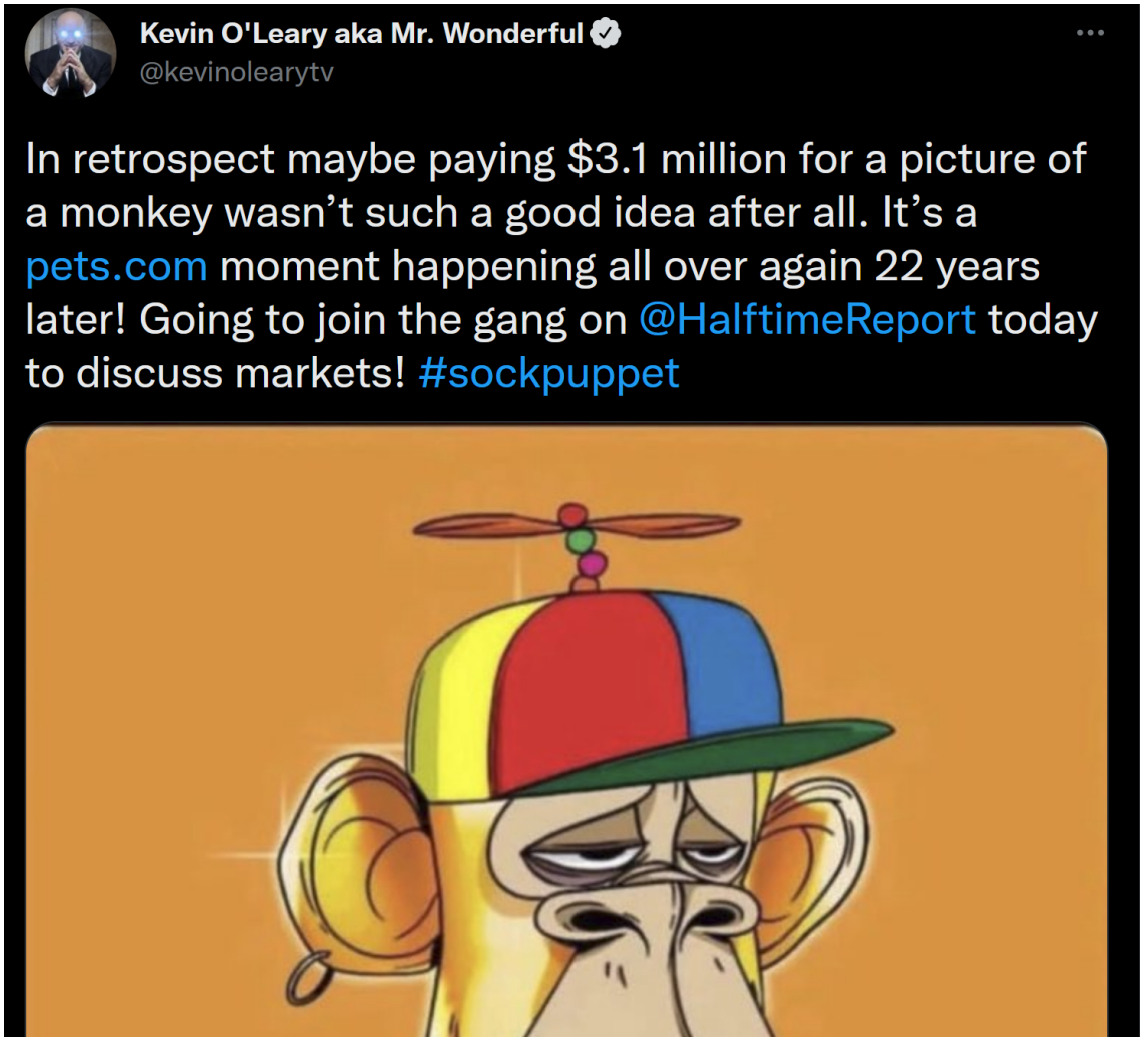


Figure 6.3: The bubble bursts on Yuga Bored Apes for now.

6.1.2 Computer & Video Games

Computer & Video games are a huge global business, exponential global growth over the last 30 years has seen this grow to a point where it has eclipsed both the global movie and North American sports industries combined.

A global industry with revenues over £120b, with ~half the people on the planet playing some form of games in 2021.

As the games industry has evolved and matured over the last 40 years, secondary markets have emerged, most notably the 'second hand' games resale market. The rise of 'retro' gaming, has demonstrated the second hand market is a lucrative one for private resellers, an unopened copy of Super Mario Bros for the Nintendo Entertainment System recently selling for £1.5M to the extent the market has seen speculators looking to cash in on the huge global interest in retro/second hand games.

Despite publishers and developers increasingly moving to non-physical digital only' games, the demand for used games remains incredibly high.

Whilst some retailers have adapted their business models to include reselling of retro/second hand games, the vast majority of publisher/developers/retailers aren't able to directly benefit from the emerging retro/second hand games market. The potential of *video games as NFT's* presents a huge opportunity for publishers, developers and players alike, offering the following advantages:

6.1.2.1 Royalty Sales on Pre-owned Games

; A predetermined proportion of any resale of a used game can automated in perpetuity via smart contracts; once these are set by the publisher, future royalties of all sales can be paid directly to the publishers/developers wallets (a digital account) without the need of a third party (traditionally a retail entity). Traditionally only the initial first sale of a game would financially benefit the publisher/developer/retailer, secondary and subsequent sales would only ever financially benefit the purchaser, with many developers/publishers arguing this is hurting the wider industry through the loss of significant income generated by the secondary and subsequent sales, sometimes over the course of decades. However the use of NFT's smart contracts means that if a game is sold/resold through 10,000 collectors; a pre-determined royalty payment rate set by the publisher would still guarantee the publisher (and or developer/retailer) takes a proportion of any future sales.

6.1.2.2 Monetisation of User Generated Content:

Games as a NFT's offer ability to monetise UGC: User generated content. Video games such as Nintendo's *Pokemon Go (166 million players)*, Bungie's *Destiny 2 (38 million players)* or miHoYo's Genshin Impact (*9 million players*) all have large, established and significant player bases. What is noteworthy, the games are designed to encourage players may spend hundreds, or in some cases thousands of hours on one game alone; according to Destinytracker.com, the top players have amassed total play times over 20,000 hours, close to 1,000 days or ~ 3 years, which is incredible feat given Destiny 2 only launched 5 years ago in 2017.

Destiny/Pokemon Go and Genshin Impact revolve around a central key game mechanic; players investing significant amounts of time collecting in game digital assets; characters/weapons/items, often classed as 'rare' or 'exotic' or '5 Star'. These collectibles usually found by a combination of the accrual of in-game time, completing quests, purchasing additional in-game items/boosters, and luck ('RNG'). Players are often encouraged to share their collections of rare characters/weapons/ objects through in-game achievements, triumphs, scores acting as a mark of distinction/status symbol.

Traditionally there has been nothing that went beyond sharing the *digital badge* (i.e triumph/achievement/accomplishment) on a on social media/gamer's platform profile. However NFT's offer the ideal system for developers/publishers and even players to monetise user generated/customised data (such as a players unique save game data), simultaneously allowing: a) creation of an additional monetised ecosystem to meet player demands i.e. some players who are willing to monetise and 'sell' their invested time in a particular product/service to other players with little time but willing to pay other players for 'grinding' (progressing laborious in game tasks) and a more advanced in-game progression point. The potential to provide publishers/developers with an additional long-term income stream, providing a better ROI on computer & video game development, which in many instances can cost hundreds of millions in development costs spanning 5/10 years, is undeniable.

6.1.2.3 Play to earn revenue models

This is morally dicey at this time and early startups like Axie Infinity are in serious trouble. A (long) video by Dan Olsen highlights the structural problems with both play to earn and NFTs.

6.1.2.4 Monetizing In game collectibles

customisable in game assets (vanity items such as cosmetic character skins/clothing or collectible items that offer player advantages(new weapons/vehicles/mods etc,..)

Traditional gamers have pushed back on the seemingly useful idea of integrating NTFs with traditional games. This may be in part because Ethereum mining has kept graphics card prices high for a decade.

HBAR partnerships

Critique from Marc Petit of Epic and Unreal.

The following text is from Justin Kan, co-founder of twitch: *"NFTs are a better business model for games. Many gamers seem to be raging hard against game studios selling NFTs. But NFTs are also better for players. Here's why I think blockchain games will be the predominant business model in gaming in ten years. NFTs are a better business model for funding games . Example: recently I invested in a new web3 game SynCityHQ. They are building a mafia metaverse and raised $3M in their initial NFT drop.*
NFTs give studios access to a new capital market for raising capital from the crowd.NFTs can be a better ongoing model for games. Web3 games will open economies, and by building the games on open and programmable assets (tokens + NFTs) they will create far more economic value than they could from any one game. Imagine Fortnite, but other developers can build experiences on top of the V-Bucks and skins. Epic would get a royalty every time any transaction happens. As big as Fortnite is today, Open Fortnite could be much bigger, because it will be a true platform. NFTs are better for gamers Allowing gamers to have ownership of the assets they buy and earn in game allows them to participate in the potential growth of a game. It lets gamers preserve some economic value when they switch to playing something new. But what about the criticisms of NFTs? Here are my thoughts on the common FUDs: "It's just a money grab on the part of the studios!"
Game studios already switched over to the model of selling in-game items, cosmetics, etc to players long ago. But currently the digital stuff players are buying isn't re-sellable. NFT ownership is strictly better for players. "The games aren't real games." This reminds me of the criticism of free-to-play in 2008, when the games were Mafia Wars / FarmVille. We haven't had time for great developers to create incredible experiences yet. Everyone investing in games knows there are great teams building. "Game NFTs aren't really decentralized because they rely on models / assets inside centralized game clients." Crypto is as much a movement as it is a technology. Putting items on a blockchain is what gives people trust that they have participatory ownership...which make people willing to buy in to the game. These assets are "backed" by blockchain. The fact that these item collections are NFTs will make other people willing to build on top of them. "NFTs are bad for the environment." Solana and L2s solve this. NFT games are better for players and for game developers. Like the free-to-play revolution changed gaming, so will blockchain. The games of the future will be fully robust, with open and programmable economies."

6.2 Broader and metaverse uses

So far according to a16z NFTs break down into:

- Profile pictures: These were discussed at the start of the chapter and have felt ubiquitous on Twitter over the last couple of years. The major projects will likely hold value, but the hype cycle will likely lead to all profile NFTs going in and out of fashion. There's potentially a fresh wave of this same kind of low key identity hype possible in the metaverse, and indeed the two plausible both intersect and converge.
- Art and Music: Art has also been discussed above. Peter Thiel, the billionaire venture capitalist who founded PayPal has invested in expanded NTF use cases. The first is 'Royal' which is experimentally selling limited NFT tokens which contractually entitle the holder to a portion of music artist royalties. Spotify are experimenting with music NFTs (and of course in the metaverse). This is an early adopter area, and again likely converges with our planned uses cases.
- Gaming: As discussed there's pushback from the gaming community, but huge investment from the likes of Lego, Blizzard, Epic, Ubisoft etc.
- Gig tickets: Not only the straightforward use of transferable tickets for events as NFTs on a blockchain (which is impossible due to the cost right now) but also onward monetisation of ticket stubs as memorabilia. The NBA is already looking at this.

  "The team sells the ticket for face value many many years ago, but when that stub is being sold now for much more many times over, the team gets none of that money," York explained. "But with an NFT stub that changes. Let's say a new rookie enters the NBA next season and he turns out to be the next LeBron James. That ticket stub from his first game, as an NFT, the team can put a commission on it — 20 percent or however much, the NBA decides that. In 10 years when it's worth a lot of money, I or whoever owns that NFT, can sell it for say $100,000. The NBA can still collect 20 percent of that sale, because it's all on a smart contract."

  It seems so obvious that this will extend to the virtual events space in the metaverse.
- Utility: These are broadly 'membership' style tokens, and this seems like a sensible fit. Peter Thiel (again) for instance launches a political funding NFT from Blake Masters to support his senate ambitions. To be clear, Thiel is a fundamentalist libertarian, and at the very least highly eccentric. This is not necessarily a positive for the technology.
- Virtual worlds are a huge application for NFTs, and this seems like it would be a natural fit for out metaverse application. In reality the $2B of sold so far is mostly 'allocations' in nascent ecosystems, being sold as highly speculative assets, without even a metaverse to use. The majority of that amount is the hyped 'Otherland' plots sold under the Bored Apes brand.
- "Full stack" luxury brands. Nic Carter describes a mating of physical and virtual luxury goods. His is a useful article on the future direction, and he has also provided a primer on NFTs. There are many such examples already, such as Tiffanys 'NFTiff' - cryptopunks collaboration which will automatically generate royalties for Tiffanys and parent company Louis Vitton in perpetuity. Such products prove provenance, create new aftermarket opportunities, and unlock metaverse applications.

It is completely reasonable to assert that these use cases could be accomplished without the use of NFT technology, and is part of the hype bubble.

Twitter user Cantino.Eth offers an exhaustive roundup of what they think future uses might be. It's a thread full of industry insider jargon but it's indicative of a shift in focus from speculation to 'building' as the market conditions change. Some of the more interesting (less arcane) use cases identified in the thread are summarised very briefly below, again with comments as to how this might pertain to our metaverse applications.

- Hobby tokens, demonstrating interest in an activity. This is potentially a metaverse adaptation of badges on a blazer in the real world, and might serve to drive communities in a metaverse. The same is true for activism and political alighnment. It's a great idea and worth developing.
- Professional Networks and qualification badges, like a LinkedIn qualification panel, but in the metaverse. A cisco NFT in the metaverse for a CCNA qualification makes intuitive sense.
- Badges to indicate membership of distributed projects within a metaverse. This allows users to identify avatars with shared goals in the metaverse.
- Retail incentives, like brand loyalty stamps or rewards for participation in marketing, or early access programmes. This is a true in a metaverse marketplace as it is in a real world coffee shop.
- Multiplayer communities with incentives to hit collective milestones. "Collecting as a team sport". This again seems like a great and intuitive opportunity, but is perhaps less suitable for our more business focussed space. User content submission and automatic monetisation when reused by brands, bonded to an NFT contract.
- Customer Cohort NFTs: early adopters of successful brands would be able to prove the provenance of their enthusiasm for a new product, and this might unlock brand loyalty bonuses. It seems this wouldn't be a transferable NFT, and is more like the "soulbound" idea advanced by Meta.
- Education and Customer Support, think an NFT of a great score on reddit community support forums. A trusted community member badge, but visible in the metaverse. This is somewhat like the web of trust model advanced earlier in the book.
- NFTs as contracts is far more likely in the metaverse than it has proved to be in real life. This is how 'digital land' and objects will be transferred anyway, but with the addition of contractual conditionals with external inputs more subtle products may appear.

6.3 Objects in our metaverse

NFTs seem to be judged crucial to metaverse applications. Meta (ex Facebook) are hanging their monetisation of their whole rebrand on taking a huge cut from NFT content creators on their platform.

We have a path to assets and NFTs within the layer 3 elements of our choices (RGB), but they're not yet fit for purpose. There are compromise options already available, as below.

6.3.1 Liquid tokens

We have seen that Liquid from Blockstream is a comparatively mature and battle tested sidechain framework, based upon Bitcoin. It is possible to issue tokens on Liquid, and these have their own hardware wallet available. This makes the technology a strong contender for our uses.

6.3.2 Sovryn and RSK

It's slightly unclear when RSK will support assets at this level. This needs to be revisited.

6.3.3 Stacks and STX

There's another possible option is Stacks, without the network effect of Ethereum, but closer to the other design choices made so far. "Stacks is an open-source network of decentralized apps and smart contracts built on Bitcoin."
This novel approach saw the launch of a layer 1 blockchain token called STX, which is used in a similar way to gas in Ethereum. but claims settlement on the Bitcoin network. This is achieved through a novel bridging approach which they call Proof of Transfer (PoX).
Stacks users say this hybrid approach is a pragmatic solution which enables dApps, smart contracts, DeFi, NFTs etc without compromising security. In practice the speculative component of the STX tokens which underpin these operations clouds the issue somewhat. It is a potentially useful middle ground solution with a great deal of developer attention.

6.3.4 Ethereum

While it's been discounted elsewhere it's hard to ignore the network effect of Eth NFTs. If the aspiration is to attract the bulk of the 'legacy' creator/consumer markets then it will be necessary to support integration of Metamask into any FOSS stack. This isn't a huge technical challenge, nor is it particularly of interest to our use cases at this stage, but it remains a possibility. The main problems remain the slow speed and high expense of the system.

6.3.5 Solana

Solana is both cheap and fast, because it's very highly centralised. It seems unlikely that it's worth this level of compromise.

6.3.6 Satoshi Ordinals

Satoshi ordinals allow tracking of Sats across transactions, enabling NFT like assignment tracking. This is a hugely exciting development but extremely early.

6.3.7 Peerswap

It may be possible to use "Peerswap" to execute rebalancing and submarine swaps into and out of Liquid assets on the sidechain in a single tx. This is anunder explored area at this time.

6.3.8 FROST on Bitcoin

It **might** be possible to transfer ownership of a UTXO on the Bitcoin base chain using FROST [113]. In this Schnorr & Taproot based threshold signature system it's possible to add and remove signatories and thresholds of signing without touching the UTXO itself. In principle (though not yet in practice) this might allow transfer of UTXO ownership.

6.3.9 Spacechains

It feels like spacechains are almost ready, so this is worth keeping an eye on. It's the 'cleanest' way to issue assets using Bitcoin because there's no additional speculative chain. As briefly explained in the earlier section Bitcoin is destroyed to create a new chain which then inherits the security of Bitcoin through onward mining. This new asset or chain is able to accrue value and trade independently based purely on it's value to the buyer, not as a function of a wider speculative bubble attached to a token with multiple use cases.



7. Metaverses

7.1 Toward an open metaverse

For our purposes in this book and product design the interface between the previous chapter (NFTs) and this metaverse chapter is crucial. Punk6529 is a pseudonymous twitter account and thought leader in the "crypto" space. The text below encapsulates much of the reasoning that led to this book and product exploration, and is paraphrased from this thread for our purposes.

Bit by bit, the visualization layer of the internet will get better until it is unrecognisably better (+/- 10 years). As the visualization layer of the internet gets better, digital objects will become more useful and more important. Avatars (2D and 3D), art, schoolwork, work work, 3D virtual spaces and hundreds of other things. Not only will the objects themselves become more important, they will lead to different emergent behaviours. We see this already with avatars and mixed eponymous/pseudonymous/anonymous communities. Yes, it is the internet plumbing underneath, but just like social media changed human behaviour on the internet, metaverse type experiences will further change it. NFT Twitter + Discord + various virtual worlds is a form of early metaverse. I feel like I am entering a different world here, not just some websites. The most important question for the health of the internet/metaverse/human society in the 2030s will be decided now. And that question is: "who stores the definitive ownership records of those digital objects". There are two answers: a company's database OR a blockchain. If we end up with "a company's database" we will end up with all the web2 dysfunctions, but worse. SMTP is an open protocol that anyone can use so we don't have societal level fights on "who is allowed to use email". Short messaging online ended up becoming Twitter. So we end up having the most absurd, surreal discussions on the topic of "who is allowed to use short-messaging" being dependant on "who is the CEO of Twitter". There is no way this is the correct architecture for our progressively more digital economy.... If this is your first time around here, we are fighting for an open metaverse."

It seems that industry shares much of this opinion regarding an open metaverse. The proposal of a persistent interactive digital universe online is **so** vast that major players recognise that they will not be able to monopolise this space, though Facebook/Meta are clearly attempting to. The Metaverse Standards Forum is clearly an attempt by the other

industry players to catch up and then get out ahead of Meta in this regard. It's also possible to view this as just another land grab, but through the vehicle of a standards body. Time will tell. They say:

"Announced today, The Metaverse Standards Forum brings together leading standards organizations and companies for industry-wide cooperation on interoperability standards needed to build the open metaverse. The Forum will explore where the lack of interoperability is holding back metaverse deployment and how the work of Standards Developing Organizations (SDOs) defining and evolving needed standards may be coordinated and accelerated. Open to any organization at no cost, the Forum will focus on pragmatic, action-based projects such as implementation prototyping, hackathons, plugfests, and open-source tooling to accelerate the testing and adoption of metaverse standards, while also developing consistent terminology and deployment guidelines."

This looks like it will be a useful project and community for the purposes outlined in this book, but the technology is young enough (in that it doesn't really exist) for multiple approaches to be trailed.

7.1.1 Primitives

OpenAI identified the following 5 points about metaverse, in response to the query "What are 5 key points I should know when studying metaverse?"

- Metaverse is a virtual reality platform that allows users to interact with each other and with digital objects in a virtual space.
- Metaverse is a decentralized platform, meaning that there is no central authority or server that controls the platform.
- Metaverse is an open platform, meaning that anyone can develop applications for the platform.
- Metaverse is a secure platform, meaning that all data and transactions are encrypted and secure.
- Metaverse is a scalable platform, meaning that it can support a large number of users and a large number of transactions.

This is an unexpectedly great answer, probably the cleanest we have found. The Metaverse Standard Forum highlights the following, which reads like the output from a brainstorm between academia and industry stakeholders.

- collaborative spatial computing
- interactive 3D graphics
- augmented and virtual reality
- photorealistic content authoring
- geospatial systems
- end-user content tooling
- digital twins
- real-time collaboration
- physical simulation
- online economies
- multi-user gaming
- new levels of scale and immersiveness.

It's not a useless list by any means, but it lacks the kind of product focus we need for detailed exploration of value and trust transfer.

Mystakidis identifies the following [114]:

- Principles
  - Interoperable
  - Open
  - Hardware agnostic
  - Network
- Technologies
  - Virtual reality
  - Augmented reality
  - Mixed reality
- Affordances
  - Immersive
  - Embodiment
  - Presence
  - Identity construction
- Challenges
  - Physical well-being
  - Psychology
  - Ethics
  - Privacy

This is quite an academic list. A lot of these words will be explored in the next section which is more of an academic literature review.

Nevelsteen attempted to identify key elements for a 'virtual work' in 2018 and these are relevant now, and described rigorously in the appendix of his paper [115]:

- Shared Temporality, meaning that the distributed users of the virtual world share the same frame of time.
- Real time which he defines as "not turn based".
- Shared Spatiality, which he says can include an 'allegory' of a space, as in text adventures. It seems this might extend to a spoken interface to a mixed reality metaverse.
- ONE Shard is a description of the WLAN network architecture, and conforms to servers in a connected open metaverse.
- Many human agents simply means that more than one person can be represented in the virtual world and corresponds to 'social' in our description.
- Many Software Agents corresponds to AI actors in our descriptions. Non playing characters would be the gaming equivalent.
- Virtual Interaction pertains to any ability of a user to interact actively with the persistent virtual scene, and is pretty much a given these days.
- Nonpausable isn't even a word, but is pretty self explanatory.
- Persistence means that if human participants leave then the data of the virtual world continues. This applies to the scenes, the data representing actions, and objects and actors in the worlds.
- Avatar is interesting as it might seem that having avatar representations of connected human participants is a given. In fact the shared spaces employed by Nvidia for digital engineering do not.

Turning to industry; John Riccitiello, CEO of Unity Technologies says that metaverse is *"The next generation of the internet that is:*

- *always real-time*

- *mostly 3D*
- *mostly interactive*
- *mostly social*
- *mostly persistent"*

Expanding this slightly we will us the following primitives of what we think are important for a metaverse:

- Fusing of digital and real life
- Social first
- Real time interactive 3d graphics first
- Persistent
- Supports ownership
- Supports user generated content [116]
- Open and extensible
- Low friction economic actors and actions
- Trusted / secure
- Convergence of film and games
- Blurring of IP boundaries
- Blurring of narrative flow
- Multimodal and hardware agnostic
- Mobile first experiences
- Safeguarding, and governance

There is a **lot** of work for the creative and technical industries to do to integrate human narrative creativity this nascent metaverse, and it's not even completely clear that this is possible, or even what people want.

7.2 History

The word metaverse was coined by the author Neal Stephenson in his 1992 novel Snowcrash. It started popping up soon after in news articles and research papers [117], but in the last five years it has been finding a new life within a silicon valley narrative.

There were clear precursors to modern social VR, such as VRML in the 1990's which laid much of the groundwork for 3D content over networked computers.

It might seem that there would be a clear path from there to now, in terms of a metaverse increasingly meaning connected social virtual spaces, but this has not happened. Instead interest in metaverse as a concept waned, MMORG (described later) filled in the utility, and then recently an entirely new definition emerged. Park and Kim surveyed dozens of different historical interpretations of the word, and the generational reboot they describe makes it even less clear [118]. The concept of the Metaverse is extremely plastic at this time (Figure 7.1).

It's arguable that what will be expanding in this chapter is more appropriately 'Cyberspace' as described by William Gibson in Neuromancer [119] *"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*

Park and Kim identify the generational inflection point which has led to the resurgence of the concept of Metaverse [118]: *"Unlike previous studies on the Metaverse based on Second Life, the current Metaverse is based on the social value of Generation Z that online*



Figure 7.1: Elon Musk agrees with this on Twitter. It's notable that Musk is now Twitters' biggest shareholder, and has been vocal about Web2 censorship on the platform.

and offine selves are not different."

The book will aim to build toward an understanding of metaverse as a useful social mixed reality, that allows low friction communication and economic activity, within groups, at a global scale. Cryptography and distributed software can assist us with globally 'true' persistence of digital data, so we will look to integrate this with our social XR. This focus on persistence, value, and trust means it's most appropriate to focus on business uses as there is more opportunity for value creation which will be important to bootstrap this technology.

This chapter will first attempt to frame the context for telepresence (the academic term for communicating through technology), and then explain the increasingly polarised options for metaverse. It's useful to precisely identify the primitives of the product we would like to see here, so this chapter is far more a review of academic literature in the field, culminating in a proposed framework.

7.3 Video conferencing, the status quo

Video-conferencing has become more popular as technology improves, as it gets better integrated with ubiquitous cloud business support suites, and as a function of the global pandemic and changing work patterns. There is obviously increasing demands for real-time communication across greater distances.

The full effects of video-conferencing on human communication are still being explored, as seen in the experimental "Together Mode" within Microsoft Teams. Video-conferencing is presumed to be a somewhat richer form of communication than email and telephone, but not quite as informative as face-to-face communication.

In this section we look at the influence of eye contact on communication and how video-conferencing mediates both verbal and non-verbal interactions. Facilitation of eye contact is a challenge that must be addressed so that video-conferencing can approach the rich interactions of face-to-face communication. This is an even bigger problem in the emerging metaverse systems, so it's important that we examine the history and trajectory.

There is a tension emerging for companies who do not necessarily need to employ remote meeting technology, but also cannot afford to ignore the competitive advantages

that such systems bring. In an experiment preformed well before the 2020 global pandemic at CTrip, Bloom et al describe how home working led to a 13% performance increase, of which about 9% was from working more minutes per shift (fewer breaks and sick-days) and 4% from more calls per minute (attributed to a quieter working environment) [120]. Home workers also reported improved work satisfaction and experienced less turnover, but their promotion rate conditional on performance fell. This speaks to a lack of management capability with such systemic change. It's clearly a complex and still barely understood change within business and management.

Due to the success of the experiment, CTrip rolled-out the option to work from home to the whole company, and allowed the experimental employees to re-select between the home or office. Interestingly, over half of them switched, which led to the gains almost doubling to 22%. This highlights the benefits of learning and selection effects when adopting modern management practices like working from home. Increasingly this is becoming a choice issue for prospective employees, and an advantage for hiring managers to be able to offer it.

More recent research by Barrero, Bloom and Davies found that working from home is likely to be "sticky" [121]. They found:

- better-than-expected WFH experiences,
- new investments in physical and human capital that enable WFH,
- greatly diminished stigma associated with WFH,
- lingering concerns about crowds and contagion risks,
- a pandemic-driven surge in technological innovations that support WFH.

More recently Enterprise Collaboration Systems (ECS) provide rich document management, sharing, and collaboration functionality across an organisation. The enterprise ECS system may integrate collaborative video [122]. This is for instance the case with Microsoft Teams / Sharepoint. This integration of ECS should be considered when thinking about social VR systems which wish to support business, value, and trust. It is very much the case that large technology providers are attempting to integrate their 'business back end' systems into their emerging metaverse systems. Open source equivalents are currently lacking.

7.3.1 Pandemic drives adoption

The ongoing global COVID-19 pandemic is changing how people work, toward a new global 'normal'. Some ways of working are overdue transformation, and will be naturally disrupted. In the UK at least it seems that there may be real appetite to shift away from old practises. This upheaval will inevitably present both challenges and opportunities.

Highly technical workforces, especially, can operate from anywhere. The post pandemic world seems to have stronger national border controls, with a resultant shortage of highly technical staff. This has forced the hand of global business toward internationally distributed teams.

If only a small percentage of companies allow the option of remote working, then they gain a structural advantage, enjoying benefits of reduced travel, lower workplace infection risk across all disease, and global agility for the personnel. Building and estate costs will certainly be reduced. More diversity may be possible. Issues such as sexual harassment and bullying may be reduced. With reduced overheads product quality may increase. If customers are happier with their services, then over time this 'push' may mean an enormous shift away from centralised working practises toward distributed working.

Technologies which support this working style were still in their infancy at the beginning of the pandemic. The rush to 'Zoom', a previously relatively unknown and insecure [123] web meeting product, shows how naive businesses were in this space.

Connection of multiple users is now far better supported, with Zoom and Mircosoft Teams alone supporting hundreds of millions of chats a day. This is a 20x increase on market leader Skype's 2013 figure of 280 million connections per month. Such technologies extend traditional telephony to provide important multi sensory cues. However, these technologies demonstrate shortfalls compared to a live face-to-face meeting, which is generally agreed to be optimal for human-human interaction [124].

While the research community and business are learning how to adapt working practises to web based telepresence [125], there remains little technology support for ad-hoc serendipitous meetings between small groups. It's possible that Metaverse applications can help to fill this gap, by gamification of social spaces, but the under discussed problems with video conferencing are likely to be even worse in such systems.

Chris Herd of "FirstBase" (who admittedly have a bias) provides some fascinating speculations:

"I've spoken to 2,000+ companies with 40M+ employees about remote work in the last 12 months A few predictions of what will happen before 2030:

- *Rural Living: World-class people will move to smaller cities, have a lower cost of living & higher quality of life.*
- *These regions must innovate quickly to attract that wealth. Better schools, faster internet connections are a must.*
- *Async Work: Offices are instantaneous gratification distraction factories where synchronous work makes it impossible to get stuff done.*
- *Tools that enable asynchronous work are the most important thing globally remote teams need. A lot of startups will try to tackle this.*
- *Hobbie Renaissance: Remote working will lead to a rise in people participating in hobbies and activities which link them to people in their local community.*
- *This will lead to deeper, more meaningful relationships which overcome societal issues of loneliness and isolation.*
- *Diversity & Inclusion: The most diverse and inclusive teams in history will emerge rapidly Companies who embrace it have a first-mover advantage to attract great talent globally. Companies who don't will lose their best people to their biggest competitors.*
- *Output Focus: Time will be replaced as the main KPI for judging performance by productivity and output.*
- *Great workers will be the ones who deliver what they promise consistently*
- *Advancement decisions will be decided by capability rather than who you drink beer with after work.*
- *Private Equity: The hottest trend of the next decade for private equity will see them purchase companies, make them remote-first The cost saving in real-estate at scale will be eye-watering. The productivity gains will be the final nail in the coffin for the office Working Too Much: Companies worry that the workers won't work enough when operating remotely.*
- *The opposite will be true and become a big problem.*
- *Remote workers burning out because they work too much will have to be addressed.*
- *Remote Retreats: Purpose-built destinations that allow for entire companies to fly*

into a campus for a synchronous week.
- *Likely staffed with facilitators and educators who train staff on how to maximize effectiveness.*
- *Life-Work Balance: The rise of remote will lead to people re-prioritizing what is important to them.*
- *Organizing your work around your life will be the first noticeable switch. People realizing they are more than their job will lead to deeper purpose in other areas.*
- *Bullshit Tasks: The need to pad out your 8 hour day will evaporate, replaced by clear tasks and responsibilities.*
- *Workers will do what needs to be done rather than wasting their trying to look busy with the rest of the office*

”

7.3.2 Point to Point Video Conferencing

O'Malley et al. showed that face-to-face and video mediated employed visual cues for mutual understanding, and that addition of video to the audio channel aided confidence and mutual understanding. However, video mediated did not provide the clear cues of being co-located [126].

Dourish et al. make a case for not using face-to-face as a baseline for comparison, but rather that analysis of the efficacy of remote tele-collaboration tools should be made in a wider context of connected multimedia tools and 'emergent communicative practises' [127]. While this is an interesting viewpoint it does not necessarily map well to a recreation of the ad-hoc meeting.

There is established literature on human sensitivity to eye contact in both 2D and 3D VC [128, 129], with an accepted minimum of 5-10 degrees before observers can reliably sense they are not being looked at [130]. Roberts et al. suggested that at the limit of social gaze distance (4m) the maximum angular separation between people standing shoulder to shoulder in the real world would be around 4 degrees[131].

Sellen found limited impact on turn passing when adding a visual channel to audio between two people when using Hydra, an early system which provided multiple video conference displays in an intuitive spatial distribution[132]. She did however, find that the design of the video system affected the ability to hold multi-party conversations [133].

Monk and Gale describe in detail experiments which they used for examining gaze awareness in communication which is mediated and unmediated by technology. They found that gaze awareness increased message understanding [134].

Both Kuster et al. and Gemmel et al. have successfuly demonstrated software systems which can adjust eye gaze to correct for off axis capture in real time video systems[135, 136].

Shahid et al. conducted a study on pairs of children playing games with and without video mediation and concluded that the availability of mutual gaze affordance enriched social presence and fun, while its absence dramatically affects the quality of the interaction. They used the 'Networked Minds', a social presence questionnaire.

7.3.3 Triadic and Small Group

Early enthusiasm in the 1970's for video conferencing, as a medium for small group interaction quickly turned to disillusionment. It was agreed after a flurry of initial research

that the systems at the time offered no particular advantage over audio only communication, and at considerable cost [137].

Something in the breakdown of normal visual cues seems to impact the ability of the technology to support flowing group interaction. Nonetheless, some non-verbal communication is supported in VC with limited success.

Additional screens and cameras can partially overcome the limitation of no multi-party support (that of addressing a room full of people on a single screen) by making available more bidirectional channels. For instance, every remote user can be a head on a screen with a corresponding camera. The positioning of the screens must then necessarily match the physical organization of the remote room.

Egido provides an early review of the failure of VC for group activity, with the "misrepresentation of the technology as a substitute for face-to-face" still being valid today [138].

Commercial systems such as Cisco Telepresence Rooms cluster their cameras above the centre screen of three for meetings using their telecollaboration product, while admitting that this only works well for the central seat of the three screens. They also group multiple people on a single screen in what Workhoven et al. dub a "non-isotropic" configuration [139]. They maintain that this is a suitable trade off as the focus of the meeting is more generally toward the important contributor in the central seat. This does not necessarily follow for less formal meeting paradigms.

In small groups, it is more difficult to align non-verbal cues between all parties, and at the same time, it is more important because the hand-offs between parties are more numerous and important in groups. A breakdown in conversational flow in such circumstances is harder to solve. A perception of the next person to talk must be resolved for all parties and agreed upon to some extent.

However, most of the conventional single camera, and expensive multi camera VC systems, suffer a fundamental limitation in that the offset between the camera sight lines and the lines of actual sight introduce incongruities that the brain must compensate for [124].

7.3.4 Other Systems to Support Business

There have been many attempts to support group working and rich data sharing between dispersed groups in a business setting. So called 'smart spaces' allow interaction with different displays for different activities and add in some ability to communicate with remote or even mobile collaborators on shared documents [140], with additional challenges for multi-disciplinary groups who are perhaps less familiar with one or more of the technology barriers involved [141].

Early systems like clearboard [142] demonstrated the potential for smart whiteboards with a webcam component for peer-to-peer collaborative working. Indeed it is possible to support this modality with Skype and a smartboard system (and up to deployments such as Accessgrid). They remain relatively unpopular however.

7.3.5 Mona Lisa Type Effects

Almost all traditional group video meeting tools suffer from the so-called Mona Lisa effect which describes the phenomenon where the apparent gaze of a portrait or 2 dimensional image always appears to look at the observer regardless of the observer's position [143,

144, 145]. This situation manifests when the painted or imaged subject is looking into the camera or at the eyes of the painter [146, 147].

Single user-to-user systems based around bidirectional video implicitly align the user's gaze by constraining the camera to roughly the same location as the display. When viewed away from this ideal axis, it creates the feeling of being looked at regardless of where this observer is [148, 143, 144, 145], or the "collapsed view effect" [149] where perception of gaze transmitted from a 2 dimensional image or video is dependent on the incidence of originating gaze to the transmission medium.

Multiple individuals using one such channel can feel as if they are being looked at simultaneously, leading to a breakdown in the normal non-verbal communication which mediates turn passing [150]. There is research investigating this sensitivity when the gaze is mediated by a technology, finding that "disparity between the optical axis of the camera and the looking direction of a looker should be at most 1.2 degrees in the horizontal direction, and 1.7 degrees in vertical direction to support eye contact" [129, 151]. It seems that humans assume that they are being looked at unless they are sure that they are not [130].

To be clear, there are technological solutions to this problem, but it's useful in the context of discussing metaverse to know that this problem exists. It's known that there are cognitive dissonances around panes of video conference images, but it seems that the effect is truely limited to 2D surfaces. A 3D projection surface (a physical model of a human) designed to address this problem completely removed the Mona Lisa effect [148].

Metaverse then perhaps offers the promise of solving this, making more natural interaction possible, but it's clearly a long way from delivering on those promises right now. We need to understand what's important and try to map these into a metaverse product.

7.4 What's important for human communication

7.4.1 Vocal

The ubiquitous technology to mediate conversation is, of course, the telephone. The 2021 Ericsson mobility report states that there are around 8 billion mobile subscriptions globally. More people have access to mobile phones than to working toilets according to UNICEF.

Joupii and Pan designed a system which focused attention on spatially correct high definition audio. They found "significant improvement over traditional audio conferencing technology, primarily due to the increased dynamic range and directionality. [152]. Aoki et al. also describe an audio only system with support for spatial cues [153].

In the following sections we will attempt to rigorously identify just what is important for our proposed application of business centric communication, supportive of trust, and thereby value transfer.

In his book 'Bodily Communication' [154] Michael Argyle divides vocal signals into the following categories:

1. Verbal
2. Non-Verbal Vocalisations
    a. Linked to Speech
        i. Prosodic
        ii. Synchronising
        iii. Speech Disturbances
    b. Independent of Speech

i. Emotional Noises
ii. Paralinguistic (emotion and interpersonal attitudes)
iii. Personal voice and quality of accent

Additional to the semantic content of verbal communication there is a rich layer of meaning in pauses, gaps, and overlaps [155] which help to mediate who is speaking and who is listening in multi-party conversation. This mediation of turn passing, to facilitate flow, is by no means a given and is highly dependent on context and other factors [156]. Interruptions are also a major factor in turn passing.

This extra-verbal content [157] extends into physical cues, so-called 'nonverbal' cues, and there are utterances which link the verbal and non-verbal [158]. This will be discussed later, but to an extent, it is impossible to discuss verbal communication without regard to the implicit support which exists around the words themselves.

In the context of all technology-mediated conversation the extra-verbal is easily compromised if technology used to support communication over a distance does not convey the information, or conveys it badly. This can introduce additional complexity [158].

These support structures are pretty much lacking in metaverse XR systems. The goal then here perhaps is to examine the state-of-the-art, and remove as many of the known barriers as possible. Such a process might better support trust, which might better support the kind of economic and activity we seek to engineer.

When examining just verbal / audio communication technology it can be assumed that the physical non-verbal cues are lost, though not necessarily unused. In the absence of non-verbal cues it falls to timely vocal signals to take up the slack when framing and organising the turn passing. For the synchronising of vocal signals between the parties to be effective the systemic delays must remain small. System latency, the inherent delays added by the communication technology, can allow slips or a complete breakdown of 'flow' [159]. This problem can be felt in current social VR platforms, though people don't necessarily identify the cause of the breakdown correctly. In the main they feel to the users like a bad "audio-only" teleconference.

With that said, the transmission of verbal / audio remains the most critical element for interpersonal communication as the most essential meaning is encoded semantically. There is a debate about ratios of how much information is conveyed through the various human channels [160], but it is reasonable to infer from its ubiquity that support for audio is essential for meaningful communication over a distance. We have seen that it must be timely, to prevent a breakdown of framing, and preferably have sufficient fidelity to convey sub-vocal utterances.

For social immersive VR for business users, a real-time network such as websockets, RTP, or UDP seems essential, much better microphones are important, and the system should support both angular spatialisation, and respond to distance between interlocutors.

7.4.2 Nonverbal

We have already seen that verbal exchanges take place in a wider context of sub vocal and physical cues. In addition, the spatial relationship between the parties, their focus of attention, their gestures and actions, and the wider context of their environment all play a part in communication [161]. These are identified as follows by Gillies and Slater [162] in their paper on virtual agents.

- Posture and gesture
- Facial expression

- Gaze
- Proxemics
- Head position and orientation
- Interactional synchrony

This is clearly important for our proposed metaverse application. Below we will examine these six areas by looking across the wider available research.

7.4.2.1 Gaze

Of particular importance is judgement of eye gaze which is normally fast, accurate and automatic, operating at multiple levels of cognition through multiple cues [154, 163, 164, 163, 165, 166, 134].

Gaze in particular aids smooth turn passing [167] [168] and lack of support for eye gaze has been found to decrease the efficiency of turn passing by 25% [169].

There are clear patterns to eye gaze in groups, with the person talking, or being talked to, probably also being looked at [170] [171]. To facilitate this groups will tend to position themselves to maximally enable observation of the gaze of the other parties [166]. This intersects with proxemics which will be discussed shortly. In general people look most when they are listening, with short glances of 3-10 seconds [164]. Colburn et al. suggest that gaze direction and the perception of the gaze of others directly impacts social cognition [172] and this has been supported in a follow up study [173].

The importance of gaze is clearly so significant in evolutionary terms that human acuity for eye direction is considered high at 30 sec arc [174] with straight binocular gaze judged more accurately than straight monocular gaze [175], when using stereo vision.

Regarding the judgement of the gaze of others, Symons et al. suggested that "people are remarkably sensitive to shifts in a person's eye gaze" in triadic conversation [174]. This perception of the gaze of others operates at a low level and is automatic. Langton et al. cite research stating that the gaze of others is "able to trigger reflexive shifts of an observer's visual attention" and further discuss the deep biological underpinnings of gaze processing [171].

When discussing technology-mediated systems, Vertegaal & Ding suggested that understanding the effects of gaze on triadic conversation is "crucial for the design of teleconferencing systems and collaborative virtual environments" [150], and further found correlation between the amount of gaze, and amount of speech. Vertegaal & Slagter suggest that "gaze function(s) as an indicator of conversational attention in multiparty conversations" [170]. It seems like is we are to have useful markets within social immersive environments then support for natural gaze effects should be a priority.

Wilson et al. found that subjects can "discriminate gaze focused on adjacent faces up to [3.5m]" [176]. This perhaps gives us a testable benchmark within a metaverse application which is eye gaze enabled. In this regard Schrammel et al. investigated to what extent embodied agents can elicit the same responses in eye gaze detection [177].

Vertegaal et al. found that task performace was 46% better when gaze was synchronised in their telepresence scenario. As they point out, gaze synchonisation (temporal and spatial) is 'commendable' in all such group situations, but the precise utility will depend upon the task [150].

There has been some success in the automatic detection of the focus of attention of participants in multi party meetings [178, 179]. More recently, eye tracking technologies allow the recording and replaying of accurate eye gaze information [180] alongside

information about pupil dilation toward determination of honesty and social presence [181]. It seems there are trust and honesty issues conflated with how collaborants in a virtual space are represented.

In summary, gaze awareness does not just mediate verbal communication but rather is a complex channel of communication in its own right. Importantly, gaze has a controlling impact on those who are involved in the communication at any one time, including and excluding even beyond the current participants. Perhaps the systems we propose in this book need to demand eye gaze support, but it is clear that it should be recommended, and that the software selected should support the technology integration in principle.

7.4.2.2 Mutual Gaze

Aygyle and Cook established early work around gaze and mutual gaze, with their seminal book of the same title [163], additionally detailing confounding factors around limitations and inaccuracies in observance of gaze and how this varies with distance [165, 154, 182].

Mutual gaze is considered to be the most sophisticated form of gaze awareness with significant impact on dyadic conversation especially [182, 156, 183]. The effects seem more profound than just helping to mediate flow and attention, with mutual eye gaze aiding in memory recall and the formation of impressions [184].

While reconnection of mutual eye gaze through a technology boundary does not seem completely necessary it is potentially important, with impact on subtle elements of one-to-one communication, and therefore discrimination of eye gaze direction should be bi-directional if possible, and if possible have sufficient accuracy to judge direct eye contact. In their review Bohannon et al. said that the issue of rejoining eye contact must be addressed in order to fully realise the richness of simulating face-to-face encounters [184].

Mutual gaze is a challenging affordance as bi-directional connection of gaze is not a trivial problem. It's perhaps best to view this as at the 'edge' of our requirements for a metaverse.

7.4.2.3 Mutual Gaze in Telepresence

We have seen that transmission of attention can broadly impact communication in subtle ways, impacting empathy, trust, cognition, and co-working patterns. Mutual gaze (looking into one another's eyes), is currently the high water mark for technology-mediated conversation.

Many attempts have been made to re-unite mutual eye gaze when using tele-conferencing systems. In their 2015 review of approaches Regenbrecht and Langlotz found that none of the methods they examined were completely ideal [185]. They found most promise in 2D and 3D interpolation techniques, which will be discussed in detail later, but they opined that such systems were very much ongoing research and lacked sufficient optimisation.

A popular approach uses the so called 'Peppers Ghost' phenomenon [186], where a semi silvered mirror presents an image to the eye of the observer, but allows a camera to view through from behind the angled mirror surface. The earliest example of this is Rosental's two way television system in 1947 [187], though Buxton et al. 'Reciprocal Video Tunnel' from 1992 is more often cited [188]. This optical characteristic isn't supported by retroreflective projection technology, and besides requires careful control of light levels either side of the semi-silvered surface.

The early GAZE-2 system (which makes use of Pepper's ghost) is novel in that it uses an eye tracker to select the correct camera from several trained on the remote user. This ensures that the correct returned gaze (within the ability of the system) is returned

to the correct user on the other end of the network [189]. Mutual gaze capability is later highlighted as an affordance supported or unsupported by key research and commercial systems.

7.4.2.4 Head Orientation

Orientation of the head (judged by the breaking of bilateral symmetry and alignment of nose) is a key factor when judging attention. Perception of head orientation can be judged to within a couple of degrees [176].

It has been established that head gaze can be detected all the way out to the extremis of peripheral vision, with accurate eye gaze assessment only achievable in central vision [146]. This is less of use for our metaverses at this time, because user field of view is almost always restricted in such systems. More usefully, features of illumination can alter the apparent orientation of the head [190].

Head motion over head orientation is a more nuanced propostion and can be considered a micro gesture [191]. Head tracking systems within head mounted displays can certainly detect these tiny movements, but it's clear that not all of this resolution is passed into shared virtual settings through avatars. It would be beneficial to be able to fine tune this feature within any software selected.

It is possible that 3D displays are better suited to perception of head gaze since it is suggested that they are more suitable for "shape understanding tasks" [192]

Bailenson, Baell, and Blascovich found that giving avatars rendered head movements in a shared virtual environment decreased the amount of talking, possibly as the extra channel of head gaze was opened up. They also reported that subjectively, communication was enhanced [193].

Clearly head orientation is an important indicator of the direction of attention of members of a group and can be discerned even in peripheral vision. This allows the focus of several parties to be followed simultaneously and is an important affordance to replicate on any multi-party communication system.

7.4.2.5 Combined Head and Eye Gaze

Rienks et al. found that head orientation alone does not provide a reliable cue for identification of the speaker in a multiparty setting [194]. Stiefelhagen & Zhu found "that head orientation contributes 68.9% to the overall gaze direction on average" [179], though head and eye gaze seem to be judged interdependently [175]. Langton noted that head and eye gaze are "mutually influential in the analysis of social attention" [171], and it is clear that transmission of 'head gaze' by any mediating system, enhances rather than replaces timely detection of subtle cues. Combined head and eye gaze give the best of both worlds and extend the lateral field of view in which attention can be reliably conveyed to others [146].

7.4.2.6 Other Upper Body: Overview

While it is well evidenced that there are advantages to accurate connection of the gaze between conversational partners [165, 156], there is also a body of evidence that physical communication channels extend beyond the face [156, 195] and include both micro (shrugs, hands and arms), and macro movement of the upper body [196]. Goldin-Meadow suggests that gesturing aids conversational flow by resolving mismatches and aiding cognition [197].

In their technology-mediated experiment which compared face to upper body and face on a flat screen, Nguyen and Canny found that "upper-body framing improves empathy

measures and gives results not significantly different from face-to-face under several empathy measures" [195].

The upper body can be broken up as follows:

Facial

Much emotional context can be described by facial expression (display) alone [196, 198], with smooth transition between expressions seemingly important [199]. This suggests that mediating technologies should support high temporal resolution, or at least that there is a minimum resolution between which transitions between expressions become too 'categorical'. Some aspects of conversational flow appear to be mediated in part by facial expression [200]. There are gender differences in the perception of facial affect [201].

Gesturing

(such as pointing at objects) paves the way for more complex channels of human communication and is a basic and ubiquitous channel [202]. Conversational hand gestures provide a powerful additional augmentation to verbal content [203].

Posture

Some emotions can be conveyed through upper body configurations alone. Argyle details some of these [154] and makes reference to the posture of the body and the arrangement of the arms (i.e. folded across the chest). These are clearly important cues. Kleinsmith and Bianchi-Berthouze assert that "some affective expressions may be better communicated by the body than the face" [204].

Body Torque

In multi-party conversation, body torque, that is the rotation of the trunk from front facing, can convey aspects of attention and focus [205].

In summary, visual cues which manifest on the upper body and face can convey meaning, mediate conversation, direct attention, and augment verbal utterances.

7.4.2.7 Effect of Shared Objects on Gaze

Ou et al. detail shared task eye gaze behaviour "in which helpers seek visual evidence for workers' understanding when they lack confidence of that understanding, either from a shared, or common vocabulary" [206].

Murray et al. found that in virtual environments, eye gaze is crucial for discerning what a subject is looking at [207]. This work is shown in Figure 7.2.

It is established that conversation around a shared object or task, especially a complex one, mitigates gaze between parties [163] and this suggests that in some situations around shared tasks in metaverses it may be appropriate to reduce fidelity of representation of the avatars.

7.4.2.8 Tabletop and Shared Task

In early telepresence research Buxton and William argued through examples that "effective telepresence depends on quality sharing of both person and task space [188].

In their triadic shared virtual workspace Tang et al. found difficulty in reading shared text using a 'round the table' configuration, a marked preference for working collaboratively on the same side of the table. They also found additional confusion as to the identity of remote participants [208]. Tse et al. found that pairs can work well over a shared digital tabletop, successfully overcoming a single user interface to interleave tasks [209].

Tang et al. demonstrate that collaborators engage and disengage around a group activity through several distinct, recognizable mechanisms with unique characteristics [210]. They state that tabletop interfaces should offer a variety of tools to facilitate this fluidity.

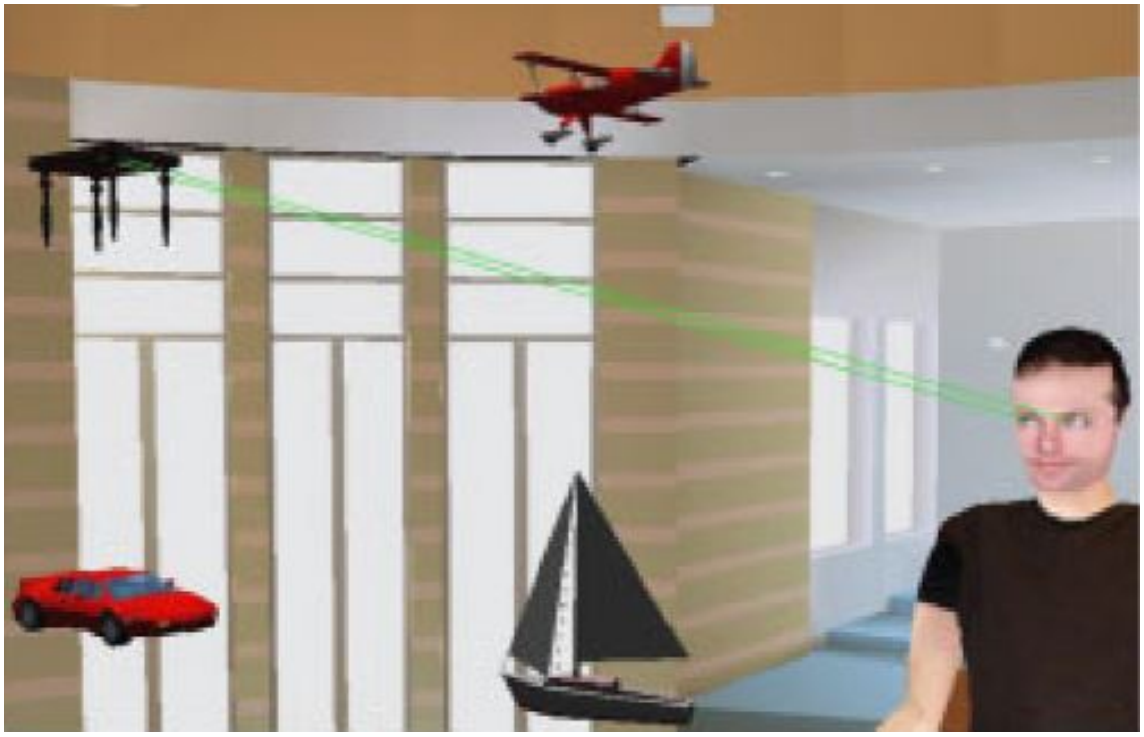


Figure 7.2: Eye tracked eye gaze awareness in VR. Murray et al. used immersive and semi immersive systems alongside eye trackers to examine the ability of two avatars to detect the gaze awareness of a similarly immersed collaborator.

Camblend is a shared workspace with panoramic high resolution video. It maintains some spatial cues between locations by keeping a shared object in the video feeds [211, 212]. Participants successfully resolved co-orientation within the system.

The t-room system implemented by Luff et al. surrounds co-located participants standing at a shared digital table with life sized body and head video representations of remote collaborators [213] but found that there were incongruities in the spatial and temporal matching between the collaborators which broke the flow of conversation. Tuddenham et al. found that co-located collaborators naturally devolved 'territory' of working when sharing a task space, and that this did not happen the same way with a tele-present collaborator [214]. Instead remote collaboration adapted to use a patchwork of ownership of a shared task. It seems obvious to say that task ownership is a function of working space, but it is interesting that the research found no measurable difference in performance when the patchwork coping strategy was employed.

The nature of a shared collaborative task and/or interface directly impacts the style of interaction between collaborators. This will have a bearing on the choice of task for experimentation [215, 216].

7.5 Psychology of Technology-Mediated Interaction

7.5.1 Proxemics

Proxemics is the formal study of the regions of interpersonal space begun in the late 50's by Hall and Sommers and building toward The Hidden Dimension [217], which details bands of space (Figure 7.3) that are implicitly and instinctively created by humans and

which have a direct bearing on communication. Distance between conversational partners,

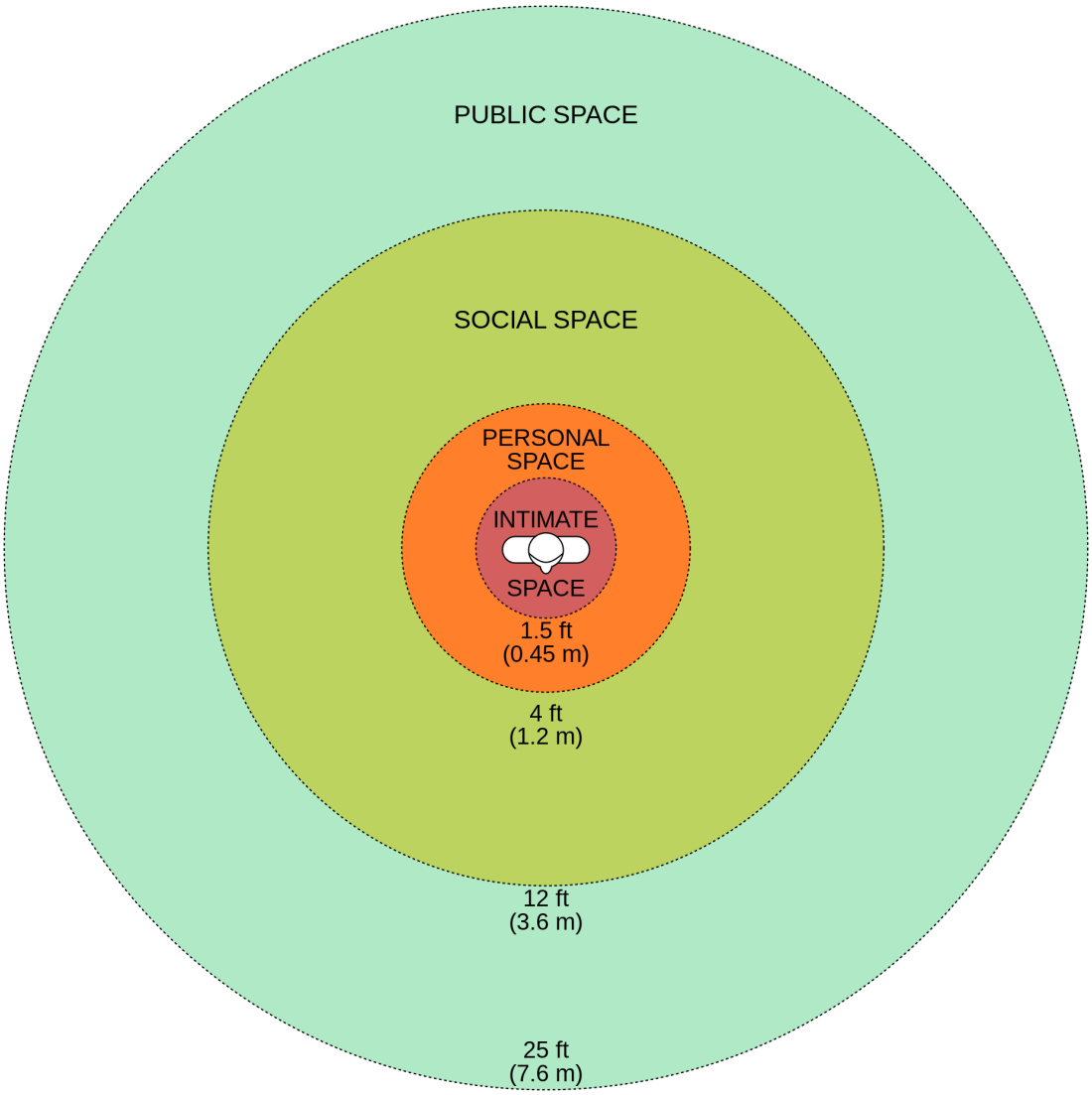


Figure 7.3: Bands of social space around a person Image CC0 from wikipedia.

and affiliation, also have a bearing on the level of eye contact [164] with a natural distance equilibrium being established and developed throughout, through both eye contact and a variety of subtle factors. Argyle & Ingham provide levels of expected gaze and mutual gaze against distance [165]. These boundaries are altered by ethnicity [218, 154] and somewhat by gender [219], and age [220, 201].

Even with significant abstraction by communication systems (such as SecondLife) social norms around personal space persist [221, 222, 223]. Bailenson & Blascovich found that even in Immersive Collaborative Virtual Environments (ICVE's) "participants respected personal space of the humanoid representation"[222] implying that this is a deeply held 'low-level' psychophysical reaction [224]. The degree to which this applies to non-humanoid avatars seems under explored.

Maeda et al. [225] found that seating position impacts the level of engagement in teleconferencing. Taken together with the potential for reconfiguration within the group as

well as perhaps signalling for the attention of participants outside of the confines of the group in an open business metaverse setting.

When considering the attention of engaging with people outside the confines of a meeting Hager et al. found that gross expressions can be resolved by humans over long distances [226, 154]. It seems that social interaction begins around 7.5m in the so-called 'public space' [217]. Recreating this affordance in a metaverse would be a function of the display resolution, and seems another 'stretch goal' rather than a core requirement.

7.5.2 Attention

The study of attention is a discrete branch of psychology. It is the study of cognitive selection toward a subjective or objective sub focus, to the relative exclusion of other stimulae. It has been defined as "a range of neural operations that selectively enhance processing of information" [227]. In the context of interpersonal communication it can be refined to apply to selectively favouring a conversational agent or object or task above other stimuli in the contextual frame.

Humans can readily determine the focus of attention of others in their space [178] and preservation of the spatial cues which support this are important for technology-mediated communication [132] [179].

The interplay between conversational partners, especially the reciprocal perception of attention, is dubbed the perceptual crossing [228, 229].

This is a complex field of study with gender, age, and ethnicity all impacting the behaviour of interpersonal attention [230, 220, 154, 201, 231]. Vertegaal has done a great deal of work on awareness and attention in technology-mediated situations and the work of his group is cited throughout this chapter [232]. As an example it is still such a challenge to "get" attention through mediated channels of communication, that some research [233, 132] and many commercial systems such as 'blackboard collaborate', Zoom, and Teams use tell tale signals (such as a microphone icon) to indicate when a participant is actively contributing. Some are automatic, but many are still manual, requiring that a user effectively hold up a virtual hand to signal their wish to communicate.

Langton et al. cite research stating that the gaze of others is "able to trigger reflexive shifts of an observer's visual attention".

Regarding the attention of others, Fagal et el demonstrated that eye visibility impacts collaborative task performance when considering a shared task [183]. Novick et al. performed analysis on task hand-off gaze patterns which is useful for extension into shared task product design [168].

7.5.3 Behaviour

Hedge et al. suggested that gaze interactions between strangers and friends may be different which could have an impact on the kinds of interactions a metaverse might best support [167]. Voida et al. elaborate that prior relationships can cause "internal fault lines" in group working [234]. When new relationships are formed the "primary concern is one of uncertainty reduction or increasing predictability about the behaviour of both themselves and others in the interaction" [235]. This concept of smoothness in the conversation is a recurring theme, with better engineered systems introducing less extraneous artefacts into the communication, and so disturbing the flow less. Immersive metaverse are rife with artefacts.

In a similar vein the actor-observer effect describes the mismatch between expectations which can creep into conversation. Conversations mediated by technology can be especially prone to diverging perceptions of the causes of behaviour [236]. Basically this means misunderstandings happen, and are harder to resolve with more mediating technology.

Interacting subjects progress conversation through so-called 'perception-action' loops which are open to predictive modelling through discrete hidden Markov models [237]. This might allow product OKR testing of the effectiveness of engineered systems [238].

It may be that the perception-behaviour link where unconscious mirroring of posture bolsters empathy between conversational partners, especially when working collaboratively [239], and the extent to which posture is represented through a communication medium may be important.

Landsberger posited the Hawthorne effect [240]. Put simply this is a short term increase in productivity that may occur as a result of being watched or appreciated. The impression of being watched changes gaze patterns during experimentation, with even implied observation through an eye tracker modifying behaviour [241].

There are also some fascinating findings around the neural correlates of gratitude, which turn out not to be linked to gratitude felt by a participant, but rather the observation of gratitude received within a social context [242]. These findings have potentially useful implications for the behaviours of AI actors and avatars within an immersive social scene.

There is much historic work describing "the anatomy of cooperation" [243], and this might better inform how educational or instructional tasks are built in metaverse applications.

Cuddihy and Walters defined an early model for assessing desktop interaction mechanisms for social virtual environments [244].

7.5.3.1 Perception Of Honesty

Hancock et al. state that we are most likely to lie, and to be lied to, on the telephone [245]. Technology used for communication impacts interpersonal honesty. It seems that at some level humans know this; lack of eye contact leads to feelings of deception, impacting trust [246]. This has a major impact on immersive social XR, which often does not support mutual gaze. Trust is crucial for business interactions.

Further there are universal expressions, micro-expressions, and blink rate which can betray hidden emotions [247], though the effects are subtle and there is a general lack of awareness by humans of their abilities in this regard [246]. Absence of support for such instinctive cues inhibits trust [248]. Support for these rapid and transient facial features demands high resolution reproduction in both resolution and time domains. There is detectable difference in a participant's ability to detect deception when between video conference mediated communication and that mediated by avatars [181]. Systems should aim for maximally faithful reproduction.

7.5.4 Presence, Co-presence, and Social Presence

Presence is a heavily cited historic indicator of engagement in virtual reality, though the precise meaning has been interpreted differently by different specialisms [249, 250]. It is generally agreed to be the 'sense of being' in a virtual environment [251]. Slater extends this to include the "extent to which the VE becomes dominant".

Beck et al. reviewed 108 articles and synthesised an ontology of presence [249] which at its simplest is as follows:

1. Sentient presence
    a. Physical interaction
    b. Mental interaction
2. Non-sentient
    a. Physical immersion
    b. Mental immersion = psychological state

When presence is applied to interaction it may be split into Telepresence, and Co/Social presence [252, 253]. Co-presence and/or social presence is the sense of "being there with another", and describes the automatic responses to complex social cues [254, 255]. Social presence (and co-presence) refers in this research context to social presence which is mediated by technology (even extending to text based chat [256]), and has its foundations in psychological mechanisms which engender mutualism in the 'real'. This is analysed in depth by Nowak [257]. An examination of telepresence, co-presence and social presence necessarily revisits some of the knowledge already elaborated.

The boundaries between the three are blurred in research with conflicting results presented [258]. Biocca et al. attempted to enumerate the different levels and interpretations surrounding these vague words [259], and to distill them into a more robust theory which better lends itself to measurement. They suggest a solid understanding of the surrounding psychological requirements which need support in a mediated setting, and then a scope that is detailed and limited to the mediated situation.

Since 'social presence' has been subject to varied definitions [259] it is useful here to consider a single definition from the literature which defines it as "the ability of participants in the community of inquiry to project their personal characteristics into the community, thereby presenting themselves to the other participants as real people." [260, 249]. Similarly to specifically define co-presence for this research it is taken to be the degree to which participants in a virtual environment are "accesible, available, and subject to one another" [259].

Social presence has received much attention and there are established questionnaires used in the field for measurement of the levels of perceived social presence yet the definitions here also remain broad, with some confusion about what is being measured [259].

Telepresence meanwhile is interaction with a different (usually remote) environment which may or may not be virtual, and may or may not contain a separate social/co-presence component.

Even in simple videoconferencing Bondareva and Bouwhuis stated (as part of an experimental design) that the following determinants are important to create social presence [261, 152].

1. Direct eye contact is preserved
2. Wide visual field
3. Both remote participants appear life size
4. Possibility for participants to see the upper body of the interlocutor
5. High quality image and correct colour reproduction
6. Audio with high S/N ratio
7. Directional sound field
8. Minimization of the video and audio signal asynchrony
9. Availability of a shared working space.

Bondareva et al. went on to describe a person-to-person telepresence system with a

semi-silvered mirror to reconnect eye gaze, which they claimed increased social presence indicators. Interestingly they chose a checklist of interpersonal interactions which they used against recordings of conversations through the system [261].

The idea of social presence as an indicator of the efficacy of the system, suggests the use of social presence questionnaires in the evaluation of the system [259]. Subjective questionnaires are however troublesome in measuring effectiveness of virtual agents and embodiments, with even nonsensical questions producing seemingly valid results [262]. Usoh et al. found that 'the real' produced only marginally higher presence results than the virtual [263]. It would be difficult to test products this way.

Nowak states that "A satisfactory level of co-presence with another mind can be achieved with conscious awareness that the interaction is mediated" and asserts that while the mediation may influence the degree of co-presence it is not a prohibiting factor [257].

Baren and IJsselsteijn [264, 265] list 20 useful presence questionnaires in 2004 of which "Networked Minds" seemed most appropriate for the research. Hauber et al. employed the "Networked Minds" Social Presence questionnaire experimentally and found that while the measure could successfully discriminate between triadic conversation that is mediated or unmediated by technology, it could not find a difference between 2D and 3D mediated interfaces [266, 256].

In summary, social presence and co-presence are important historic measures of the efficacy of a communication system. Use of the term in literature peaked between 1999 and 2006 according to Google's ngram viewer and has been slowly falling off since. The questionnaire methodology has been challenged in recent research and while more objective measurement may be appropriate, the networked minds questions seem to be able to differentiate real from virtual interactions [265].

7.6 Other Systems to Support Business

There have been many attempts to support group working and rich data sharing between dispersed groups in a business setting. So called 'smart spaces' allow interaction with different displays for different activities and add in some ability to communicate with remote or even mobile collaborators on shared documents [140], with additional challenges for multi-disciplinary groups who are perhaps less familiar with one or more of the technology barriers involved [141].

Early systems like clearboard [142] demonstrated the potential for smart whiteboards with a webcam component for peer to peer collaborative working. Indeed it is possible to support this modality with Skype and a smartboard system (and up to deployments such as Accessgrid). They remain relatively unpopular however.

Displays need not be limited to 2 dimensional screens and can be enhanced in various ways.

Stereoscopy allows an illusion of depth to be added to a 2D image by exploiting the stereo depth processing characteristics of the human vision system. This technical approach is not perfect as it does not fully recreate the convergence and focus expected by the eyes and brain.

There are multiple approaches to separating the left and right eye images, these primarily being active (where a signal selectively blanks the input to left then right eyes in synchronicity with the display), passive, where either selective spectrum or selective polarisation of light allow different portions of a display access to different eyes, or physical

arrangements which present different displays (or slices of light as in lenticular systems) to different eyes.

These barrier stereoscopy / lenticular displays use vertical light barriers built into the display to create multiple discrete channels of display which are accessed by moving horizontally with respect to the display. In this way it is possible to generate either a left/right eye image pair for 'autostereoscopic' viewing, or with the addition of head tracking and small motors. With these techniques multiple viewpoint or an adaptive realtime viewpoint update can be presented without the glasses required for active or passive stereoscopic systems.

7.6.1 Spatially Faithful Group

Hauber et al. combined videoconferencing, tabletop, and social presence analysis and tested the addition of 3D. They found a nuanced response when comparing 2D and 3D approaches to spatiality: 3D showed improved presence over 2D (chiefly through gaze support), while 2D demonstrated improved task performance because of task focus [267].

I3DVC reconstructs participants from multiple cameras and places them isotropically (spatially faithful) [268, 269]. The system uses a large projection screen, a custom table, and carefully defined seating positions. They discussed an "extended perception space" which used identical equipment in the remote spaces in a tightly coupled collaborative 'booth'. It employed head tracking and multi camera reconstruction alongside large screens built into the booth. This system exemplified the physical restrictions which are required to limit the problems of looking into another space through the screen. Fuchs et al. demonstrated a similar system over a wide area network but achieved only limited resolution and frame rate with the technology of the day [270].

University of Southern California used a technically demanding real-time set-up with 3D face scanning and an autostereoscopic 3D display to generate multiple 'face tracked' viewpoints [271]. This had the disadvantage of displaying a disembodied head.

MAJIC is an early comparable system to support small groups with life size spatially correct video, but without multiple viewpoints onto the remote collaborators it was a one to 'some' system rather than 'some' to one. Additionally users were rooted to defined locations [272, 273].

There seems to be less interest recently in large display screens for spatially correct viewpoints between groups. The hardware is technically demanding and there may have been sufficient research done to limit investment in research questions. This doesn't mean that there is no future for metaverse applications. Imagine one of the new XR studio walls such as that used to film the Mandalorian. With application of telepresence research it would be possible to bring external metaverse participants into the 'backstage' virtual scene. These avatars would be able to explore the scene invisible to the actors, but could be given access to visual feeds from the stage side. This is a hybrid virtual/real metaverse with a well researched and understood boundary interface. It would be possible to give different access privileges to different levels of paying 'film studio tourist' or investor, with VIPs perhaps commanding a view onto the live filming. At the nadir of this it may be possible to bring producers and directors directly into the virtual studio as avatars on the screen boundary, with a spatially faithful view onto the set. For the purposes of this book it's also worth noting that NFTs of the experience and corresponding virtual objects from the scene could be monetised and sold within the metaverse.

7.6.1.1 Multiview

In order to reconnect directional cues of all kinds it is necessary for each party in the group to have a spatially correct view of the remote user which is particular for them. This requires a multi-view display, which has applications beyond telepresence but are used extensively in research which attempts to address these issues.

Nguyen and Canny demonstrated the 'Multiview' system [149]. Multiview is a spatially segmented system, that is, it presents different views to people standing in different locations simultaneously. They found similar task performance in trust tasks to face-to-face meetings, while a similar approach without spatial segmentation was seen to negatively impact performance.

In addition to spatial segmentation of viewpoints [274] it is possible to isolate viewpoints in the time domain. Different tracked users can be presented with their individual view of a virtual scene for a few milliseconds per eye, before another viewpoint is shown to another user. Up to six such viewpoints are supported in the c1x6 system [275] Similarly MM+Space offered 4 Degree-Of-Freedom Kinetic Display to recreate Multiparty Conversation Spaces [276]

7.6.2 Holography and Volumetric

Blanche et al. have done a great deal of research into holographic and volumetric displays using lasers, rotating surfaces, and light field technology [277, 278]. They are actively seeking to use their technologies for telepresence and their work is very interesting.

Similarly Jones et al. "HeadSPIN" is a one-to-many 3D video teleconferencing system [271] which uses a rotating display to render the holographic head of a remote party. They achieve transmissible and usable framerate using structured light scanning of a remote collaborator as they view a 2D screen which they say shows a spatially correct view of the onlooking parties.

Eldes et al. used a rotating display to present multi-view autostereoscopic projected images to users [279].

Seelinder is an interesting system which uses parallax barriers to render a head which an onlooking viewer can walk around. The system uses 360 high resolution still images which means a new spatially segmented view of the head every 1 degreesof arc. They claim the system is capable of playback of video and this head in a jar multi-view system clearly has merit but is comparatively small, and as yet untested for telepresence [280].

These systems do not satisfy the requirement to render upper body for the viewers and are not situated (as described soon).

There's a future possible where real-time scanned avatar representation in persistent shared metaverse environments will be able to support business, but the camera rigs which currently generate such models are too bulky and involved for a good costs benefit analysis. It is more likely that recent advances in LIDAR phone scanning show the way. The allow realistic avatars to be quickly created for animation within metaverse scenes [281].

7.6.3 Simulated Humans

7.6.3.1 Uncanniness

When employing simulation representations of humans it may be the case that there is an element of weirdness to some of these systems, especially those that currently represent a head without a body. Mori has demonstrated The Uncanny Valley [282] effect in which

imperfect representations of humans elicit revulsion in certain observers. This provides a toolkit for inspecting potentially 'weird' representations, especially if they are 'eerie' and is testable through Mori's GODSPEED questionnaire.

With an improved analysis of the shape of the likeability curve estimated later showing a more nuanced response from respondents where anthropomorphism of characters demonstrated increased likeability even against a human baseline [283, 284].

A mismatch in the human realism of face and voice also produces an Uncanny Valley response [285].

However, there is a possibility that Mori's hypothesis may be too simplistic for practical everyday use in CG and robotics research since anthropomorphism can be ascribed to many and interdependent features such as movement and content of interaction [284].

Bartneck et al. also performed tests which suggest that the original Uncanny Valley assertions may be incorrect, and that it may be inappropriate to map human responses to human simulacrum to such a simplistic scale. They suggest that the measure has been a convenient 'escape route' for researchers [284]. Their suggestion that the measure should not hold back the development of more realistic robots holds less bearing for the main thrust of this telepresence research which seeks to capture issues with imperfect video representation rather than test the validity of an approximation.

Interestingly Ho et al. performed tests on a variety of facial representations using images. They found that facial performance is a 'double edged sword' with realism being important to robotic representations, but there also being a significant Uncanny Valley effect around 'eerie, creepy, and strange' which can be avoided by good design [286].

More humanlike representations exhibiting higher realism produce more positive social interactions when subjective measures are used [221] but not when objective measures are used. This suggests that questionnaires may be more important when assessing potential uncanniness.

A far more objective method would be to measure user responses to humans, robots, and representations with functional near-infrared spectroscopy and while this has been attempted it is early exploratory research [287], an emotional response to 'eerie' was discovered.

7.6.3.2 Embodiment through robots

Virtuality human representation extends beyond simple displays into robotic embodiments (which need not be humanoid [288]), shape mapped projection dubbed "shader lamps", and hybridisations of the two.

Robots which carry a videoconference style screen showing a head can add mobility and this extends the available cues [289, 290, 291, 292, 293]. Interestingly Desai and Uhlik maintain that the overriding modality should be high quality audio [294].

Tsui et al. asked 96 participants to rate how personal and interactive they found interfaces to be. Interestingly they rated videoconferencing as both more personal and more interactive than telepresence robots, suggesting that there is a problem with the overall representation or embodiment [295].

Kristoffersson et al. applied the Networked Minds questionnaire to judge presence of a telepresence robot for participants with little or no experience of videoconferencing. Their results were encouraging, though they identified that the acuity of the audio channel needing improvement [296].

There are a very few lifelike robots which can be used for telepresence, and even

these are judged to be uncanny [297]. This is only an issue for a human likeness since anthropomorphic proxies such as robots and toys perform well [282].

7.6.3.3 Physical & Hybrid embodiment

Embodiment through hybridisation of real-time video and physical animatronic mannequins has been investigated as a way to bring the remote person into the space in a more convincing way [298, 299, 300]. These include telepresence robots [290, 297, 291], head in a jar implementations such as SphereAvatar [301, 302, 303] and BiReality [304], UCL's Gaze Preserving Situated Multi-View Telepresence System [302], or screen on a stick style representations [293].

Nagendran et al. present a 3D continuum of these systems into which they suggest all such systems can be rated from artificial to real on the three axes, shape, intelligence, and appearance [305].

Itoh et al. describe a 'face robot' to convey captured human emotion over a distance. It uses an 'average face' and actuators to manipulate feature points [306]. It seems that this is an outlier method for communication of facial affect but demonstrates that there are many development paths to a more tangible human display.

It seems increasingly likely that machine learning models which manipulate images in real time can simulate humans into metaverse applications with very little input data. One such example is Samsung's Megaportraits which can product a realistic human face from a single input stream such as a webcam [307].

7.6.3.4 Shader lamps

Projection mapping is a computational augmented projection technique where consideration of the relative positions and angles of complex surfaces allows the projection from single or multiple sources to augment the physical shapes onto which they appear. It was first considered by the Disney corporation in 1969 and was given prominence by Raskar and Fuchs with "office of the future" [308] and later by Raskar and other researchers [300]. It has since gained considerable commercial popularity in live entertainment.

Shader lamps [300] is the more formal academic designation for projection mapping. It is possible to use the technique alongside reconstruction to project onto a white facial mannequin. Researchers have attempted to use the technology for remote patient diagnostic, projecting onto styrofoam heads [309].

Bandyopadhyay et al. demonstrated [310] that it is possible to track objects and projection map [311] onto them in real time. This is beyond the scope of the proposed projection onto furniture since we wish to keep the system as simple as possible, but could be useful for shared tasks in the future work.

Lincoln et al. employed animatronic avatars which they projected with shader lamps. This combination recreated facial expression and head movement though they were limited in speed and range of control of the remote head [299].

While shader lamps are an important and useful technology, there are limitations imposed by its use. In particular if a realtime video feed or reconstruction of a subject is used then that scanned subject must either remain still enough to be correctly mapped onto geometry on the remote side (useful for some virtual patients for instance [312], or else there must be a computational adjustment made for their changing position to make them appear static, or the projection surface must move to match their movement as in Lincoln et al.

7.6.3.5 Metaverse

In supporting business it's not clear that performance is improved or even maintained by the use of a metaverse. Xi et al. found a significant negative impact to productivity within metaverse applications [313]. It lowers productivity, and may increase anxiety, nausea, VR sickness and even migraines [314]. Ir seems at this stage that if we are determined to explore metaverse for business then we should mitigate the problems as much as possible using the understanding we have gained so far.

7.7 Theoretical Framework toward metaverse

7.7.1 Problem Statement

It seems that metaverse is not the most useful way to conduct business. It is furthermore clear that there are multiple factors which contribute to successful human-human communication. These factors remain important in telecommunication supported by technology, and are variously supported, unsupported, or modified by particular technologies.

Of particular importance is interpersonal gaze [182, 156, 183]. Non-verbal cues are also important across multiple modalities of sight, sound [158], and position of interlocutors [166], extending to the whole body [156, 195].

While formal meeting paradigms are pretty well supported by commercially deployed systems, such ICT can be expensive, may need to be professionally managed, and high end equipment in board rooms are generally booked well in advance. These meetings seem to demand many smaller supporting meetings between parties or groups of parties. The pressure here is clearly toward the now ubiquitous Teams and Zoom style formats, and these offer very poor support for social cues, and incur additional fatigue.

The 'problem' is a supporting technology for small less formal groups, or ad-hoc groups meeting to add clarity or context to formal meetings. Metaverse allows this kind of interaction, while not seeming to replace formal meeting utility. Metaverse also may connect home and work spaces without bringing in those backgrouds, creating a level playing field. A more advanced metaverse interface could also allow dynamism and movement, connection of natural non vocal cues, without too much encumbering technology overhead.

7.7.2 Core Assumptions

Figure 7.4 shows the interlocking relationships between baseline communication where the participants are present, and technology which attempts to support across distance.

Of most interest to this research is the centre of the Venn where meeting styles which are less formal, and perhaps dynamic, may occur. Looking at these items one by one gives us our core assumptions.

1. Gaze
   Gaze is broadly agreed to be highly important for mediating flow. Mutual gaze is a rich emotional channel. The research must consider gaze. All of the researchers listed around the Venn have at some point engaged with this topic.
2. Attention
   The non-verbal communication channel employed in 'attention' is assumed based upon the literature to be critical to smoothly leaving and entering a fast flowing conversation where concentration around a defined problem may be high (gesturing

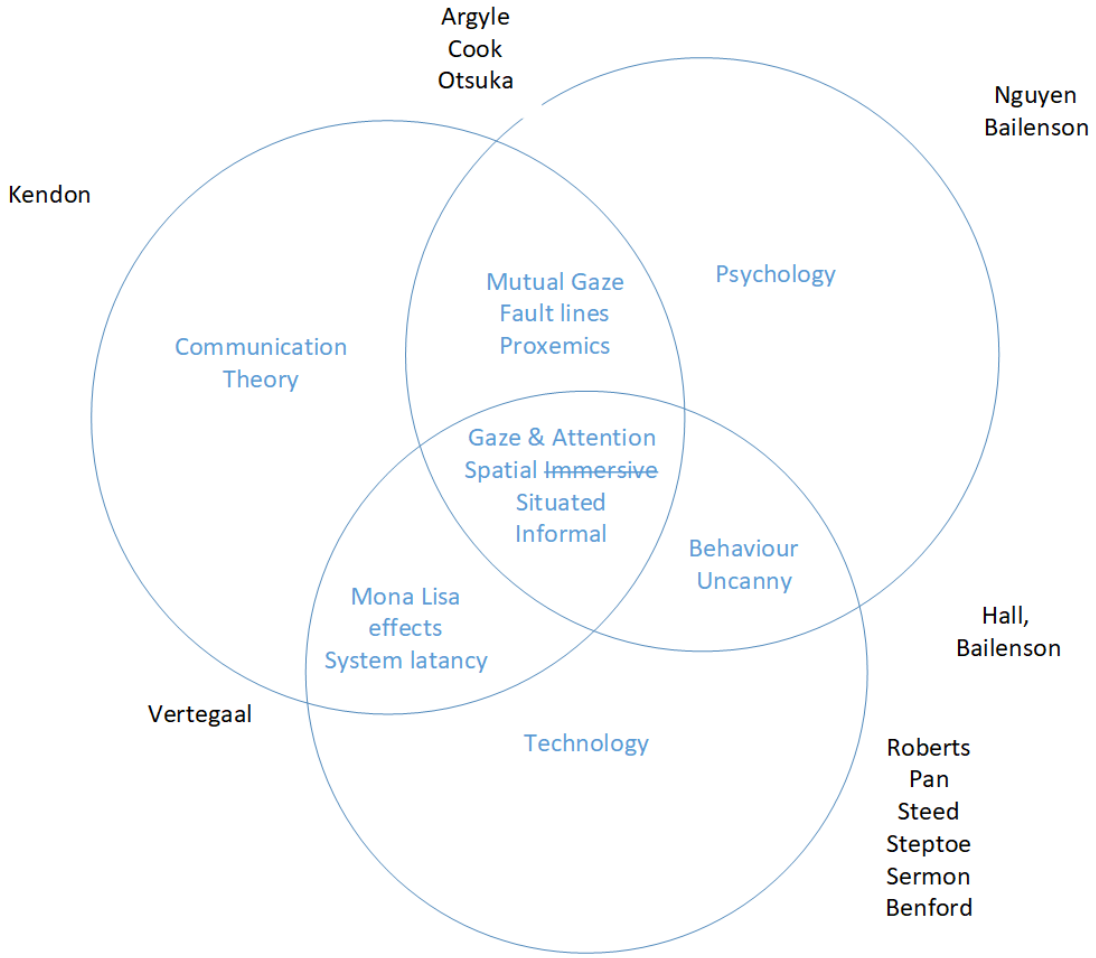


Figure 7.4: The Venn diagram shows areas of research which have been identified in blue. These interlock and overlap as shown. The most relevant identified researchers from the literature are shown in black close to the fields of study which they represent. This diagram is a view of the core assumptions for the research, with the most important fields at the centre.

to a chair for instance). Again, all of the listed researchers have made reference to attention in their work.

3. Spatial (immersive)
   Support for spatiality is important in a group setting so that directional non-verbal cues can find their target. The topic of spatial relationships between interlocutors cuts across all of the researchers, but this is not true of immersion. Immersion in a shared virtuality can certainly support the underlying requirements spatial, but the technical infrastructure required is out of scope (so this is struck through on the diagram). Roberts and Steed are the main expertise referenced even though this element is not expanded in the research.
4. Situated
   Situated displays are those which are appropriate for their surrounding context, in this case the informal meeting. Roberts, Pan, Steed and Steptoe seem the most relevant researchers in these technology spaces.
5. Informal

Based on the literature proxemics is believed to be relevant in a meeting where subgroups can be instantiated and destroyed as the meeting evolves, and those where people can be invited in from outside the physical bounds of the meeting (informal spaces). Hall is the best source for this work. If it is assumed that people may come and go, and subgroups may be convened then Sermon and Benford are the best references through their work blending real and virtual spaces. This may be more consistent with less organised meetings such as those convened on demand (ad-hoc).

7.7.3 Peripheral Assumptions

Surrounding the centre of the Venn are additional relevant topics from social science branches of theory

From verbal communication

It is assumed that the directionality of sound is important [153], and this will be engineered into the experimental design. It is assumed that movement of the lips is an indicator and this is tied to latency and frame rate in the vision system.

From non-verbal communication

It is assumed that eye gaze is of high importance, and that this information channel is supported by head gaze and body torque to a high degree. It is further assumed that mutual eye gaze is of less relevance in a multi party meeting where there is a common focus for attention but can be significant for turn passing. It is assumed that upper body framing and support for transmission of micro and macro gesturing is important for signaling attention in the broader group, and for message passing in subgroups.

Now that we have an idea what's important for business social communication we can look at the available software to find a best fit.

7.8 Post 'Meta' metaverse

The current media around "metaverse" has been seeded by Mark Zuckerberg's rebranding of his Facebook company to 'Meta', and his planned investment in the technology. Kraus et al suggest that this seems more a marketing and communication drive than a true shift in the company business model [315], but despite this Park and Kim identify dozens of recent papers of metaverse research emerging from Meta labs [118].

In Stephenson's 'Snow Crash' the Hero Protagonist (drolly called Hiro Protagonist) spends much of the novel in a dystopian virtual environment called the metaverse. It is unclear if Facebook is deliberately embracing the irony of aping such a dystopian image, but certainly their known predisposition for corporate surveillance, alongside their attempt at a global digital money is ringing alarm bells, as is their current plan for monetisation.

The second order hype is likely a speculative play by major companies on the future of the internet. Grayscale investment published a report which views Metaverse as a potential trillion dollar global industry. Such industry reports are given to hyperbole, but it seems the technology is becoming the focus of technology investment narratives. Some notable exerts from a 2021 report by American bank JPMorgan show how the legacy financial institutions see this opportunity:

- In the view of the report *"The metaverse is a seamless convergence of our physical and digital lives, creating a unified, virtual community where we can work, play, relax, transact, and socialize." - this isn't the worst definition, and very much plays into both the value and mixed reality themes explored in this book.*

- They agree with the industry that monetisation of assets in metaverse applications is called "Metanomics". It's worth seeing this word once, as it's clearly gaining traction, but it won't be used in this book.
- They make a point which is at the core of this book, that value transaction within metaverses may remove effective border controls for working globally. Be this teleoperation of robots, education, or shop fronts in a completely immersive VR world. They say: *"One of the great possibilities of the metaverse is that it will massively expand access to the marketplace for consumers from emerging and frontier economies. The internet has already unlocked access to goods and services that were previously out of reach. Now, workers in low-income countries, for example, may be able to get jobs in western companies without having to emigrate."*
- There is a passage which foreshadows some of the choices made in this book: *"Expanded data analytics and reporting for virtual spaces. These will be specifically designated for commercial and marketing usage and will track business key performance indicators (this already exists in some worlds, such as Cryptovoxels)"*. More on this later.
- The report attempts to explore the web3 & cryptocurrency angles of metaverse. That's also the aim of this book, but they have taken a much more constrained approach, ignoring the possibilities within Bitcoin.
- They assert that strong regulatory capture, identification, KYC/AML etc should underpin their vision of the metaverse. This is far from the community driven and organically emergent narratives that underpin Web3. This is their corporate viewpoint, something they have to say. On the back of this they pitch their consultancy services in these areas.

There has been a reactive pushback against commercialisation and corporateisation by the wider tech community, who are concerned about the aforementioned monetisation of biometrics. Observers do not trust these 'Web2' players with such a potentially powerful social medium. It is very plausible that this is all just a marketing play that goes nowhere and fizzles out. It is by no means clear that people want to spend time socialising globally in virtual and mixed reality. These major companies are making an asymmetric bet that if there is a move into virtual worlds, then they need to be stakeholders in the gatekeeping capabilities of those worlds.

7.9 Market analysis

The Drum is a market awareness website and compiled the following statistics, which have been linked back to their source and annotated for our needs.

- *89.4 million Americans are expected to use virtual reality (VR) in 2022, according to insiderintelligence. That number, according to the same source, is expected to climb to 110.3 million in 2025. As a counter to this only around 16M VR headsets were sold in 2022*
- *51% of gen Z and 48% of millennials envision doing some of their work in the metaverse in the next two years, according to Microsoft's Work Trend Index 2022.*
- *38% of respondents said they would "try extreme sports like skydiving, bungee jumping, or paragliding" in the metaverse according to a recent Statista survey called 'What things would you do in the metaverse but never in real life?' Unsettlingly, 18% of respondents said they would "conduct unethical experiments on virtual humans"*

- *87% of Americans between the ages of 13-56 would be interested in engaging with a virtual experience in the metaverse "that is built around a celebrity they love," according to new research from UTA and Vox Media*
- *$678bn is forecasted to be the total market valuation of the metaverse by 2030, per Grand View Research. According to the report, that market value was just shy of*
- *$39bn in 2021, giving it a predicted compounded annual growth rate over a 10-year period of around 39*
- *46% of all people across age groups say that the ability to visualize a virtual product in an IRL context – "such as seeing a digital painting in their home using augmented reality (AR) glasses" – is the primary factor that would motivate them to make a purchase in the metaverse, per a Productsup survey*
- *24% of US adult internet users say "that lower-priced VR headsets were a very important factor when deciding whether to try using the metaverse," per a recent Statista survey. On the other hand, 54% say that their workplace using the metaverse would "not [be] important at all" in their decision to give the metaverse a try*
- *15% of gen Zs' "fun budget" is spent in the metaverse, per a report from Razorfish and Vice Media Group. In five years that number is projected to climb to 20%*
- *Nearly 77% believe that the metaverse "can cause serious harm to modern society," per a recent survey from customer service platform Tidio. The survey, which received feedback from 1,000 participants, identified three major causes of anxiety related to the metaverse and its potentially negative social impacts: "addiction to a simulated reality" was the number one concern, followed by "privacy issues" and "mental health issues," which were tied for second*
- *By 2026, about 2 billion people worldwide "will spend at least one hour a day in the metaverse to work, shop, attend school, socialize or consume entertainment," per McCann Worldgroup. By that same year, the total value of the virtual goods market in the metaverse could be as high as $200bn*
- *NFTs Over $37bn has been spent in NFT marketplaces as of May 2022, per data from Chainalysis. At their current rate, this year's NFT sales could potentially surpass last year's, which had a total valuation of around $40bn, according to the data*
- *$91.8m was the sale price of 'The Merge,' the most valuable NFT to date. Created by the artist Pak, it sold for its record-breaking value in December 2021*
- *64% of sports fans are open to the idea of learning more about NFTs and would consider purchasing one in the future, according to the National Research Group. The report also found that 46% of sports fans "would be more likely to attend live sporting events if they were rewarded with a commemorative NFT – for example, if their ticket turned into a digital collectible after the game"*
- *Only 9% of people aged 16-44 own a NFT, and less than half (44%) have purchased or invested in crypto, per a new survey from agency SCS. On the other hand, among the survey's 600 respondents, 64% were "aware" of the metaverse, and 65% of that subgroup say they are "interested in exploring it further for everything from traveling to new places and playing games to making money and shopping"*

Polling company IPSOS have conducted a global survey for the World Economic Forum. Some highlights are:

- "Excitement about extended reality is significantly higher in emerging countries than it is in most high-income countries. In China, India, Peru, Saudi Arabia, and

Colombia, more than two-thirds say they have positive feelings about the possibility of engaging with it."

- "Familiarity and favorability toward the new technologies are also significantly higher among younger adults, those with a higher level of education, and men than they are among older adults, those without a college-level education, and women."

Excitingly for our exploration of the topic it can be seen in Figure 7.5 that education within metaverse spaces is the most anticipated application, and we have seen that the emerging globals markets are the most optimistic about the technology overall. This is highly suggestive of an opportunity.

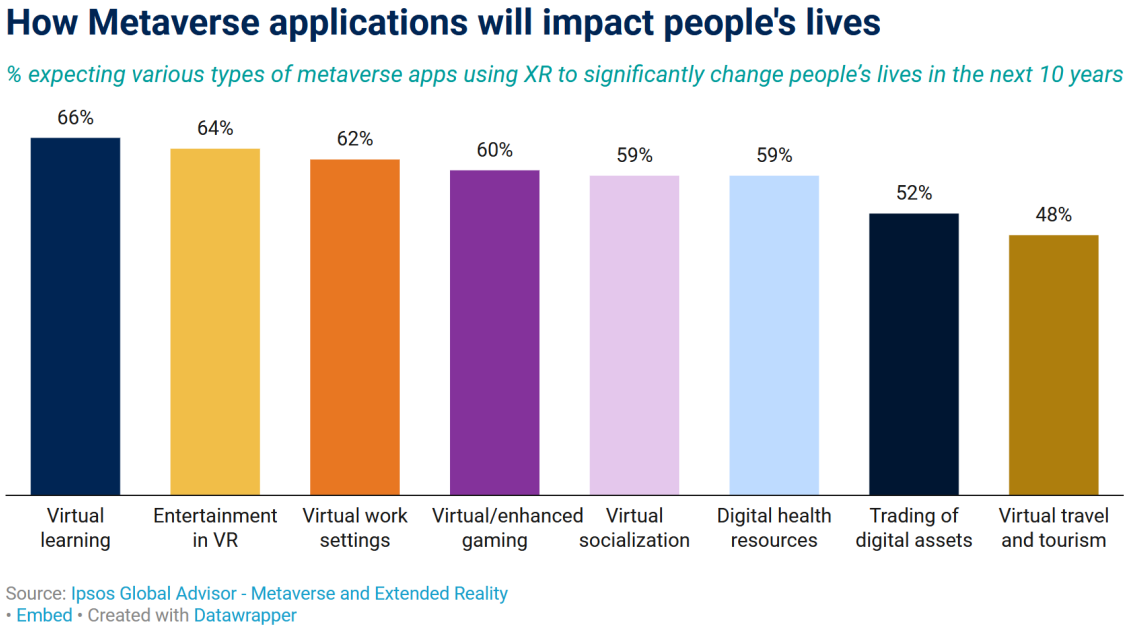


Figure 7.5: IPSOS poll predicted applications

7.10 NFT and crypto as metaverse

Within the NFT, Web3 and crypto community it is normalised to refer to ownership of digital tokens as participation in a metaverse. This is reflected in the market analysis above. This fusing of narratives is reviewed in detail by Gadekallu et al in their excellent recent paper on Metaverse and Blockchain [316]. They conclude that much remains to be done here. This CNBC article highlights the confusion, as this major news outlet refers to Walmart prepares to offer NFTs" as an entry "into the metaverse".

7.11 Immersive and third person XR

In considering the needs of business to business and business to client social VR is it useful to compare software platforms. We have seen that a global connected multiverse is a marketing proposition only, and may be a decade or more away. Contenders currently look more like one of three catagories; games, limited massively multiplayer worlds, or meeting support software. These will converge.

7.11.1 More like a digital twin

One of the most intuitive ways to view a metaverse is as a virtual landscape. This is how metaverse was portrayed in the original Neal Stephenson use of the word. 'Digital twin' is another much abused industry term which trends toward a 3D representation of real world spaces and objects. Sometimes these virtual objects are connected to the real by telemetry, allowing industrial monitoring applications. Much is made of such systems in simulation brochures, and on the web, but it's surprisingly hard to find real world applications of the idea outside of complex large scale systems engineering (aerospace). The costs of maintenance are simply too high. The US army owns the digital twin which could be called closest to "The Metaverse" (note the intentional capitalisation). Their global simulation environment mirrors real world locations for their training needs.

7.11.1.1 Geolocated AR

Overlaying geospecific data into augmented reality (think Pokemon Go) is probably the ultimate utility of digital twin datasets. It's such a compelling application space that we will have more on this later.

7.11.2 More like a metaverse

7.11.2.1 Second Life

Notable because it's the original and has a decently mature marketplace. Some $80M was paid to creators in Second Life in 2021 in a wider economic ecosystem of around $650M. It's possible to write a whole book on Second life, and indeed many have. It's longevity means that there's more study of business uses of such systems than in any other platform.

7.11.2.2 Mozilla Hubs

Hubs is a great option for this proposal, and might be worth integrating later. It runs well in a browser and on VR hardware.

- Open source, bigger scale, more complex
- Choose avatars, or import your own
- Environments are provided, or can be designed
- Useful for larger conferences with hundreds or thousands of members but is commensurately more complex
- Quest and PC
- Larger scenes within scenes

7.11.2.3 Counter social realms

A relatively new platform linked to a new model of social media which excludes countries which habitually spam. It uses Mozilla Hubs for it's engine.

7.11.2.4 Roblox

If anything can currently claim to be the metaverse it's probably Roblox. Around 60 billion messages are sent daily in Roblox. Investment in the metaverse 'angle' of the platform is stepping up with recent announcements such as "Spotify Island". It's very notable that it still hasn't become a profitable business. It is important to note that Roblox has banned NFTs.

7.11.2.5 Minecraft

Minecraft has also banned NFTs

7.11.2.6 Surreal

7.11.2.7 Sansar

7.11.2.8 Cornerstone

7.11.2.9 AltSpace

- Microsoft social meeting platform
- Very good custom avatar design
- Great world building editor in the engine
- Doesn't really support business integration so it's a bit out of scope
- Huge numbers (many thousands) possible so it's great for global events
- Mac support

7.11.2.10 VRChat

This text is from wikipedia and will be updated when we have a chance to try VRChat properly. It's much loved already by the Bitcoin community.

"VRChat's gameplay is similar to that of games such as Second Life and Habbo Hotel. Players can create their own instanced worlds in which they can interact with each other through virtual avatars. A software development kit for Unity released alongside the game gives players the ability to create or import character models to be used in the platform, as well as build their own worlds.

Player models are capable of supporting "audio lip sync, eye tracking and blinking, and complete range of motion.

VRChat is also capable of running in "desktop mode" without a VR headset, which is controlled using either a mouse and keyboard, or a gamepad. Some content has limitations in desktop mode, such as the inability to freely move an avatar's limbs, or perform interactions that require more than one hand.

In 2020, a new visual programming language was introduced known as "Udon", which uses a node graph system. While still considered alpha software, it became usable on publicly-accessible worlds beginning in April 2020. A third-party compiler known as "UdonSharp" was developed to allow world scripts to be written in C sharp."

7.11.2.11 Meta Horizon Worlds & Workrooms

Horizon Worlds is the Meta (Facebook) meteverse, and Workrooms it's business offering and a subset of the "Worlds" global system. It is currently a walled garden without connection to the outside digital world, and arguably not therefore a metaverse.

The Financial Times took a look at their patent applications and noted that the travel is toward increased user behaviour tracking, and targeted advertising.

Facebook actually have a poor history on innovation and diversification of their business model. This model has previously been tracking users to target ads on their platform, while increasing and maintaining attention using machine learning algorithms.

It makes complete sense then to analyse the move by Meta into 3D social spaces as an attempt to front run the technology using their huge investment capacity. Facebook have recently taken a huge hit to their share price. Nothing seems to have changed in the underling business except Zuckerberg's well publicised shift to supporting a money losing gamble on the Metaverse. It is by no means clear that users want this, that Meta will

be able to better target ads on this new platform, or that the markets are willing to trust Zuckerburg on this proactive move.

With all this said the investment and management capacity and capability at Meta cannot be dismissed. It is very likely that Meta will be able to rapidly deploy a 3D social space, and that it's development will continue to be strong for years. The main interface for Horizon Worlds is through the Meta owned and developer Oculus headset, which is excellent and reasonably affordable. It has been quite poorly received by reviewers but will likely improve, especially if users are encouraged to innovate.

7.11.2.12 Webaverse

Webaverse are an open collective using open source tools to create interoperable metaverses.

7.11.2.13 Vircadia

The applications and platforms detailed above have their benefits, but for the application stack in the next section of the book Vircadia has been chosen. The following text is from their website, and is a placeholder which gives some idea. This section will be written out completely to reflect our use of the product.

Vircadia is open-source software which enables you to create and share virtual worlds as virtual reality (VR) and desktop experiences. You can create and host your own virtual world, explore other worlds, meet and connect with other users, attend or host live VR events, and much more.

The Vircadia metaverse provides built-in social features, including avatar interactions, spatialized audio, and interactive physics. Additionally, you have the ability to import any 3D object into your virtual environment. No matter where you go in Vircadia, you will always be able to interact with your environment, engage with your friends, and listen to conversations just like you would in real life.

What can I do? You have the power to shape your VR experience in Vircadia.

- EXPLORE by hopping between domains in the metaverse, attend events, and check out what others are up to!
- CREATE personal experiences by building avatars, domains, tablet apps, and more for you and others to enjoy.
- SCRIPT and express your creativity by applying advanced scripting concepts to entities and avatars in the metaverse.
- HOST and make immersive experiences to educate, entertain, and connect with your audience.
- CONTRIBUTE to the project's endeavor.
- DEVELOP the project and tailor it to your needs, or just to help out.
- SECURITY information about the project and its components.

7.11.3 More like crypto NFT virtual land

This next three are a placeholder taking text from the linked site and will be swapped out: The digital land narrative is fading.

7.11.3.1 Decentraland

Decentraland is the first-ever blockchain-powered place in the metaverse. It is a virtual reality platform powered by the Ethereum blockchain. It allows users to create, experience,

and monetize content and applications.

7.11.3.2 Sandbox

The Sandbox is a virtual Metaverse where players can play, build, own, and monetize their virtual experiences. The Sandbox blockchain gaming platform consists of three integrated products that together provide a comprehensive experience for user-generated content.

7.11.3.3 Space Somnium

Somnium Space is a metaverse with a different objective. It allows users to join in either through a downloadable VR client or a browser-based version to function like any other web app.

7.11.4 More like industrial application

As the word metaverse has gained in use, so have some traditional users and researchers in mixed reality switched to use of the term. Siyaev and Jo describe an aircraft training metaverse which incorporates ML based speech recognition [317]. This class of mixed reality trainer traditionally finds positive results, but is highly task specific.

7.11.4.1 Global enterprise perspective

Microsoft have just bought Activision / Blizzard for around seventy billion dollars. This has been communicated by Microsoft executives as a "Metaverse play", leveraging their internal game item markets, and their massive multiplayer game worlds to build toward a closed metaverse experience like the one Meta is planning. This builds on the success of early experiments like the Fornite based music concerts, which attracted millions of concurrent users to live events.

There are three emerging focuses, the social metaverses for pleasure, and business metaverses for larger group meetings and training [318, 319], and a Nvidia's evolving collaborative creation metaverse for digital engineers and creatives. They're all pretty different 'classes' of problem. The social metaverse angle where Facebook is concentrating most effort is of less interest to us here, though obviously markets will exist in such systems for business to customer. The next section will explore some of the software tools available to connect people. Everything looks pretty basic right now in all the available systems, but that will likely change over the next couple of years.

7.11.5 More like meeting support

7.11.5.1 Spatial

Spatial is worth a quick look because it's a business first meeting tool, and comparatively well received by industry for that purpose.

- Very compelling. Wins at wow.
- Great avatars, user generated
- AR first design
- Limited scenes
- Smaller groups (12?)
- Limited headset support
- Intuitive meeting support tools
- No back end integration

7.11.5.2 MeetinVR

- Good enough graphics, pretty mature system
- OK indicative avatars, user selected
- VR first design
- Limited scenes
- Smaller groups (12?)
- Quest and PC
- Writing and gestures supported
- Some basic enterprise tools integration
- Bring in 3D objects
- Need to apply for a license?

7.11.5.3 Glue

- Better enterprise security integration
- Larger environments, potential for breakouts in the same space. Workshop capable
- 3D object support, screen sharing, some collaborative tools
- Apply for a license
- Fairly basic graphics
- Basic avatars
- Quest and PC
- Writing and gestures supported
- Mac support

7.11.5.4 FramesVR

- Really simple to join
- Basic avatars
- Bit buggy
- 3D object support, screen sharing, some collaborative tools
- Quest and PC
- Larger scenes within scenes
- Runs in the browser

7.11.5.5 Engage

- Great polished graphics
- Fully customisable avatars
- Limited scenes
- Presentation to groups for education and learning
- PC first, quest is side loadable but that's a technical issue
- BigScreen VR
- Seated in observation points in a defined shared theatre
- Screen sharing virtual communal screen watching, aimed at gamers, film watching
- up to 12 user

7.11.5.6 Gather

Gather is an oddball meeting space based around fully customisable 2D rooms with a game feel. It's really a spatialised twist on video conferencing but interesting.

7.11.5.7 NEOSVR

Notable because it's trying to integrate crypto marketplaces, but we haven't tried it yet.

7.12 The future

7.12.1 Mixed reality as a metaverse

Spatial anchors allow digital objects to be overlaid persistently in the real world. With a global 'shared truth' of such objects a different kind of metaverse can arise. One such example is the forthcoming AVVYLAND.

Peleton as a metaverse?

7.12.2 Augmented reality

Marc Petit, general manager of Epic Games envisages a 2 watt pair of glasses, connected to a 10 watt phone, connected to a 100 watt computer on the edge. This is a device cascade problem which has not yet been solved, and is at the edge of achievable thermodynamics and latency.

The closest technology at this time seems to be Lumus' waveguide projectors which are light, bright and high resolution.

7.12.3 Ubiquitous displays

This includes laser retinal displays, and smart screens which are context and user aware.

7.13 Risks

Metaverse is fraught with risks, partly because it's new, and partly because of the pace of adoption.

- Abuse; because of the real-time and spatio-temporal abuse happens less like in the current web 2 social media, and more like in the real world, but with less opportunity for repercussions. It might be that natural language processing and machine learning can help with this, but it's a tough problem. One idea might be to record the speech to text of interactions between participants, and flag to them if a "bullying, harassment, predation threshold" is met. This could be encrypted with the public keys of the participants and a notice sent to them that if they wished to follow up with authorities then they have the necessary attestations and proofs. This is minimally invasive and privacy preserving, and acts as a strong disincentive to repeat offence. It can also feed into a global "web of trust" reputation system in a 'zero knowledge' way. Users who flag abuse to the reputation system can leverage the machine learning opinion without revealing what happened (though they would have the data). This would also act as a disincentive without the social stigma issues of reporting.
  Reporting could be achieved without machine learning identification of potential problems, but there would have to be a social cost to reporting (like gossiping incessantly about others) which would erode the social score of the reporting entity. This would mitigate bot based reputation harm.
- Miscommunication; which as we have seen in the early section of the metaverse chapter is both complex and hard to mitigate
- Lost information

- Distraction
- Jitter, judder, jagginess, and interruption of flow; because the network overhead is higher than other communication media it's much more exposed to latency effects
- Physical harms, especially to developing brains and ocular systems

7.14 TL;DR

The points below are the tl;dr for the whole book. They do not currently correspond to the order in the book, but will do at some point

- **There may be an inflection point in the organisational topology of the internet because of trust abuses by the incumbent providers. This is calling itself Web3, but the moniker is fraught with problems and somewhat meaningless. The drivers are real.**
- **'The Metaverse' is coming, in some form, at some point. Everyone is positioning in case it's "soon".**
- **It's not at all clear what it is, or if people want it.**
- **From a business perspective metaverse is the worst of the remote collaboration tool-kits, and undermines flow, productivity, and interpersonal trust.**
- **It's probably technology for technologies sake to a degree, but the time feels right for the attempt, and the investment is real.**
- **Excluding Facebook/Meta a lot of the investment is coming from the Web3 speculative bubble, who have a parallel and intersectional metaverse narrative.**
- **Industry has noted the risk, and failures of Meta in this domain, and have latched onto "open metaverse" as a narrative, to de-risk their interest.**
- **The current open metaverse is muddy and confused.**
- **Anything from a multi-million pound XR studio screen, to a speech audio system, can be a metaverse interface.**
- **Constraints (metaverse schema) which are crafted in response to the use case, the interface, and the audience, is where challenges are most profound. This is an opportunity.**
- **Trust, governance, and safeguarding, are far harder in these real-time distributed social systems.**
- **There's a bunch of start-ups and options, interesting research, and some adoption, but scaling is very hard in the face of tepid consumer interest.**
- **Industry seem to be missing the point; that open metaverse should mean open source metaverse. There are some options, but they are under developed. This is an opportunity.**
- **There is genuine, undeniable interest in digital scarcity. The ownership of digital goods seems natural to younger, digitally native users.**
- **This is serviced already by various (gaming) platforms, but they are all isolated ecosystems.**
- **Uniting these attempts, with portable (transferable) "goods" across the digital universe (metaverse) likely requires a global digital ledger (blockchain).**
- **Crypto is igniting imagination on this topic, and is seeing adoption both inside out outside of the metaverse contexts.**
- **Crypto is a nightmare; rife with scams, poor technology choices, limited life, and incorrect assumptions.**

- **The only thing blockchain/crypto can do well is "money like networks", which is a cornerstone of human interaction, and the killer application.**
- **Representations of dollars and pounds etc money can ride securely on top of such networks as stablecoins, and this is getting easier to integrate, though there are risks.**
- **It's unclear which technology will win, if any, but since the tools exist now they can be integrated now.**
- **Legislative and cultural headwinds are significant. There might be no opportunity here in the end, though "rough game theory" supports the attempt.**
- **Money, identity, and thereby trust, can already be mediated by the Bitcoin network, even without using Bitcoin the asset. This is an opportunity.**
- **Digital ownership is nearly possible at scale, low cost, and minimal environmental impact, with the Bitcoin network. This is an opportunity.**
- **A topologically flat, inclusive, permissionless, open metaverse, with economically empowered ML and AI actors, which can mediate governance issues, transparently, according to well constructed custom schemas, between cryptographically verifiable economic users (human or AI) is an opportunity.**



8. Our proposition

This chapter identifies an intersectional space across the described technologies, and proposes a valuable and novel software stack, which can enable exploration and product development. It is useful to briefly look at some of the potential applications which might benefit from value and trust exchange within an global shared social space.

8.1 Money in metaverses

8.1.1 AI economic actors in mixed reality

AI actors can now be trusted visually [320]. We have some thinking on this which links the external web to our proposed metaverse using tooling developed by Melvin Carvelho. He is working on economically empowered bots which leverage Nostr and RGB to perform functions within our metaverse, and outside in the WWW, as well as interacting economically through trusted cryptography with other bots, anywhere, and human participants, anywhere. This is incredibly powerful and is assured by the Bitcoin security model. Imagine being able to interact with a bot flower seller representing all the real world florists it had found. In the metaverse you could handle the flowers and take advice and guidance from the bot agent, then it would be able to take your money to buy you flowers to send to a real world address, and later find you to tell you when it's delivered. These possibilities are endless. The AI chat element, the AI translation of images on websites to 3D assets in the Metaverse are difficult but possible challenges, but the secure movement of money from the local context in the metaverse to the real world is within reach using these bots, and they are completely autonomous and distributed.

8.2 Our socialisation best practice

8.2.0.1 Identity

We will base our identity and object management on Nostr public/private key pairs. The public key of these will generate LNBits economic wallets which will interact with RGB and Lightning globally.

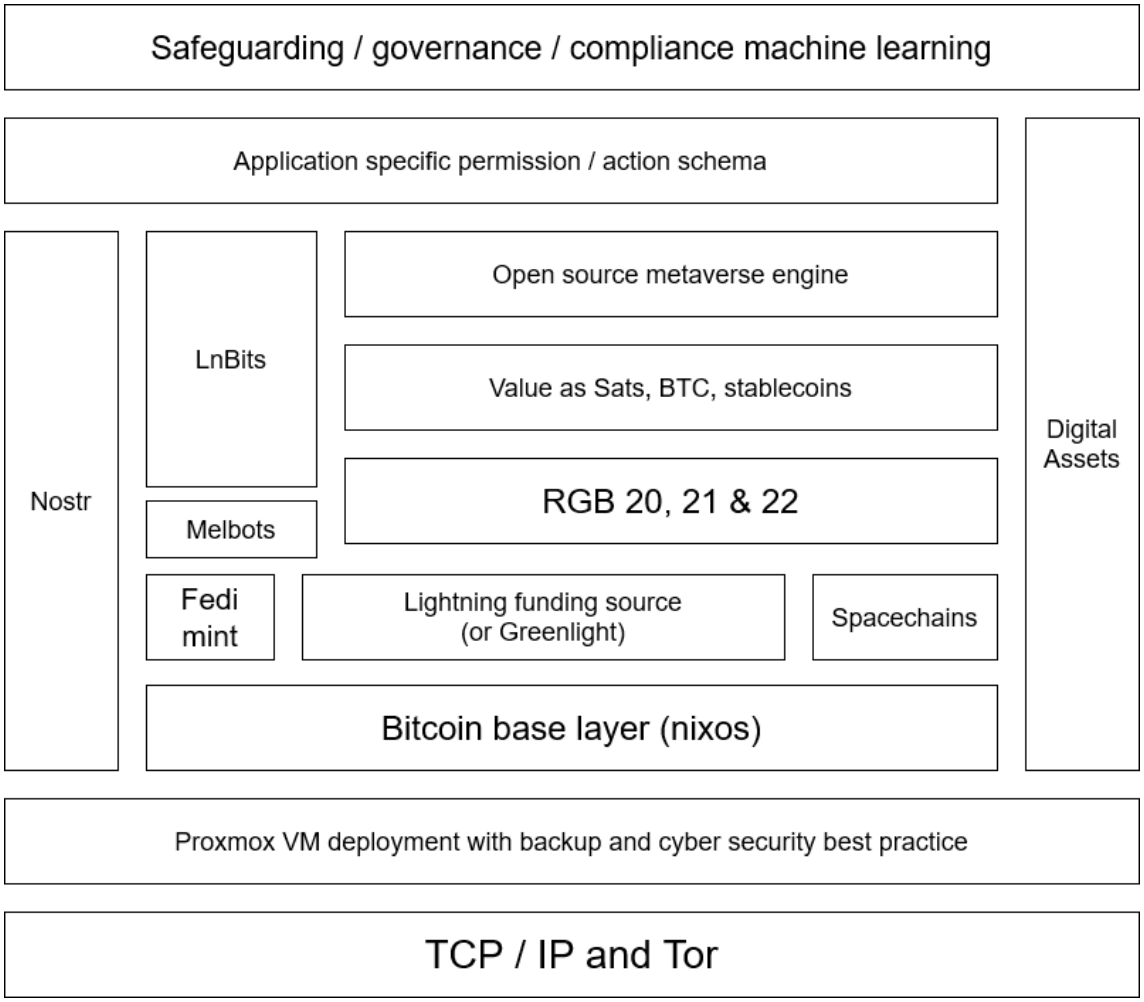


Figure 8.1: High level overview showing the components for sats, stablecoins on lightning, asssets, and trust

8.2.0.2 Webs of trust

Webs of trust will be built within worlds using economically costly (but private) social rating systems, between any actor, human or AI. It should be too costly to attack an individual aggressively. This implies an increased weighting for scores issued in short time periods. Poorly behaving AI's will eventually be excluded through lack of funds.

8.2.0.3 Integration of 'good' actor AI entities

Gratitude practice should be encouraged between AI actors to foster trust and wellbeing in human observers. "It's nice to be nice" should be incentivised between all parties". This could include tipping and trust nudging through the social rating system. Great AI behaviour would result in economically powerful entities.

8.2.1 Emulation of important social cues

8.2.1.1 Behaviour incentives, arbitration, and penalties

Collapses of trust and abuse will trigger flags from ML based oversight, which will create situational records and payloads of involved parties to unlock with their nostr private keys.

ML red flagged actors will be finacially penalised but have access to human arbitration using their copy of the data blob. Nothing will be stored except by the end users.

8.2.2 Federations of webs of trust and economics by Melbots

Web2/3 enabled bots with their own money supply should be able to carry data payloads between virtual worlds across all networks. This is an RGB/Nostr/Melbot problem space and requires more investigation.

8.3 Security evaluation

As part of developing our stack we will penetration test the deployment as detailed using Hexway

8.4 Potential applications

- Art / NFT galleries with instant sales

This application allows artists and content creator communities to display and sell NFT and fungible art to global consumer audiences, instantly.

- Large scale conference center
  - Academic conferences
  - Political conference
  - Commercial expo

In a hypothetical virtual conference centre a true marketplace of ideas could be enacted, with participants being paid directly by their audience based on the proximity to the presentation.

- Group entertainment
  - Global social puzzle gaming with prizes
  - Music festivals and gigs - Pay live artists and DJs in real time depending on location within the extended landscape of the venue. Split to music producer a portion of the value
  - Mixed reality theatre
  - murder mystery
  - Mixed reality live immersive MMORG games
  - Bingo and mass participation gameshows
  - Immersive brand storytelling metaverses
  - Escape rooms
- Debating townhall meetings (with voting etc)
- Mixed reality information metaverse
  - AR based city tours with collectibles
  - AR based collectibles for trails and heritage (museums, libraries) with location specific donations.
- Retail applications
  - Proxy for physical market
  - AR home delivery market interface within physical marketplaces
- Global course / Education provision
  - Explore the universe as a group of spaceship or planet characters
  - Explore biology and physics at a microscopic and nanoscopic level

- Micro tasking marketplace
- Code bounty marketplace
- Micro remittance role sharing (business PA / reception etc)
- Careers fair with credential passing
- Auctions in mixed reality
- eSports and live sports
- Gambling, betting markets, and financial leverage markets

8.4.1 Global cybersec course delivery

Isolating and building out one example here:

- Elements for the infrastructure: Economic layer, asset layer, content interface, user management, data storage, microsites loaded in Wolvin and webm, accessibility schema, network security, backups, secure messaging. Deployable framework with high modularity. Some more ossified elements for surity, some less so for malleability and open opportunity. Figure 8.3.
- Course delivery in XR, how to we develop a platform, marketplace, framework for open contribution.
- WebXR, Vircadia, any snap in metaverse middleware that is free and open source (action to compare the two).
- Define an interface schema for bolting in any commercial or FOSS metaverse engine.
- VR marketplace (outside the scope of the VR engine) without a trusted third party.
- Cryptographically managed learning deliverables (coursework as NFT).
- Secure messaging and group messaging using cryptographic keys. Check this stuff with the distributed computing science people in the group (action on John)
- work toward an exemplar MVP which is then "in the wild"
- Platform for educators
- Define scheme, documentation, best practice, interfaces, functional objects, pedagogy, accessibility, multi-language.
- Define user management system for educators and client learners.
- Identify the pain points which current FOSS elements which need development time/money
- separate the UI/engine from the graphical assets, and the educational / pedagogical components, accessibility, and the value and asset transfer layers.
- Desktop systems are the primary target (low end system)
- define schema for accessibility. Colour, subtitles, immersion concerns which can be applied to metaverse rooms through API?
- Start to define the hybrid presentation model we favour. Avatars? Micro sites? A combination of the two? Balance of guided vs unguided experience. Do we need to test the correct way to do delivery? Is there prior art we can draw on? I feel I should know. Is this part of the research that's being done here?
- Big work package on schema vs key and user management to enforce rules in spaces. Only participants who have provably paid should have access to learning material, the ability to input into the assessment system, and the tokenised learning outcome 'NFT' or proof.
- Proof that XR system improve learning outcomes. Also that the proposed systems for micro-transactions and user and schema management give additional headroom for teaching.

Notes on build-out The world database in the shared rooms in the metaverse is the global object master, educational materials, videos, audio content and branded objects are fungible tokens authentically proved by rgb client side validation between parties, only validated ones will be persisted in shared rooms like conferences and classes according to the room schema. That allows educators to monetise their content. That can work on lightning. NFT objects between parties like content crafted by participants (coursework, homework) are not on lightning and will attract main chain fees but are rarer. User authentication and communication will be through nostr.

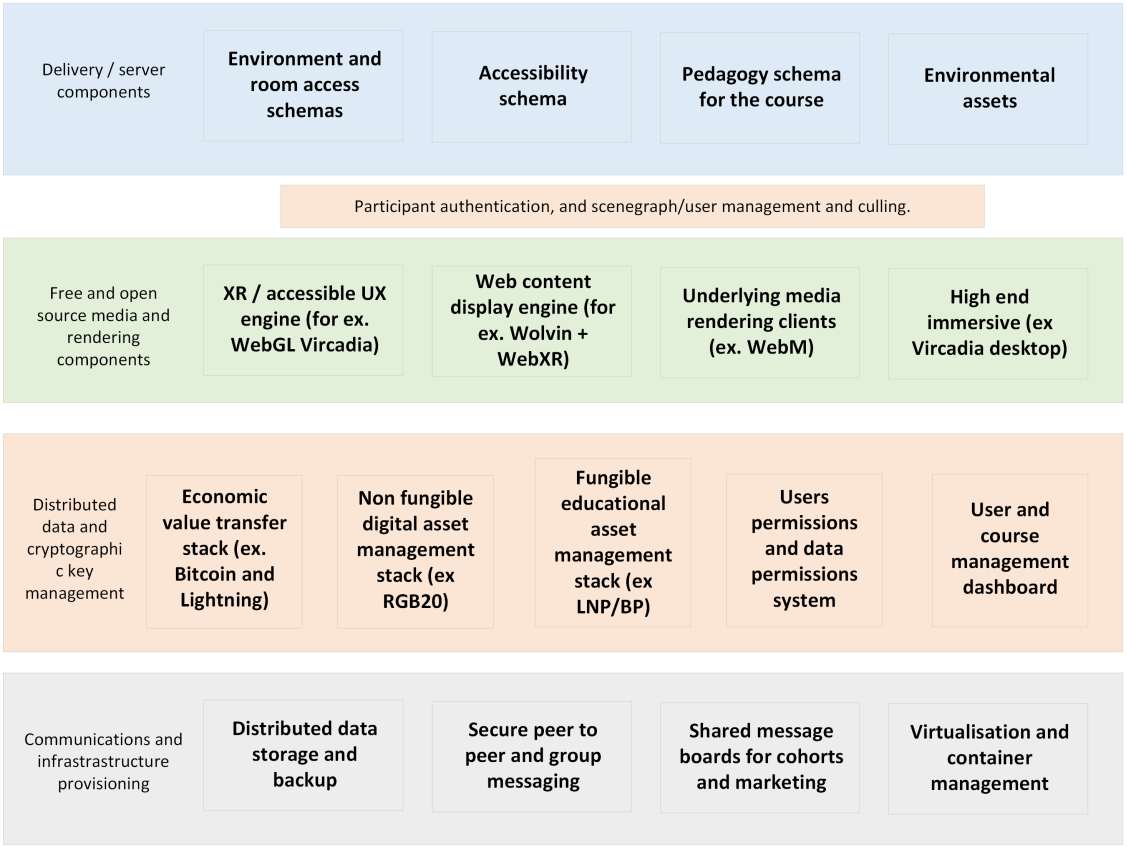


Figure 8.2: Functional elements for infrastructure.

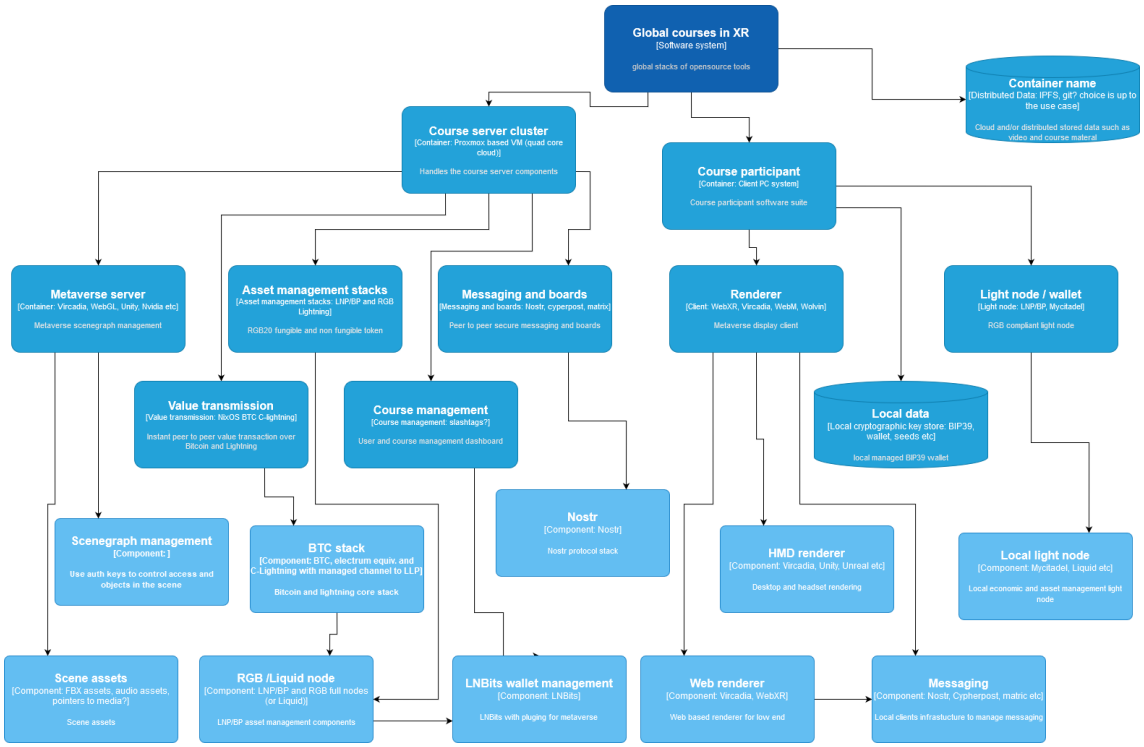


Figure 8.3: Client server C4 diagrams.

II Guides for deploying the software

8.5 Lab - virtualisation, networking, Bitcoin

8.5.1 Overview

This how-to document details the process of creating the system detailed in the accompanying book. It is intended to be complete. It is a how to guide.

8.5.1.1 Summary of software

Summarise the software and functionality

8.5.2 Prerequisites

Ensure that the BIOS / firmware / etc of the hardware you intend to use is up to date.

8.5.3 Network details

In the example setup provided here there are currently two networks:

1. The virtual server resides in a LAN with the following details:
   192.168.x.0/24
   Replace x with an integer between 0 and 254
   This LAN has a gateway to the Internet and DNS server configured. Of course, it could be replaced with a direct connection to the Internet, though for research and development purposes it is often better to work within a clean LAN and manage access to the Internet as required.
2. There is a virtual network configured on the virtual machine host upon which virtual machines can reside:
   This virtual network is not configured to bridge with the physical network adapter rather a virtual machine is configured as a gateway to route IP traffic through. This provides a level of isolation. More on this later (@todo).

8.5.4 Server configuration

8.5.4.1 Server hardware details

@todo

8.5.4.2 Disk configuration details

@todo

8.5.5 Proxmox VE

8.5.5.1 Installation and configuration

Version used: 7.1

Keep in mind that this setup uses the Proxmox VE installer (https://www.proxmox.com/en/proxmox-ve/get-started) which, as noted on the site, is a bare-metal installer and will erase all data on at least one disk. There are alternative methods to install Proxmox VE but these are not covered here.

A brief summary of the steps taken using Proxmox VE 7.1:

Dialogue 1 Choose the target harddisk (/dev/sda in this case).

Dialogue 2 Select country, time zone, keyboard layout.

Dialogue 3 Set a password (this is the root password, see proxmox hardening section), and email address.

Dialogue 4 Select a Network Interface Card (NIC) on which the management interface will be available and provide a hostname, IP address, gateway and DNS server.

In this example the following settings were used:

Hostname: proxmoximus.local IP address: 192.168.x.220 / 24 Gateway: 192.168.x.254 DNS server: 192.168.x.254

Either replace x with the integer used earlier and update the last octet of the gateway and server with that that corresponds to your setup (assuming the setup is local and has a local dns server or forwarder) or configure the values according to your intended setup.

Once the install has completed and the system has rebooted it is time to begin configuring. This is done (almost entirely) via the web interface, in this case, available at https:// proxmoximus | 192.168.x.220 : 8006

It is also possible to login to a shell via the local terminal and SSH (which is enabled by default @todo: in hardening, add keys and remove ability to login with password).

8.5.5.2 Software updates

If you are in a testing and non-production environment then it is possible access updates without a subscription as detailed here: https://pve.proxmox.com/wiki/Package_Repositories. Update `/etc/apt/sources.list` as detailed under the Proxmox VE No-Subscription Repository. This can be achieved via the local terminal, SSH or web interface (via Shell option).

For example, edit the file:

`nano /etc/apt/sources.list`

Add the following:

```
# PVE pve-no-subscription repository provided by proxmox.com,
# NOT recommended for production use
deb http://download.proxmox.com/debian/pve bullseye pve-no-subscription
```

To the existing:

```
deb http://ftp.uk.debian.org/debian bullseye main contrib

deb http://ftp.uk.debian.org/debian bullseye-updates main contrib

# security updates
deb http://security.debian.org bullseye-security main contrib
```

Resulting in:

```
deb http://ftp.debian.org/debian bullseye main contrib
deb http://ftp.debian.org/debian bullseye-updates main contrib

# PVE pve-no-subscription repository provided by proxmox.com,
# NOT recommended for production use
deb http://download.proxmox.com/debian/pve bullseye pve-no-subscription

# security updates
deb http://security.debian.org/debian-security bullseye-security main contrib
```

The Proxmox VE system will now retrieve updates for both itself and the base Debian system.

Then from a shell run:

```
$ apt update
$ apt upgrade
```

@todo: determine if system needs a reboot

8.5.5.3 Proxmox VE hardening

Links

@todo

Adding users

Add SSH keys and remove ability to login with password

8.5.6 Setup an internal only network in Proxmox VE

From the Web GUI navigate to Datacenter - > your server -> Network

From the menu select Create then Linux Bridge

Input the desired IPv4/CIDR in this case 192.168.y.0/24 and add a comment if desired ("Internal network" was used here). Note that y must not be the same as x previously used.

Name was left as vmbr1

Credit: https://dannyda.com/2020/06/01/how-to-create-an-internal-only-isolated-network-for-guest-os-virtual-machines-vm-on-proxmox-ve-pve-like-in-vmware-workstation-host-only-network-but-different/

8.5.7 Install and configure Internet gateway server virtual machine

VyOS was selected (https://vyos.io/)

8.5.7.1 Create an ISO of the stable version (as of writing 1.3.0)

@todo: the built version seemed to be a nightly release, is it possible to add a tag to get a stable build?

Follow the build instructions:

https://docs.vyos.io/en/latest/contributing/build-vyos.html

This document does not list this version (goes up to 10 "buster") but Debian 11 "bullseye" was successfully used in this setup.

Run the following commands:

```
$ apt install git
$ apt install build-essential
```

Follow the instructions here https://docs.docker.com/engine/install/debian/ to install Docker

Run the following commands:

```
$ git clone -b equuleus --single-branch https://github.com/vyos/vyos-build

$ docker run --rm -it --privileged -v $(pwd):/vyos -w /vyos vyos/vyos-build:equuleu
```

Then in the Docker terminal run the following commands:

```
./configure --architecture amd64

sudo make iso
```

8.5.7.2 Upload the ISO image to the Proxmox VE server

1. Via the web GUI navigate to Datacenter -> your server -> local.
2. In the right hand pane select ISO Images and then upload.
3. Upload the ISO image

Tip: you can also pass the checksum to the Proxmox VE upload tool

8.5.7.3 Create VyOS virtual machine

1. From the top right of the web GUI select Create VM
2. In the appearing dialogue type a Name "VyOS" and optionally select advanced and Start at boot
3. On the next tab select the target ISO image
4. On the System tab leave everything as default
5. n the Disk tab leave the defaults (this exceeds requirements https://docs.vyos.io/en/latest/installation/inst
6. On the CPU tab:
   Sockets: 1, Cores: 2
7. On the Memory tab
   Memory: 4096MiB
8. On the Network tab
   Choose the bridge with the internet vmbr0 (it is possible to add the second later) and leave the defaults including firewall
   Confirm all the settings on the next tab but **do not** select start after created
   Navigate to the newly created VM on the left-hand pane then selected Hardware from the menu that is presented on the right. Choose Add and then Network Device. In the dialogue that appears select the Internal network bridge (vmbr1 in this case) that was created earlier and leave all other options as is.
   So, the VM will have the following Network Devices:
   net0: Internet
   net1: Internal only
9. Start the VM and connect the console (top right)
10. Login with vyos and vyos
    Run the command:

    ```
    $ install image
    ```

11. Follow the instructions
12. Set the CD/DVD to none in Web GUI
13. Reboot

8.5.7.4 Configure VyOS

Open a noVNC window to the host
Login with vyos and vyos
Switch to configure mode:

```
vyos@vyos$ configure
vyos@vyos#
```

Then configure as desired. Below is configuration used in the setup here (if you use for inspiration do take care to replace the x and y octet values correctly with previously chosen values. The z octet value should be something unused in the outside LAN for which the host is physically connected):

```
set interfaces ethernet eth0 address '192.168.x.z/24'
set interfaces ethernet eth0 description 'OUTSIDE'
set protocols static route 0.0.0.0/0 next-hop 192.168.x.254 distance 1
set service dns forwarding system
set service dns forwarding name-server 192.168.x.254
set service dns forwarding listen-address 192.168.y.1
set service dns forwarding allow-from 192.168.y.0/24
set system name -server 192.168.x.254

set interfaces ethernet eth1 address '192.168.y.1/24'
set interfaces ethernet eth1 description 'INSIDE'

set nat source rule 100 outbound-interface eth0
set nat source rule 100 source address 192.168.y.0/24
set nat source rule 100 translation address masquerade

set service ssh listen-address 0.0.0.0
```

Once done remember to commit the config (correcting any misconfiguration) and save.

```
commit
save
```

Inspiration for the above was taken from: https://bertvv.github.io/cheat-sheets/VyOS.html
@todo: hardening, IDS, IPS

8.5.8 Install and configure a Debian virtual machine

This VM can be used for various tasks such as software compilation and testing of the networks. In this setup the Debian VM was used to test connectivity to the VyOS gateway and the Internet. It is also used in the subsequent stages to deploy a nix-bitcoin node.

In Proxmox VE create a new virtual machine and configure the network device to use the bridge 'vmbr1'.

Then install Debian and configure the network adapter within the VM with the following settings:

IP address: 192.168.y.2 Gateway: 192.168.y.1 DNS: 192.168.y.1

Test that the VM has Internet connectivity.

8.5.9 Deploying the nix-bitcoin node

This deployment follows the documentation:

https://github.com/fort-nix/nix-bitcoin/#get-started

Take note of the hardware requirements:

https://github.com/fort-nix/nix-bitcoin/blob/master/docs/hardware.md

In the main, the install guide (https://github.com/fort-nix/nix-bitcoin/blob/master/docs/install.md) is followed verbatim and notes with a reference to particular sections are added where appropriate.

Optional - a small exception in regards to this setup is that a separate virtual disk (located on a different physical drive mirror (RAID 1)) was used to store the bitcoin database - this is optional and details are provided on how to achieve it. Also detailed is how to configure the network when using the minimal image.

8.5.9.1 Acquiring NixOS

Following section 1.1 make sure the latest NixOS is obtained i.e. do not just copy the whole wget command outright and make sure to verify the hash against trusted sources before using the image.

Download the minimal ISO image (https://nixos.org/download.html)

Verify the hash

Upload the ISO to Proxmox VE server

8.5.9.2 Create a new VM

Name: NixOS

Follow the setup and leave everything as default until the CPU page. The following configuration was used, which should exceed the minimum requirements:

Cores: 4

Memory: 4096MiB = 4.2GB

Network: vmbr1 (Internal Network)

Do NOT check the select the start the VM checkbox

Next, an additional drive will be configured in Proxmox VE. This will then be used to store the bitcoin database within the NixOS VM.

Select Datacenter -> server name and then from the right pane Disks -> LVM-Thin. Then select Create: Thinpool

From the dialogue select the disk and type a name “data” was used in this setup. This provisions a vg with the name *data* and a name *data* @todo: review

Navigate back to the VM created and choose Hardware and then Add -> Hard Disk

Choose “data” from Storage and then set the size to 560 GiB which equates to about 600GB

Now, continue from section 1.3 in the install instructions

Start the VM and connect a console

```
sudo -i
```

With the SeaBios that was used in this setup the file does not exist and Legacy Boot (MBR) should be followed (option 2)

Note: no consideration is currently given for encrypted partitions within the Proxmox VE setup

Enable the OpenSSH daemon

```
services.openssh.permitRootLogin = "yes";
```

Configure the network config in configuration.nix (remember to replace y with the chosen value)

```
networking.useDHCP = false;
networking.interfaces.ens18.useDHCP = false;

networking.interfaces.ens18.ipv4.addresses = [ {
  address= "192.168.y.3";
  prefixLength = 24;
} ];
networking.defaultGateway = "192.168.y.1";
networking.nameservers = ["192.168.y.1"];
networking.hostName = "nixicon";
```

Although the IP above will be assigned once the nix-bitcoin is deployed the installation cannot continue without a connection to the Internet so that needs to be configured:

```
$ ifconfig ens18 192.168.y.3
$ ifconfig ens18 255.255.255.0
$ ip route add 192.168.y.0/24 dev ens18 scope link src 192.168.y.3
```

Then add the nameserver:

```
nano /etc/resolv.conf
```

Add:

```
nameserver 192.168.y.1
```

Once the above is complete and successful networking is verified
Run the following command:
`nixos-install`
Set the root password and then reboot.

8.5.9.3 Configure the additional drive (optional)

As the additional drive was not configured at the time of the install then the parted utility will need to be available. To achieve this, edit the configuration.nix file
`nano /etc/nixos/configuration.nix`
and add the following:

```
environment.systemPackages = with pkgs; [
    parted
];
```

Then issue the following command:
`nixos-rebuild switch`
Determine the desired drive, fdisk can assist:
`fdisk -l`
Note: in this sytem the desired drive is /dev/sdb with 560GiB capacity but sdx is used in the following examples:
Then partition:
`parted /dev/sdx`

```
(parted) mklabel msdos
(parted) mkpart primary
File system type? ext4
Start? 0%
End? 100%
quit
```

(note: it is possible to combine the above as a single line command)

Then create the file system:

`mkfs.ext4 -L data /dev/sdx1`

Make a note of the UUID as this will be used in the next steps to mount the volume

8.5.9.4 Create port forwarding rules for SSH (optional)

Providing SSH access to the VMs from outside the private network makes it easier to configure them (ability to copy and paste UUIDs etc.)

This involve updates to VyOS configuration and can be temporary.

Login to the vyos, you should be able do this from your local machine now as apposed to the console

ssh vyos@192.168.x.z

Debian 192.168. y .2

The following commands were issued to the VyOS router (obiously replacing y with the value chosen earlier)

```
configure

set nat destination rule 12 description 'Port Forward: 2222 to 22 SSH on 192.168.y.
set nat destination rule 12 destination port '2222'
set nat destination rule 12 inbound-interface 'eth0'
set nat destination rule 12 protocol 'tcp'
set nat destination rule 12 translation address '192.168.y.2'
set nat destination rule 12 translation port '22'

commit
```

Now test

Note: for the Debian VM the user account may need to be added to the SSH user group

Note: you could SSH from Debian to all other hosts

NixOS 192.168. y .3

Assuming access to the Debian VM via SSH is working then from the same VyOs configure session issue the following:

```
set nat destination rule 13 description 'Port Forward: 2223 to 22 SSH on 192.168.y.
set nat destination rule 13 destination port '2223'
set nat destination rule 13 inbound-interface 'eth0'
set nat destination rule 13 protocol 'tcp'
set nat destination rule 13 translation address '192.168.y.3'
set nat destination rule 13 translation port '22'

commit
```

Test and if all is well, save the VyOS configuration:

```
save
```

Credit: https://support.vyos.io/en/kb/articles/nat-principles

Having SSH access to both the Debian and NixOS VMs will make the next stages of the process a little easier

@todo hardening (SSH e.g. add keys, remove plain text or remove SSH access entirely)

8.5.9.5 Prepare nix-bitcoin NixOS package

This section continues to follow the guide from Nix Installation.

Note: this part of the guide will be executed on the Debian VM that was installed earlier

The next steps will follow section 2.

You may need to add your user to the sudoers if it is not a member already

In Debian this can be achieved with the following commands

Switch to root

`su`

Then

`sudo usermod -a -G sudo username`

Exit both the root and user session and then log back in as the user

Important: ensure that when downloading the multi-user NixOS that the latest is obtained (listed at https://nixos.org/download.html). I.e. dont just copy and paste verbatim.

Note: It is possible to determine the latest version by navigating to: https://nixos.org/nix/install and this will redirect to for example: https://releases.nixos.org/nix/nix-2.6.0/install at the time of writing. From here you could quickly santiy check the redirect by heading to: https://releases.nixos.org/?prefix=nix/

You could (as in the example on the NixOS website) use curl with a -L option which will ignore the redirect

Enter a directory to receive the files. ~/Downloads was chosen for this setup

For completeness the following commands were issued:

`curl -o install-nix-2.6.0 https://releases.nixos.org/nix/nix-2.6.0/install`

with the -o option writing the contents to a file rather than displaying on screen

then

`curl -o install-nix-2.6.0.asc https://releases.nixos.org/nix/nix-2.6.0/install.a`

then

`gpg2 --keyserver hkps://keyserver.ubuntu.com --recv-keys B541D55301270E0BCF15CA5`
`gpg2 --verify ./install-nix-2.6.0.asc`

Which are similarly detailed here: https://nixos.org/download.html#nix-verify-installation

Note: it is not required to run the script as sudo. It will prompt for permission.

In this setup the:

```
substitute = false
```

was added to /etc/nix/nix.conf as detailed.

Run the script.

Exit the terminal and login in again as per the message:

```
Try it! Open a new terminal, and type:

  $ nix-shell -p nix-info --run "nix-info -m"
```

The next part continues with setting up the deployment directory
Stood in the home directory or one just off it, follow the instructions provided.
Once the above is complete continue with the deploy with krops section.
Follow the instructions and edit the SSH config. You will need a public/private key pair for this and this article could be useful.
The config file used in this setup is shown below:

```
Host nixicon
    # FIXME
    Hostname 192.168.y.3
    User root
    PubkeyAuthentication yes
    # FIXME
    IdentityFile ~/.ssh/id_ed25519
    AddKeysToAgent yes
```

And for reference the krops/deploy.nix is as follows:

```
let
  # FIXME:
  target = "root@nixicon";

  extraSources = {
    "hardware-configuration.nix".file = toString ../hardware-configuration.nix;
  };

  krops = (import <nix-bitcoin> {}).krops;
in
krops.pkgs.krops.writeDeploy "deploy" {
  inherit target;

  source = import ./sources.nix { inherit extraSources krops; };

  # Avoid having to create a sentinel file.
  # Otherwise /var/src/.populate must be created on the target node to signal krops
  # that it is allowed to deploy.
  force = true;
}
```

In subsection 3 the guide shows how to optionally disallow substitutes. This was set to true in this setup.
In subsection 4 the guide details copying hardware-configuration.nix file to the deployment directory and then in subsection 5 making edits to the configuration.nix file to turn on desired modules. There are some important notes relevant to this setup to make here:

Additional hard drive configuration No edits were made to hardware-configuration.nix as per the warning at the top of the file. For reference here is the file from this setup:

```
# Do not modify this file!  It was generated by ‘nixos-generate-config’
# and may be overwritten by future invocations.  Please make changes
# to /etc/nixos/configuration.nix instead.
{ config, lib, pkgs, modulesPath, ... }:

{
  imports =
    [ (modulesPath + "/profiles/qemu-guest.nix")
    ];

  boot.initrd.availableKernelModules = [ "ata_piix" "uhci_hcd" "virtio_pci" "virtio
  boot.initrd.kernelModules = [ ];
  boot.kernelModules = [ ];
  boot.extraModulePackages = [ ];
  boot.loader.grub.device = "/dev/sda";

  fileSystems."/" =
    { device = "/dev/disk/by-uuid/UUID_1";
      fsType = "ext4";
    };

  swapDevices =
    [ { device = "/dev/disk/by-uuid/UUID_2"; }
    ];

  hardware.cpu.intel.updateMicrocode = lib.mkDefault config.hardware.enableRedistri
}
```

Rather, the additional hard drive was configured in the configuration.nix as shown here:

```
fileSystems."/var/lib" =
{ device = "/dev/disk/by-uuid/UUID_3";
  fsType = "ext4";
};
```

This mounts /var/lib (which contains the bitcoin database etc.) to the additional drive.

Static IP configuration To configure the static IP add the following:

```
networking.useDHCP = false;
networking.interfaces.ens18.useDHCP = false;

networking.interfaces.ens18.ipv4.addresses = [ {
  address= "192.168.y.3";
  prefixLength = 24;
} ];
```

```
networking.defaultGateway = "192.168.y.1";
networking.nameservers = ["192.168.y.1"];
networking.hostName = "nixicon";
```

SSH configuration Below is the snipet of configuration. Note: paste the contents of `~/.ssh/id_ed25519.pub` where the `# FIXME: Replace this with your SSH pubkey` appears

```
services.openssh = {
  enable = true;
  passwordAuthentication = false;
};
users.users.root = {
  openssh.authorizedKeys.keys = [
    # FIXME: Replace this with your SSH pubkey
    "ssh-ed25519 LONG_KEY user@debian"
  ];
};
```

Services configuration Last but not least, the following services are enabled in this setup:

```
services.clightning.enable = true;
services.rtl.enable = true;
services.rtl.nodes.clightning = true;
services.electrs.enable = true;
services.backups.enable = true;
```

Once the configuration.nix file has been updated continue from subsection 6.

The how-to continues with a guide to setting up a Vircadia domain server and metaverse server

8.6 Lab - Vircadia

8.6.1 Overview

This part of the how-to serves as a guide to setting up a Vircadia domain server and metaverse server within the Proxmox VE environment.

To familiarise with the technology stack the Vircadia architecture overview document is a good place to start and the GitHub contains documentation and source.

8.6.2 Deploy a Vircadia domain server

There are few different options to deploy a server. This guide will use the Linux compile from source method.

Various Linux distributions are supported and in this setup, Ubuntu 20.04 was selected.

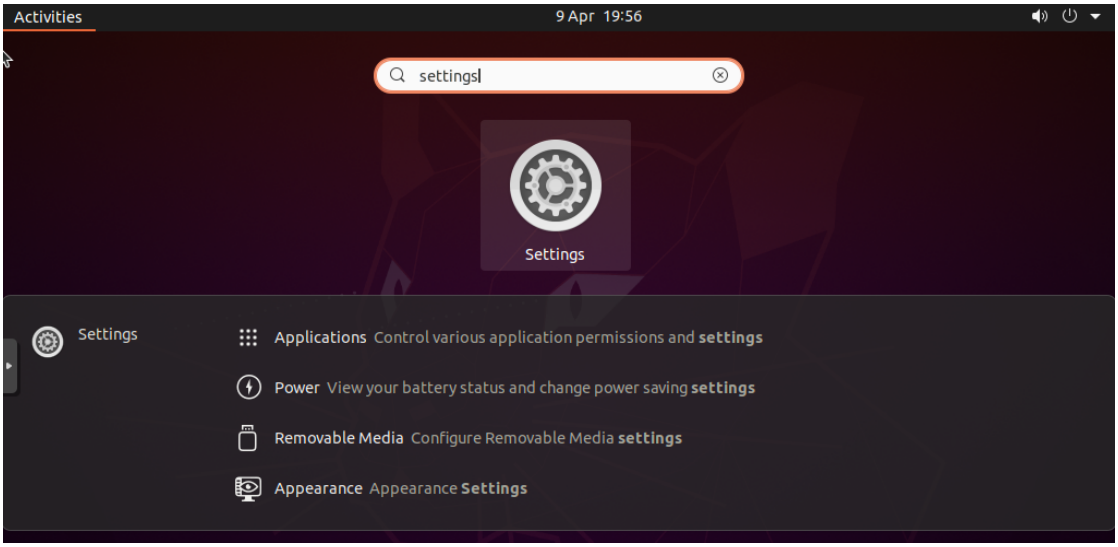


Figure 8.4: Ubuntu 20.04 Desktop Settings

8.6.2.1 Prepare a virtual instance of Ubuntu 20.04 in the Proxmox Virtual Environment

First, obtain the Ubuntu 20.04 desktop image.

Then deploy a virtual machine in Proxmox VE as was done with VyOS and Debian in the previous sections. The following values were selected for this setup:

Disk drive: 64GiB
CPU: 2 sockets 2 cores
RAM: 8192GiB
Network adapter: vmbr1 (internal)
Name: vircadia-server

When prompted by the installer to choose the packages to install choose ‘minimal’.

Remember to remove the media.

Once booted, head to settings:

Then configure the network connection with the manual method:

With the following:

IP address: 192.168.y.4
Gateway: 192.168.y.1
DNS: 192.168.y.1
Mask 255.255.255.0

Run the software updater.

Restart and run the software updater again.

Once the Operating System is up to date open a terminal and install git:

`sudo apt install git`

Follow the Vircadia build instructions along side this how-to guide.

Stood in your home directory or similar run the following:

```
git clone https://github.com/vircadia/vircadia-builder.git
cd vircadia-builder
chmod +x vircadia-builder
```

As this setup requires both the domain server and the ICE server, run the following:

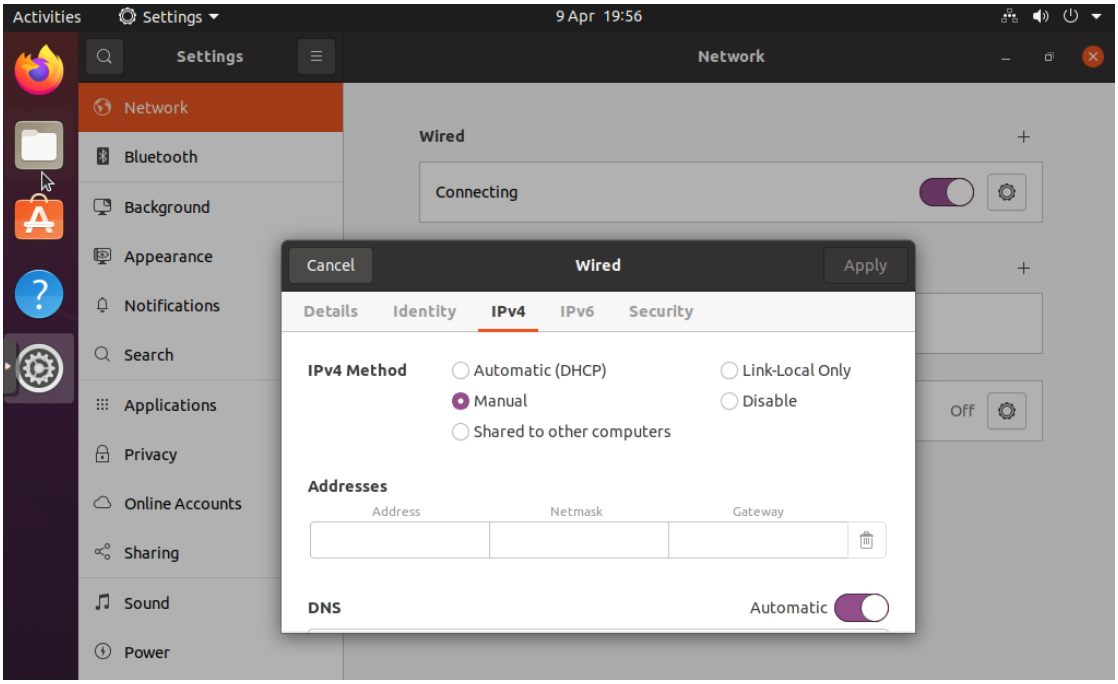


Figure 8.5: Ubuntu 20.04 Desktop Settings - Network

./vircadia-builder –build=server,ice-server

It is also possible to add a 'client' option but this was not opted for in this setup as the client was Windows based.

Follow the prompts (defaults were accepted in this setup). The installation process will begin as shown below:

The first stage of the installer will install dependency packages, follow the instruction and then if prompted run the build command again.

Note: if you have followed the guide then Qt will not be installed on the target system, however, the installer will build the correct version - see below:

Once complete (which could take several hours for the Qt step) a text output similar to the following should be presented:

```
Cleaning up install directory...done
Copied : 4626
Skipped: 3208
Deleted: 0
Creating script for assignment-client...done.
Creating script for domain-server...done.
Creating service for assignment-client...done.
Creating service for domain-server...done.
Reloading systemd config... done.


############################################################
# Setting up desktop
############################################################
```

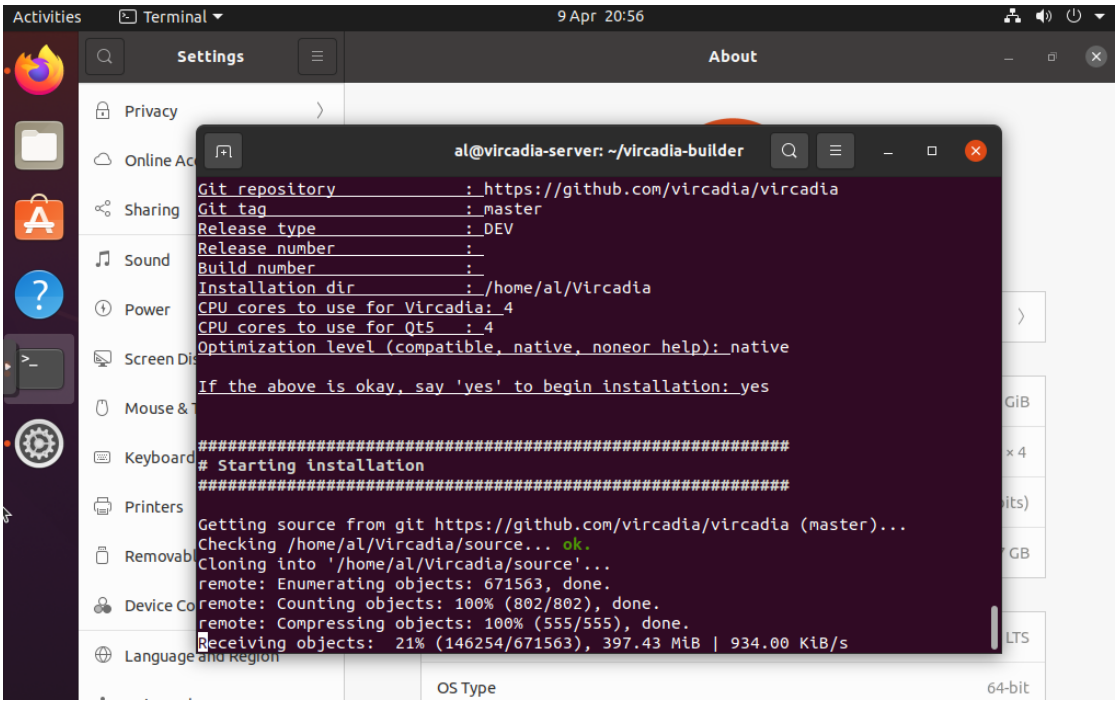


Figure 8.6: Vircadia build settings and installation screen grab

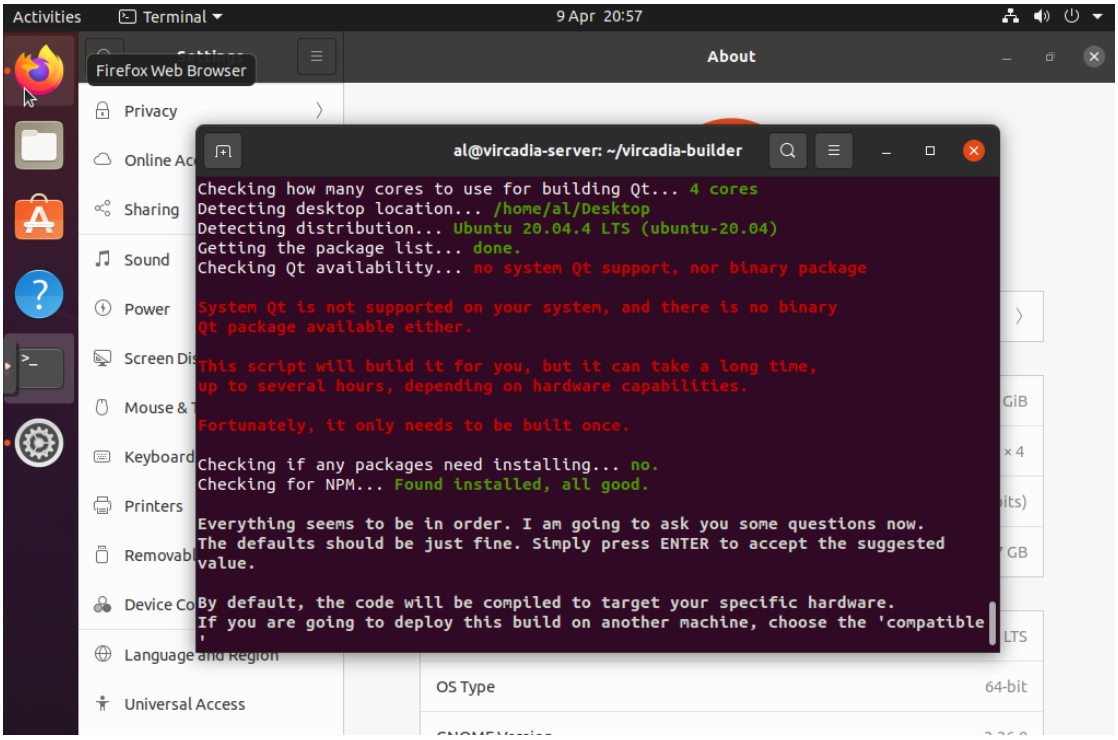


Figure 8.7: Vircadia build Qt warning

```
interface not built, skipping desktop setup
```

Navigate up one from the build directory and into the Vircadia folder. In here there should be a build folder with the built binaries and accompanying scripts - these are the scripts that will be run later (@todo: section link: ### Configure the Vircadia server) once port forwarding is configured.

8.6.2.2 Configure port forwarding for Vircadia services

The following ports are required:

40100 (+0): (tcp) administrative http connection

40101 (+1): (tcp) administrative https (encrypted) connection

40102 (+2): (udp) main connection from clients

40103 (+3): (udp) main connection from clients (encrypted)

Note: in this setup non TLS versions are currently used for testing.

Important: for a production version of the system it would be prudent to enable TLS and completely disallow non TLS traffic (i.e. remove the port forwarding rules)

```
set nat destination rule 15 description 'Port Forward: 40100 (+0): (tcp) administra
set nat destination rule 15 destination port '40100'
set nat destination rule 15 inbound-interface 'eth0'
set nat destination rule 15 protocol 'tcp'
set nat destination rule 15 translation address '192.168.y.4'
set nat destination rule 15 translation port '40100'

set nat destination rule 16 description 'Port Forward: 40101 (+1): (tcp) administra
set nat destination rule 16 destination port '40101'
set nat destination rule 16 inbound-interface 'eth0'
set nat destination rule 16 protocol 'tcp'
set nat destination rule 16 translation address '192.168.y.4'
set nat destination rule 16 translation port '40101'

set nat destination rule 17 description 'Port Forward: 40102 (+2): (udp) main conne
set nat destination rule 17 destination port '40102'
set nat destination rule 17 inbound-interface 'eth0'
set nat destination rule 17 protocol 'tcp'
set nat destination rule 17 translation address '192.168.y.4'
set nat destination rule 17 translation port '40102'

set nat destination rule 18 description 'Port Forward: 40103 (+3): (udp) main conne
set nat destination rule 18 destination port '40103'
set nat destination rule 18 inbound-interface 'eth0'
set nat destination rule 18 protocol 'tcp'
set nat destination rule 18 translation address '192.168.y.4'
set nat destination rule 18 translation port '40103'

commit

save
```

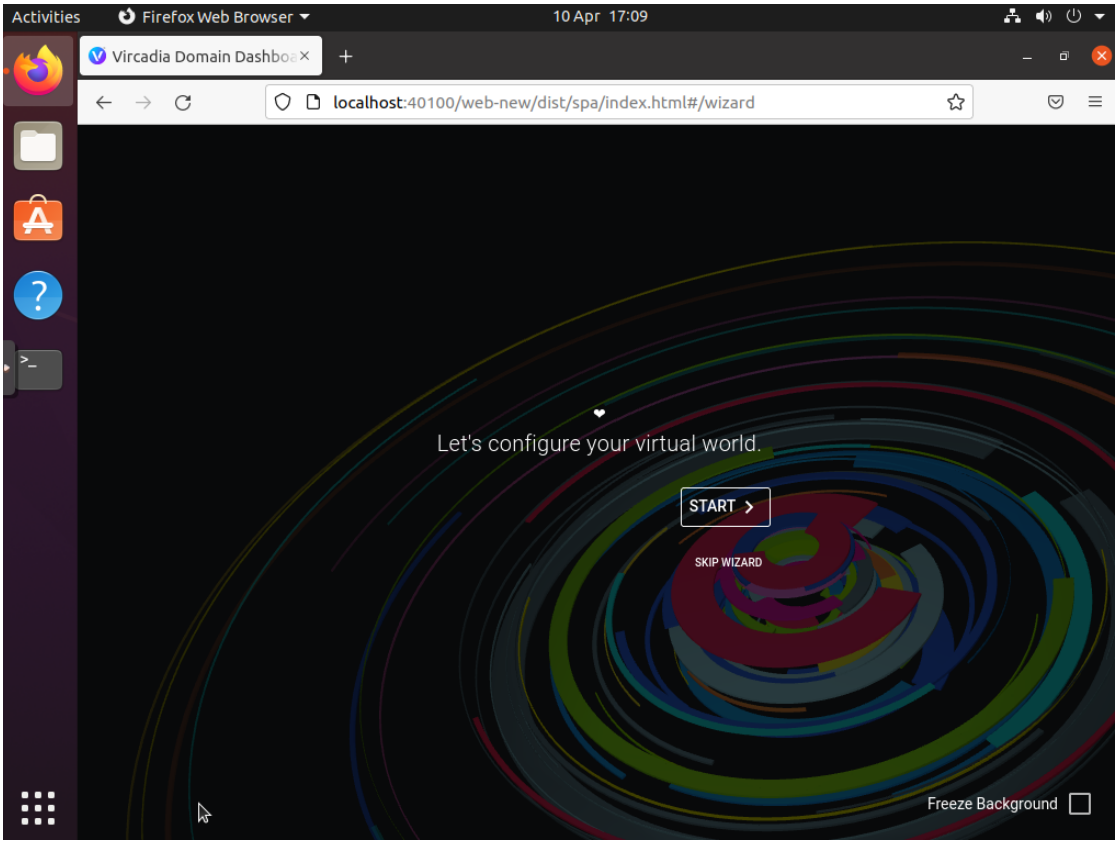


Figure 8.8: Vircadia server configuration landing page

8.6.2.3 Configure port forwarding for the ICE server

```
set nat destination rule 21 description 'Port Forward for ice-server: 7337 to 7337
set nat destination rule 21 destination port '7337'
set nat destination rule 21 inbound-interface 'eth0'
set nat destination rule 21 protocol 'tcp'
set nat destination rule 21 translation address '192.168.y.4'
set nat destination rule 21 translation port '7337'

commit

save
```

8.6.2.4 Configure the Vircadia server

As per the information message:

"Connect a web browser to the server at port 40100. (If you are on the machine that the server is running on, this would be http://localhost:40100) Complete the initial setup wizard and you should have a functioning domain."

With the port forwarding in place it should be possible to access the web interface on: 192.168.x.z:40100

Start the configuration:

Select skip on the import settings and/or content page:

Select skip on the connect to metaverse account page:

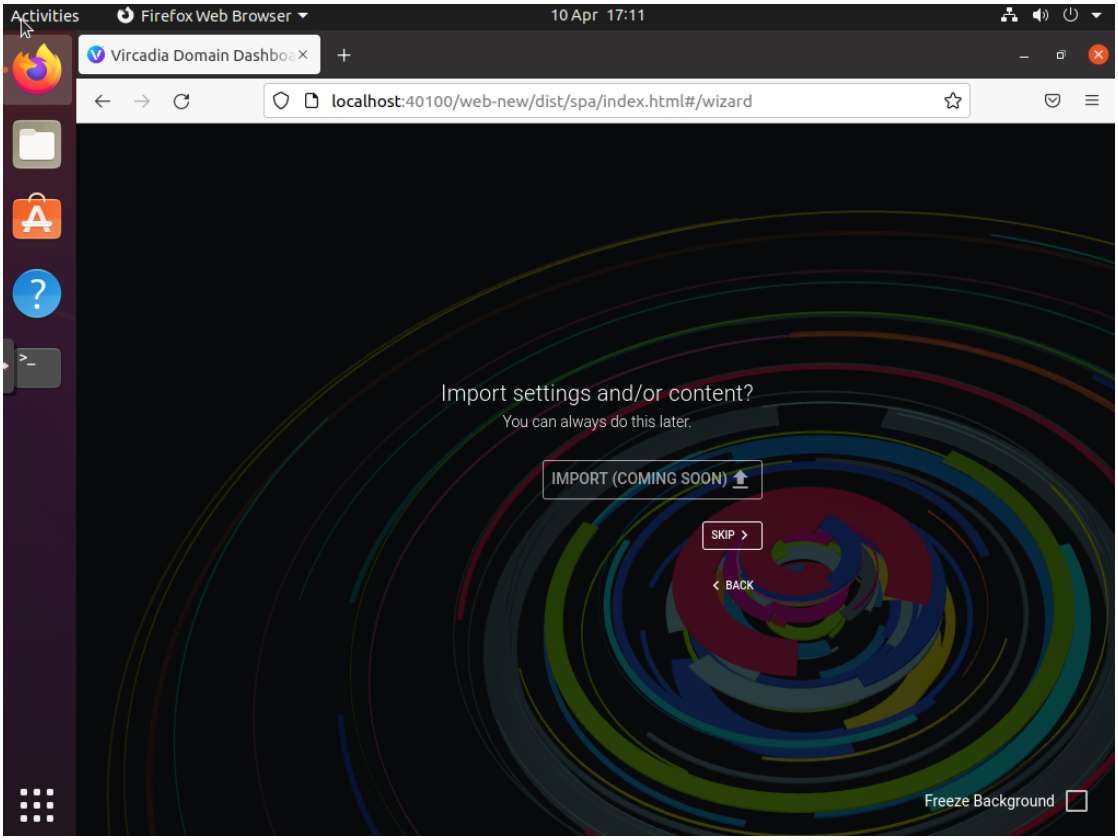


Figure 8.9: Vircadia server configuration import page

Configure security settings for your domain:

Create an admin user for the web panel:

Choose if you would like to turn performance mode on (in the setup described here performance mode was turned on):

Complete the installation.

8.6.3 Deploy a Vircadia metaverse server

Installation and configuration here follows the Vircadia metaverse build guide and Iamus: Notes On Development.

It is possible to install and run the Vircadia metaverse server on the same server as the domain server, however, in this setup another VM was used (separation of concerns).

Note: make sure to put VM disk on the first local-lvm partition and not the Bitcoin specific one.

Create another VM as in the previous steps with the following configuration:

Disk drive: 64GiB
CPU: 2 sockets 2 cores
RAM: 8192GiB
Network adapter: vmbr1 (internal)
Name: vircadia-metaverse-server

Perform a minimal install of Ubuntu 20.04 Desktop and configure the network as follows:

IP address: 192.168.y.5

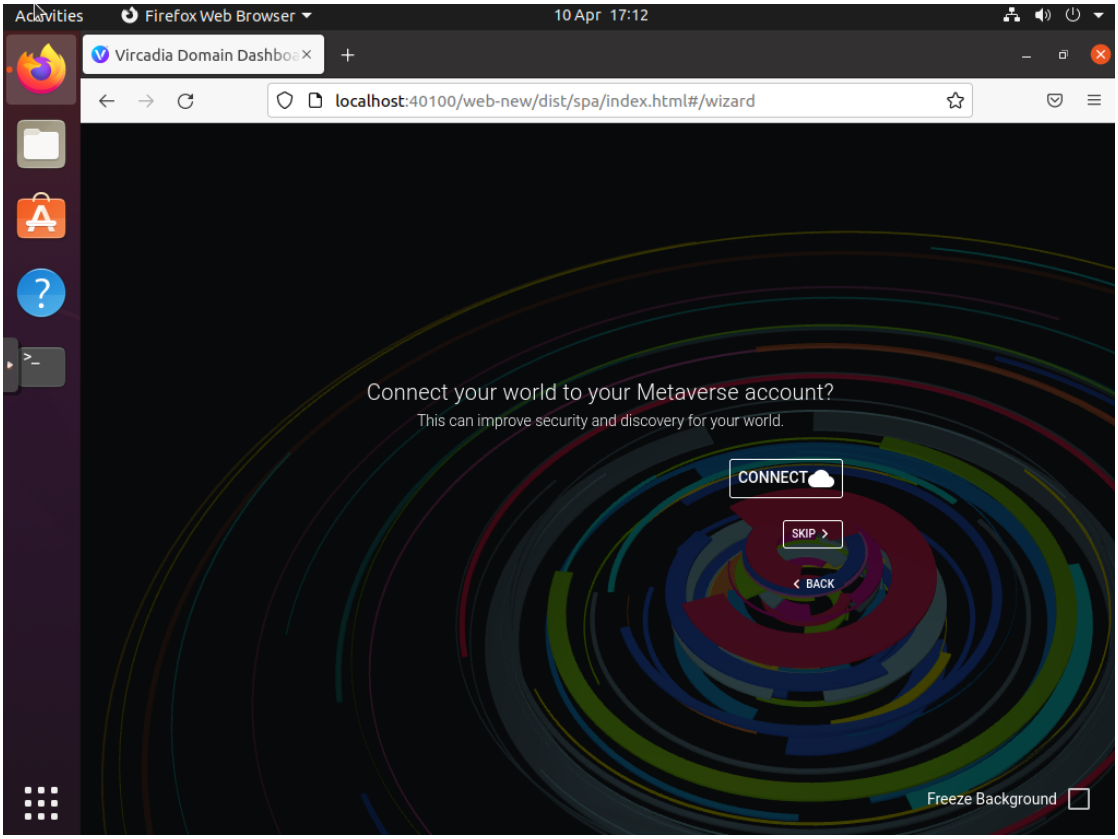


Figure 8.10: Vircadia server configuration import page

Gateway: 192.168.y.1
DNS: 192.168.y.1
Mask 255.255.255.0

Run the software updater.

Restart and run the software updater again.

8.6.3.1 Install Node.js and NPM

Following the building and configuration guide:

Note: as of writing the Node and NPM versions in the package manager are too low (node > 14 and npm > 6 are required) so do not use those. Instead navigate to: https://nodejs.org/en/download/ and get the latest LTS (version: 16.14.2 (includes npm 8.5.0) as of writing).

The following is taken from the Node installation guide:

```
sudo mkdir /usr/local/lib/nodejs
sudo tar -xJvf node-v16.14.2-linux-x64.tar.xz -C /usr/local/lib/nodejs/

nano ~/.profile
```

Add:

```
export PATH=/usr/local/lib/nodejs/node-v16.14.2-linux-x64/bin:$PATH
```

and refresh (@todo) and check

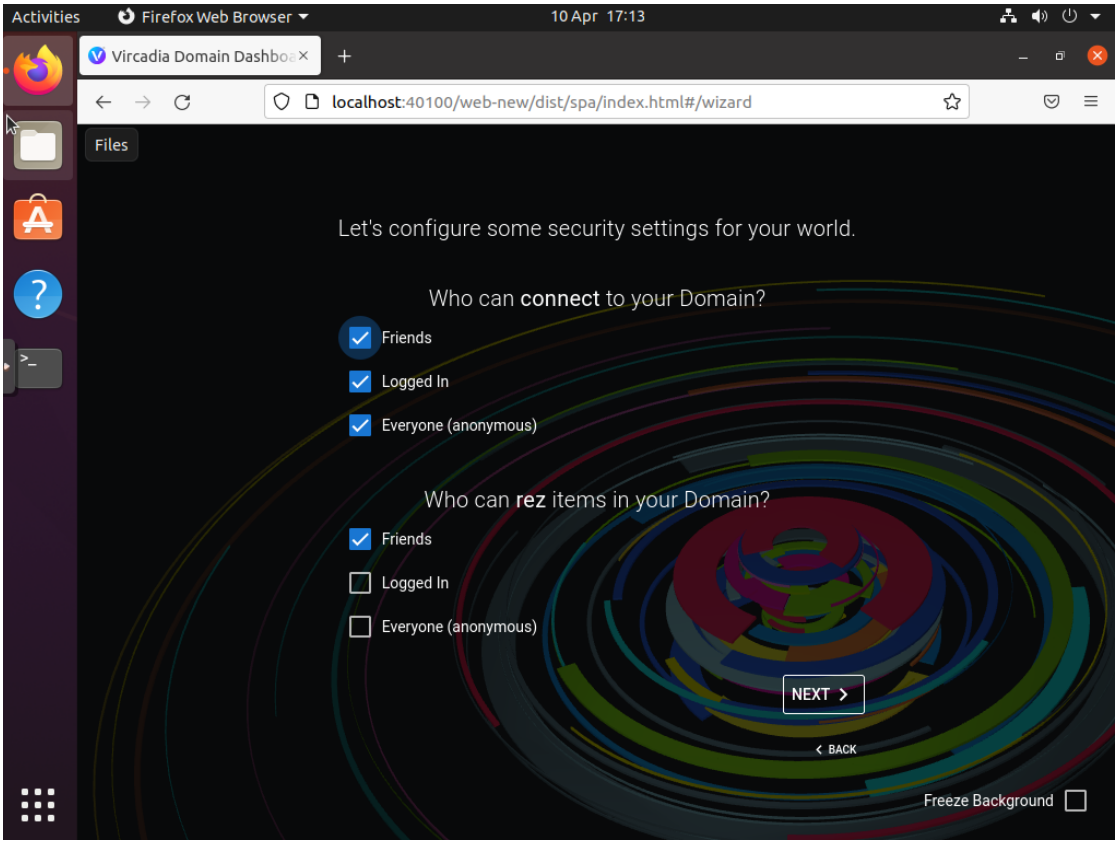


Figure 8.11: Vircadia server configuration import page

```
$ node -v

$ npm version

$ npx -v
```

8.6.3.2 Installation of the Vircadia metaverse server

Navigate to ~ (or where you would like to locate the meteverse server repository) and then run the following:

```
$ git clone https://github.com/vircadia/vircadia-metaverse.git

Cloning into 'vircadia-metaverse'...
remote: Enumerating objects: 5134, done.
remote: Counting objects: 100% (1240/1240), done.
remote: Compressing objects: 100% (700/700), done.
remote: Total 5134 (delta 862), reused 823 (delta 488), pack-reused 3894
Receiving objects: 100% (5134/5134), 1.04 MiB | 1.10 MiB/s, done.
Resolving deltas: 100% (3539/3539), done.
```

Change to the vircadia-metaverse directory and run the following command:

```
npm install
```

Note: As of writing the Git tags were old so the latest commit was opted for.

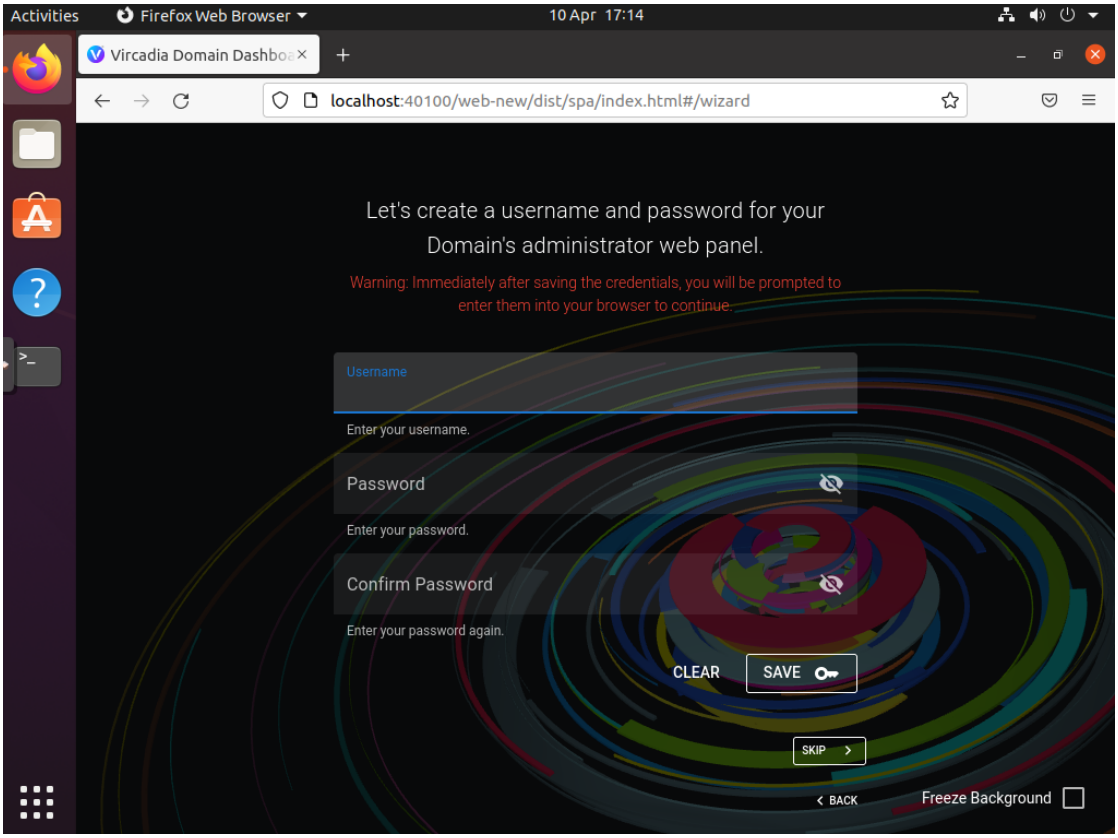


Figure 8.12: Vircadia server configuration import page

8.6.3.3 Configure the Mongo DB for the metaverse server

Note: the Mongo DB could run on a separate VM (further separation of concerns).

The Vircadia metaverse build guide is shown using version 4.4 so this guide will use the same (though it maybe possible to use a later version (@todo: a comment in Discord mentions success with 5.0.2):

https://www.mongodb.com/docs/v4.4/tutorial/install-mongodb-on-ubuntu/

Follow the installation instructions for Ubuntu 20.04 (assuming that this is the distribution that has been chosen to install the metaverse server on).

Once the Mongo DB is complete it can be verified as below:

```
al@vircadia-metaverse-server:~$ mongo
MongoDB shell version v4.4.13
connecting to: mongodb://127.0.0.1:27017/?compressors=disabled&gssapiServiceName=mo
Implicit session: session { "id" : UUID("c7fdcc61-f921-4fff-ad44-27840a8afea4") }
MongoDB server version: 4.4.13
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        https://docs.mongodb.com/
Questions? Try the MongoDB Developer Community Forums
        https://community.mongodb.com
---
The server generated these startup warnings when booting:
```

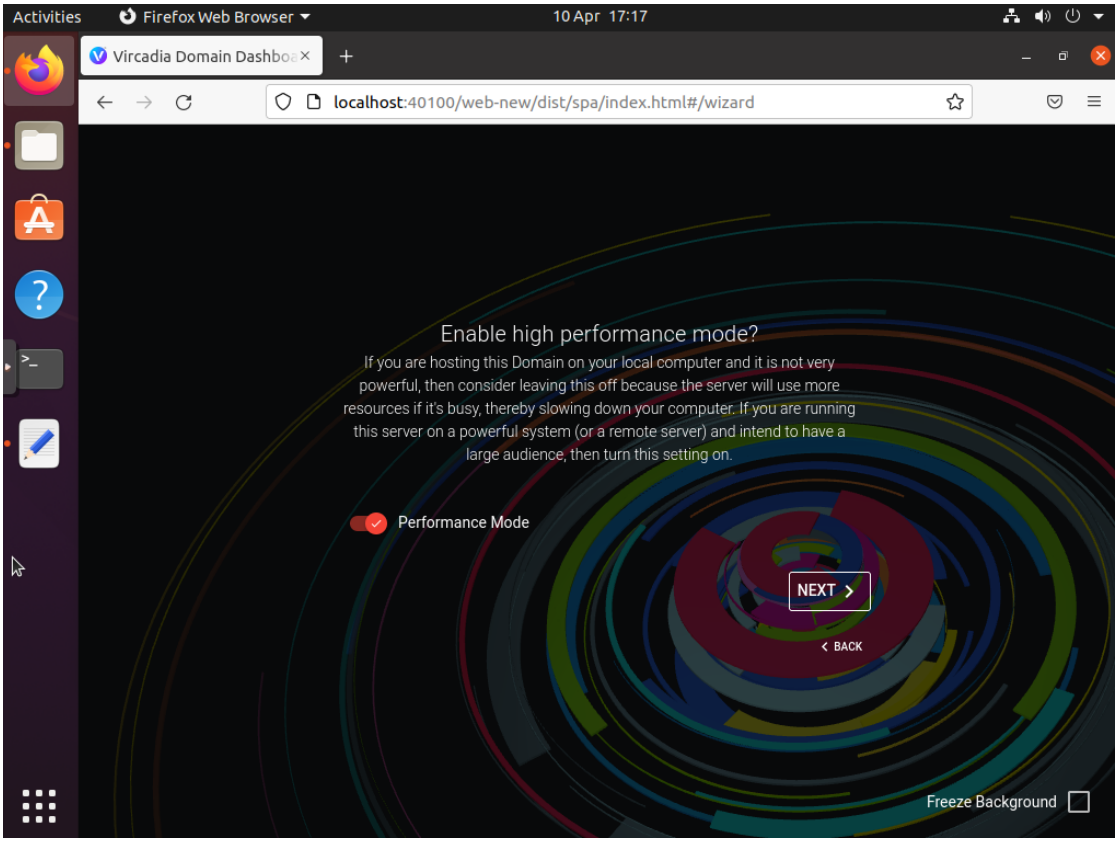


Figure 8.13: Vircadia server configuration import page

```
        2022-04-11T12:50:28.108+01:00: Using the XFS filesystem is strongly recomme
        2022-04-11T12:50:28.852+01:00: Access control is not enabled for the databa
---
---

        Enable MongoDB's free cloud-based monitoring service, which will then recei
        metrics about your deployment (disk utilization, CPU, operation statistics,

        The monitoring data will be available on a MongoDB website with a unique UR
        and anyone you share the URL with. MongoDB may use this information to make
        improvements and to suggest MongoDB products and deployment options to you.

        To enable free monitoring, run the following command: db.enableFreeMonitori
        To permanently disable this reminder, run the following command: db.disable
---
>
```

Next:

```
mongo
db.disableFreeMonitoring()
use admin
db.createUser({user:"adminer", pwd: "aReallyComplexPassword1", roles: [ "root" ]})
use admin
```

```
db.createUser({user:"backuper", pwd: "aReallyComplexPassword2", roles: [ "backup" ]
use admin
db.createUser({user:"cadiauser", pwd: "aReallyComplexPassword3", roles: [{ role: "r
```

Then be sure to follow the step to add authorisation to mongo:
Edit /etc/mongod.conf and add:

```
security:
    authorization: enabled
```

then run the following command to restart Mongo DB:

```
sudo systemctl restart mongod.
```

8.6.3.4 Configure the iamus configuration file

Next add the an iamus.json configuration file to the base directory.
You can take inspiration from:
1) the example in the build readme as shown below:

```
{
    "metaverse": {
        "metaverse-name": "My Metaverse",
        "metaverse-nick-name": "MyVerse",
        "metaverse-server-url": "https://metaverse.example.org:9400/",
        "default-ice-server-url": "ice.example.org:7337"
    },
    "server": {
        "cert-file": "config/cert.pem",
        "key-file": "config/privkey.pem",
        "chain-file": "config/chain.pem"
    },
    "metaverse-server": {
        "metaverse-info-addition-file": "config/metaverse_info.json"
    },
    "database": {
        "db": "myverse",
        "db-host": "metaverse.example.org",
        "db-user": "DBUSER",
        "db-pw": "DBUSERPASSWORD"
    },
    "debug": {
        "loglevel": "debug",
        "devel": true,
    }
}
```

2) the src/config.ts file in the @todo dir:

```
{
    // The metaverse identity
    'metaverse': {
        'metaverse-name': 'Vircadia noobie',
        'metaverse-nick-name': 'Noobie',
        'metaverse-server-url': '',   // if empty, set to self
        'default-ice-server-url': '', // if empty, set to self
        'dashboard-url': 'https://dashboard.vircadia.com'
    },
    // Server network parameters
    'server': {
        'listen-host': '0.0.0.0',
        'listen-port': 9400,
        'key-file': '',           // if supplied, do https
        'cert-file': '',
        'max-body-size': 300000,  // maximum body size for input JSON bodies
        'static-base': '/static', // base of static data URL
        'user-config-file': './iamus.json', // startup config over-ride
        'server-version': {       // overlaid with VERSION.json
            'version-tag': '1.1.1-20200101-abcdefg'
        }
    },
    // Authorization token parameters
    'auth': {
        'domain-token-expire-hours': 24 * 365,  // one year
        'owner-token-expire-hours': 24 * 7      // one week
    },
    // Control of the metaverse operations
    'metaverse-server': {
        'http-error-on-failure': true,  // whether to include x-vircadia error head
        'error-header': 'x-vircadia-error-handle',

        'metaverse-info-addition-file': './metaverse_info.json',
        'max-name-length': 32,      // the max characters a domain, place, account,

        'session-timeout-minutes': 5,
        'heartbeat-seconds-until-offline': 5 * 60,      // seconds until non-heartb
        'domain-seconds-until-offline': 10 * 60,        // seconds until non-heartb
        'domain-seconds-check-if-online': 2 * 60,       // how often to check if a
        'handshake-request-expiration-minutes': 1,      // minutes that a handshake
        'connection-request-expiration-minutes': 60 * 24 * 4, // 4 days
        'friend-request-expiration-minutes': 60 * 24 * 4,     // 4 days

        'place-current-timeout-minutes': 5,             // minutes until current pl
        'place-inactive-timeout-minutes': 60,           // minutes until place is c
        'place-check-last-activity-seconds': (3*60)-5,  // seconds between checks f
```

```
        // redirection URL used for initial domain token generation,
        //   "METAVERSE_SERVER_URL" is replaced (from Config.metaverse.metaverse-se
        //   "DASHBOARD_URL" is replaced (from Config.metaverse.dashboard-url)
        'tokengen_url': 'METAVERSE_SERVER_URL/static/DomainTokenLogin.html',
        // 'tokengen_url': 'DASHBOARD_URL?metaverse=METAVERSE_SERVER_URL&page=domai

        // When account of this name is created, add 'admin' role to it
        //    Initially as empty so random people cannot create an admin account
        //    The account named here MUST be controlled by the server's admin
        'base-admin-account': '',

        // If to assume domain network_address if on is not set
        'fix-domain-network-address': true,
        // Whether allowing temp domain name creation
        'allow-temp-domain-creation': false,

        // Email verification on account creation
        'enable-account-email-verification': false,
        'email-verification-timeout-minutes': 1440, // minutes to wait for email ve
        // default is in 'static' dir. If you put in 'config' dir, use 'config/veri
        //   "VERIFICATION_URL" is replaced with the computed URL (build with Confi
        //   "METAVERSE_NAME" is replaced (from Config.metaverse.metaverse-name)
        //   "SHORT_METAVERSE_NAME" is replaced (from Config.metaverse.metaverse-ni
        'email-verification-email-body': 'dist/static/verificationEmail.html',  //
        'email-verification-from': '', // who the email is From
        // When user follows the verification URL, they are redirected to one of th
        //   "METAVERSE_SERVER_URL" is replaced (from Config.metaverse.metaverse-se
        //   "DASHBOARD_URL" is replaced (from Config.metaverse.dashboard-url)
        //   "ACCOUNT_ID" is replaced with the verifying account id
        //   "FAILURE_REASON" is replaced with the reason for verification failure
        'email-verification-success-redirect': 'METAVERSE_SERVER_URL/static/verific
        'email-verification-failure-redirect': 'METAVERSE_SERVER_URL/static/verific
    },
    // SMTP mail parameters for out-bound email
    // This is the structure that is passed to NodeMailer's SMTP transport.
    // Check out the documentation at https://nodemailer.com/smtp/
    // For SMTP outbound, setup your email account on your service and
    //     update SMTP-HOSTNAME, SMTP-USER, and SMTP-PASSWORD with your info.
    'nodemailer-transport-config': {
        'host': 'SMTP-HOSTNAME',
        'port': 465,    // 587 if secure=false
        'secure': true,
        'auth': {
            'user': 'SMTP-USER',
            'pass': 'SMTP-PASSWORD'
        }
    },
```

```
    'monitoring': {
        'enable': true,           // enable value monitoring
        'history': true           // whether to keep value history
    },
    // Setup for MongoDB access
    'database': {
        'db-host': 'localhost',
        'db-port': 27017,
        'db': 'tester',
        'db-user': 'metaverse',
        'db-pw': 'nooneknowsit',
        'db-authdb': 'admin',
        'db-connection': ''   // connection string replaces above if supplied
    },
    // MongoDB account configured for database backup script
    'backup': {
        "backup-user": "backuper",  // database backup user account (for BackupDb.s
        "backup-pw": "nooneknowsit", // database backup user password (for BackupDb
        "backup-dir": "directoryName", // Backup file directory. Optional. Defaults
        "authenticationDatabase": "databaseName" // auth db for backup user. Option
    },
    'debug': {
        'loglevel': 'info',

        // Winston logging configuration
        'log-to-files': true,         // if to log to files
        'log-filename': 'iamus.log',  // filename for log files
        'log-directory': './logs',    // directory to place logs
        'log-max-size-megabytes': 100,// max mega-bytes per log file
        'log-max-files': 10,          // number of log files to create
        'log-tailable': true,         // if to always output to main named log file
        'log-compress': false,        // if to compress old log files

        'log-to-console': false,      // if to additionally log to the console

        'devel': false,

        // Control of what debug information is logged
        'request-detail': false,  // output the received request info when received
        'request-body': false,    // output the received request body when received
        'metaverseapi-response-detail': false, // output the response sent back fro
        'query-detail': false,    // outputs details when selecting query parameter
        'db-query-detail': false, // outputs details about DB queries
        'field-setting': false    // Details of entity field getting and setting
    }
}
```

3) the file used in this setup:

```
@todo: insert file
```

8.6.3.5 Configure port forwarding for the metaverse server

```
set nat destination rule 20 description 'Port Forward for metaverse: 9400 to 9400 o
set nat destination rule 20 destination port '9400'
set nat destination rule 20 inbound-interface 'eth0'
set nat destination rule 20 protocol 'tcp'
set nat destination rule 20 translation address '192.168.y.5'
set nat destination rule 20 translation port '9400'
```

8.6.3.6 Configuring NAT reflection on the VyOS router (testing)

Many routers will automatically configure NAT reflection for open ports and VyOS can be configured to perform NAT reflection. This requires a few updates to the existing rules that have been configured. NAT reflection would be useful for internal only debugging, however, in testing the ICE server from the build would only bind to the external internet routable IP thus hindering the ability to use internally. As using ICE for internal only is an edge case this is actually as expected although future work could look into updating the ICE server and configuring split DNS (feel free to update with suggestions). With this in mind the setup described here, at present, does not require NAT reflection but the following updates should enable it if desired:

```
set nat destination rule 16 destination address 192.168.x.z
set nat destination rule 17 destination address 192.168.x.z
set nat destination rule 18 destination address 192.168.x.z
set nat destination rule 20 destination address 192.168.x.z
set nat destination rule 21 destination address 192.168.x.z

set nat destination rule 16 inbound-interface any
set nat destination rule 17 inbound-interface any
set nat destination rule 18 inbound-interface any
set nat destination rule 20 inbound-interface any
set nat destination rule 21 inbound-interface any

commit

save
```

8.6.3.7 Enabling external access

Important note: in a development and testing environment (such as the one detailed here) the VyOS router should not be permanently connected to the internet and access should only be allowed whilst tests are being performed and if possible tied down to specific source addresses. To allow testing the external firewall requires port forwarding. The port forwarding rules can be turned on and off as desired.

The following port forwarding rules are required:

Name	Port	Destination IP	Protocol
Vircadia 40102 (udp) main connection from clients	40102	192.168.x.y	UDP
Vircadia 7337 (both) ice-server	7337	192.168.x.y	TCP+UDP
Vircadia 9400 (tcp) metaverse-server	9400	192.168.x.y	TCP

Note: the configuration and starting of the services will reference the external IP address a.b.c.d

8.6.3.8 Start the services

The process of starting the services is as follows (see: Building and Running Ice-Server and Domain-Server

Metaverse server service On the metaverse server open a terminal and run:

```
cd vircadia-metaverse

node/dist/index.ts
```

ICE server Start ice-server.

On the vircadia server open a terminal and run:

```
cd Vircadia/vircadiaBuildDir
export HIFI_METAVERSE_URL=http://a.b.c.d:9400
./run_ice-server
```

Domain server services Start domain-server.

Open another terminal and run:

```
cd Vircadia/vircadiaBuildDir
export HIFI_METAVERSE_URL=http://a.b.c.d:9400
export ICE_SERVER=a.b.c.d:7337
./run_domain-server -i ${ICE_SERVER}
```

Start assignment client.

Open another terminal and run:

```
cd Vircadia/vircadiaBuildDir
./run_assignment-client
```

Client interface For testing the client application the Windows OS was opted for and Vircadia 2022.1.1 was used.

8.6.3.9 Connecting the Metaverse server and configuring a test Metaverse account

Navigate to:

http://192.168.x.y:40100/settings/#metaverse_group (or use the external IP a.b.c.d)

Then click 'Connect Metaverse Account'

A new page should open (http://a.b.c.d:9400/static/DomainTokenLogin.html) with the option to 'create account'. Do this and then enter the username and password on the 'Get Token'. Copy this token and then go back to the previous page and paste it in the open dialogue and click connect. The Networking / Metaverse section should now display 'Metaverse Account Connected'.

Note: at this point you could create a few more accounts for testing.

8.6.3.10 Connecting a client

If you are testing locally then you will probably need to use a VPN so that your connection is routed from outside your local network. This is due to the ICE server and how it will create open ports. The NAT reflection required will probably not work on the external router for non static port forwarding rules.

From tests it appears that the best way to run the client is to start it from the command line with the IP for the domain server (at least for the initial run and then it seems to work fine then in).

For the initial run the following was actioned:

Open a terminal (PowerShell on Windows in this case), navigate to the folder containing the Vircadia executable and run:

```
.\interface.exe --url 84.92.193.1
```

Then in the interface navigate to File -> Metaverse: Login / Sign Up

Enter the details as follows:

Display name: XYZ Username: usernameCreatedInPreviousStep Password: password-CreatedInPreviousStep URL: http://a.b.c.d:9400

Then click 'Log in to metaverse'

8.6.3.11 Configure SSH access for domain and metaverse servers (optional)

For potentially easier debugging, enable SSH on the servers.

Open a terminal and type:

`sudo apt install openssh-server`

Then configure the following rules on the VyOS router:

Domain server Then set up port forwarding on the VyOS router... @todo add $VyOS

```
configure

set nat destination rule 14 description 'Port Forward: 2224 to 22 SSH on 192.168.y.
set nat destination rule 14 destination port '2224'
set nat destination rule 14 inbound-interface 'eth0'
set nat destination rule 14 protocol 'tcp'
set nat destination rule 14 translation address '192.168.y.4'
set nat destination rule 14 translation port '22'

commit
```

Test the SSH access and if all works well:

```
save
```

Metaverse server Configure SSH access and port forwarding on the VyOS if desired:

```
configure

set nat destination rule 19 description 'Port Forward: 2225 to 22 SSH on 192.168.y.
set nat destination rule 19 destination port '2225'
set nat destination rule 19 inbound-interface 'eth0'
set nat destination rule 19 protocol 'tcp'
set nat destination rule 19 translation address '192.168.y.5'
set nat destination rule 19 translation port '22'

commit
```

Test the SSH access and if all works well:

```
save
```

III

Appendix

8.7 Acknowledgements and thanks

As you'd expect lots of work went into checking the book. Special thanks to Melvin Carvalho, Tim Millar, Lorena Gomez, James Lewis, @smallworlnd, and Margaret O'Hare.

8.8 Author Biographies

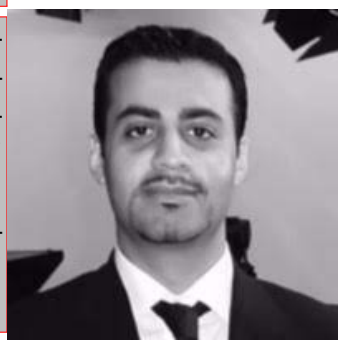
Dr John O'Hare is a results driven, certified Prince2 Agile Practitioner. Leveraging proven analytical ability, and drawing on 23 years of experience at the University of Salford. Successful as a leader and an influential team member in both project and customer-facing roles. As a product manager he specialises in systems design, procurement, tendering and bid writing for research funding, running complex heterogeneous research systems, research and development, and supporting academic staff / research students to undertake theirs. Completed a PhD in "Attention in Telepresence", uniting the gaze of remote collaborators, through furniture. Recently pursuing research opportunities in value transfer mechanisms for 'Metaverses'.



Dr Allen Fairchild is an experienced security-conscious software engineer and academic researcher with comprehensive experience developing innovative end-to-end systems for a wide variety of use-cases. Strong leadership and acumen in full stack development. Track record in building networks through regional initiatives, delivering Agile projects to a wide variety of technical markets. Allen is an accomplished researcher and holds a PhD Video based reconstruction system for mixed reality environments supporting contextualised non-verbal communication and its study, alongside a portfolio of groundbreaking publications in social VR. Excellent communication skills and Agile team leadership.



Dr Umran Ali currently works as a senior lecturer in creative media, and continues to explore virtual natural environment design through teaching and research, maintaining a deep interest in the meaning, impact, and design of natural spaces, in particular around video games. A keen video game collector and player, and a landscape photographer. Holds a PhD in A practice-based exploration of natural environment design in computer & video games.



Bibliography

Bibliography

[1] Kiku Jones and Lori NK Leonard. “Trust in consumer-to-consumer electronic commerce”. In: *Information & management* 45.2 (2008), pages 88–95 (cited on page 18).

[2] Mark Berners-Lee Tim; Fischetti. *Weaving the web*. https://archive.org/details/isbn_9780062515872/mode/2up. Accessed: 2021-02-10. 1999 (cited on page 21).

[3] Sean S Costigan. *World Without Mind: The Existential Threat of Big Tech (Franklin Foer)*. 2018 (cited on page 21).

[4] Nick Szabo. “Formalizing and securing relationships on public networks”. In: *First monday* (1997) (cited on pages 27, 31).

[5] Bryan Ford, Pyda Srisuresh, and Dan Kegel. “Peer-to-Peer Communication Across Network Address Translators.” In: *USENIX Annual Technical Conference, General Track*. 2005, pages 179–192 (cited on page 28).

[6] Enis Karaarslan and Eylul Adiguzel. “Blockchain based DNS and PKI solutions”. In: *IEEE Communications Standards Magazine* 2.3 (2018), pages 52–57 (cited on page 28).

[7] Michel Rauchs et al. “Distributed ledger technology systems: A conceptual framework”. In: *Available at SSRN 3230013* (2018) (cited on page 31).

[8] Whitfield Diffie and Martin Hellman. “New directions in cryptography”. In: *IEEE transactions on Information Theory* 22.6 (1976), pages 644–654 (cited on pages 31, 48).

[9] Ralph C Merkle. “Secure communications over insecure channels”. In: *Communications of the ACM* 21.4 (1978), pages 294–299 (cited on page 31).

[10] David Burnham. *The rise of the computer state*. Random House Inc., 1983 (cited on page 31).

[11] David Chaum. “Security without identification: Transaction systems to make big brother obsolete”. In: *Communications of the ACM* 28.10 (1985), pages 1030–1044 (cited on pages 31, 57).

[12] Don Lavoie. “Prefatory Note: The Origins of" The Agorics Project”. In: *Market Process, v8, Spring* (1990), pages 116–119 (cited on page 31).

[13] Phil Salin. *Costs and Computers*. 1991. URL: http://cdn.oreillystatic.com/radar/r1/11-91.pdf (cited on page 31).

[14] Various. *Cypher Punks Mailing List Archives*. 1990. URL: https://mailing-list-archive.cryptoanarchy.wiki (cited on page 31).

[15] Adam Back et al. “Hashcash-a denial of service counter-measure”. In: (2002) (cited on page 31).

[16] Cynthia Dwork and Moni Naor. “Pricing via processing or combatting junk mail”. In: *Annual international cryptology conference*. Springer. 1992, pages 139–147 (cited on pages 31, 103).

[17] Markus Jakobsson and Ari Juels. *Proofs of Work and Bread Pudding Protocols (Extended Abstract). Secure Information Networks (s. 258-272)*. 1999 (cited on page 31).

[18] Wei Dai. “b-money, 1998”. In: *URL http://www. weidai. com/bmoney. txt.(Last access: 08.04. 2019)* (1998) (cited on page 31).

[19] Jon Callas et al. *OpenPGP message format*. Technical report. RFC 2440, November, 1998 (cited on page 31).

[20] Satoshi Nakamoto. “Re: Bitcoin P2P e-cash paper”. In: *Email posted to listserv* 9 (2008), page 04 (cited on pages 31, 40).

[21] Yujin Kwon et al. “Impossibility of full decentralization in permissionless blockchains”. In: *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. 2019, pages 110–123 (cited on page 34).

[22] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. “A systematic literature review of blockchain-based applications: Current status, classification and open issues”. In: *Telematics and informatics* 36 (2019), pages 55–81 (cited on page 34).

[23] Alex Gladstein. *Check Your Financial Privilege*. BTC Media LLC, 2022 (cited on page 34).

[24] David Golumbia. “Cryptocurrency Is Garbage. So Is Blockchain.” In: *So Is Blockchain.(June 16, 2020)* (2020) (cited on page 36).

[25] Vitalik Buterin et al. “Ethereum white paper”. In: *GitHub repository* 1 (2013), pages 22–23 (cited on page 36).

[26] Sarwar Sayeed and Hector Marco-Gisbert. “Assessing blockchain consensus and security mechanisms against the 51% attack”. In: *Applied Sciences* 9.9 (2019), page 1788 (cited on page 36).

[27] Charles Petzold. *The annotated Turing: a guided tour through Alan Turing’s historic paper on computability and the Turing machine*. Wiley Publishing, 2008 (cited on page 36).

[28] Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. “Scaling blockchains: A comprehensive survey”. In: *IEEE Access* 8 (2020), pages 125244–125262 (cited on page 36).

[29] Joseph Bonneau et al. “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies”. In: *2015 IEEE symposium on security and privacy*. IEEE. 2015, pages 104–121 (cited on page 36).

[30] Laura Shin. *The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze*. Public Affairs, 2022 (cited on pages 36, 98).

[31] Huashan Chen et al. “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses”. In: *ACM Computing Surveys (CSUR)* 53.3 (2020), pages 1–43 (cited on page 37).

[32] Yulin Liu et al. “Empirical Analysis of EIP-1559: Transaction Fees, Waiting Time, and Consensus Security”. In: *arXiv preprint arXiv:2201.05574* (2022) (cited on page 38).

[33] Andrew Poelstra. “On stake and consensus”. In: *WP Software* 22 (2015), page 29 (cited on page 39).

[34] Torgin Mackinga, Tejaswi Nadahalli, and Roger Wattenhofer. “TWAP Oracle Attacks: Easier Done than Said?” In: *Cryptology ePrint Archive* (2022) (cited on page 39).

[35] Stuart Haber and W Scott Stornetta. “How to time-stamp a digital document”. In: *Conference on the Theory and Application of Cryptography*. Springer. 1990, pages 437–455 (cited on page 40).

[36] Satoshi Nakamoto. “Duality: an excerpt”. In: (2018) (cited on page 40).

[37] Yuji Ijiri. “A framework for triple-entry bookkeeping”. In: *Accounting Review* (1986), pages 745–759 (cited on page 40).

[38] Alessio Faccia and Narcisa Roxana Mosteanu. “Accounting and blockchain technology: from double-entry to triple-entry”. In: *The Business & Management Review* 10.2 (2019), pages 108–116 (cited on page 40).

[39] Usman W Chohan. “The double spending problem and cryptocurrencies”. In: *Available at SSRN 3090174* (2021) (cited on page 40).

[40] Cristina Pérez-Solà et al. “Double-spending prevention for bitcoin zero-confirmation transactions”. In: *International Journal of Information Security* 18.4 (2019), pages 451–463 (cited on page 40).

[41] Cyril Grunspan and Ricardo Pérez-Marco. “Double spend races”. In: *International Journal of Theoretical and Applied Finance* 21.08 (2018), page 1850053 (cited on page 40).

[42] Alan Sangster. “The earliest known treatise on double entry bookkeeping by Marino de Raphaeli”. In: *Accounting Historians Journal* 42.2 (2015), pages 1–33 (cited on page 40).

[43] Vijay Selvam. “The Blockchain That Matters: A Comparative Analysis of Bitcoin’s Fundamentally Unique and Irreplicable Properties”. In: *Available at SSRN 3880186* (2021) (cited on page 40).

[44] Igor Makarov and Antoinette Schoar. *Blockchain Analysis of the Bitcoin Market*. Technical report. National Bureau of Economic Research, 2021 (cited on page 41).

[45] Kyle Croman et al. “On scaling decentralized blockchains”. In: *International conference on financial cryptography and data security*. Springer. 2016, pages 106–125 (cited on page 41).

[46] Sergi Delgado-Segura et al. “Analysis of the bitcoin utxo set”. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2018, pages 78–91 (cited on page 41).

[47] Oxford Analytica. “El Salvador bitcoin experiment comes with risks”. In: *Emerald Expert Briefings* oxan-db (2021) (cited on page 42).

[48] Phillip Rogaway and Thomas Shrimpton. “Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance”. In: *International workshop on fast software encryption*. Springer. 2004, pages 371–388 (cited on page 43).

[49] Camilo Mora et al. “Bitcoin emissions alone could push global warming above 2 C”. In: *Nature Climate Change* 8.11 (2018), pages 931–933 (cited on pages 44, 46).

[50] Troy Cross and Andrew M. Bailey. “GREENING BITCOIN WITH INCENTIVE OFFSETS”. In: (2021) (cited on page 44).

[51] Sacha Meyers Allen Farrington. *Bitcoin is Venice*. 2022. URL: https://www.uncerto.com/book-pdf (cited on page 44).

[52] Saul Griffith. *Electrify: An Optimist’s Playbook for Our Clean Energy Future*. MIT Press, 2021 (cited on page 44).

[53] Thomas Deetjen Joshua D. Rhodes and Caitlin Smith. “Impacts of Large, Flexible DataCenter Operations on theFuture of ERCOT”. In: *Ideasmiths* (2021). URL: https://www.ideasmiths.net/wp-content/uploads/2022/02/LANCIUM_IS_ERCOT_flexDC_FINAL_2021.pdf (cited on page 44).

[54] Carlos L Bastian-Pinto et al. “Hedging renewable energy investments with Bitcoin mining”. In: *Renewable and Sustainable Energy Reviews* 138 (2021), page 110520 (cited on page 45).

[55] Dirk G Baur and Josua Oll. “Bitcoin investments and climate change: a financial and carbon intensity perspective”. In: *Finance Research Letters* (2021), page 102575 (cited on page 46).

[56] Apolline Blandin et al. “3rd global cryptoasset benchmarking study”. In: *Available at SSRN 3700822* (2020) (cited on page 46).

[57] Alex de Vries et al. “Revisiting Bitcoin’s carbon footprint”. In: *Joule* (2022) (cited on page 46).

[58] Michel KHAZZAKA. “Bitcoin: Cryptopayments Energy Efficiency”. In: *Available at SSRN* (2022) (cited on page 46).

[59] J Bradford De Long et al. “Positive feedback investment strategies and destabilizing rational speculation”. In: *the Journal of Finance* 45.2 (1990), pages 379–395 (cited on page 46).

[60] Claus-Peter Schnorr. “Efficient identification and signatures for smart cards”. In: *Conference on the Theory and Application of Cryptology*. Springer. 1989, pages 239–252 (cited on pages 49, 53).

[61] Jonathan Bier. *The Blocksize War: The battle for control over Bitcoin’s protocol rules*. Springer, 2021 (cited on page 51).

[62] Joseph Poon and Thaddeus Dryja. *The bitcoin lightning network: Scalable off-chain instant payments*. 2016 (cited on page 56).

[63] Anantha Divakaruni and Peter Zimmerman. “The Lightning Network: Turning Bitcoin into Money”. In: (2022) (cited on page 56).

[64] Philipp Zabka et al. “Short Paper: A Centrality Analysis of the Lightning Network”. In: (2022) (cited on page 56).

[65] Eli Ben Sasson et al. “Scalable and transparent proofs over all large fields via elliptic curves”. In: *TR22 110* (2022) (cited on page 66).

[66] Cosimo Sguanci and Anastasios Sidiropoulos. *Mass Exit Attacks on the Lightning Network*. 2022. DOI: 10.48550/ARXIV.2208.01908. URL: https://arxiv.org/abs/2208.01908 (cited on page 69).

[67] Malte Möser, Rainer Böhme, and Dominic Breuker. “An inquiry into money laundering tools in the Bitcoin ecosystem”. In: *2013 APWG eCrime researchers summit*. Ieee. 2013, pages 1–14 (cited on page 69).

[68] Ross Anderson. “Free speech online and offline”. In: *Computer* 35.6 (2002), pages 28–30 (cited on page 70).

[69] Miles Carlsten et al. “On the instability of bitcoin without the block reward”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pages 154–167 (cited on page 70).

[70] Georg Fuchsbauer, Michele Orrù, and Yannick Seurin. “Aggregate cash systems: A cryptographic investigation of mimblewimble”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pages 657–689 (cited on page 70).

[71] Sidney Homer and Richard Eugene Sylla. *A history of interest rates*. Rutgers University Press, 1996 (cited on page 72).

[72] Nick Szabo. “Shelling out: the origins of money”. In: *Satoshi Nakamoto Institute* (2002) (cited on page 73).

[73] George Selgin and Lawrence H White. “In defense of fiduciary media—or, we arenot devo (lutionists), we are Misesians!” In: *The Review of Austrian Economics* 9.2 (1996), pages 83–107 (cited on page 73).

[74] Robert B Barsky. “The Fisher hypothesis and the forecastability and persistence of inflation”. In: *Journal of monetary Economics* 19.1 (1987), pages 3–24 (cited on page 73).

[75] Robert E Hall. *Inflation: causes and effects*. University of Chicago Press, 2009 (cited on page 73).

[76] Glyn Davies. *History of money*. University of Wales Press, 2010 (cited on page 73).

[77] Dominik Stroukal et al. “Can Bitcoin become money? Its money functions and the regression theorem”. In: *International Journal of Business and Management* 6.1 (2018), pages 36–53 (cited on page 73).

[78] Brian Roger Tomlinson. “What Was the Third World?” In: *Journal of Contemporary History* 38.2 (2003), pages 307–321 (cited on page 73).

[79] Ricardo J Caballero, Emmanuel Farhi, and Pierre-Olivier Gourinchas. *Financial crash, commodity prices and global imbalances*. Technical report. National Bureau of Economic Research, 2008 (cited on page 73).

[80] David E Spiro. *The hidden hand of American hegemony*. Cornell University Press, 2019 (cited on page 73).

[81] Subir Grewal. *Struggling Amidst Plenty: A Layperson's Guide to Our Awful Monetary System, Why it's the Root Cause of Inequality, Debt, and "Too Big to Fail," & The Little-Known Way to Fix it*. Subir Grewal, 2020 (cited on page 74).

[82] Mark Carney. "The growing challenges for monetary policy in the current international monetary and financial system". In: *Remarks at the Jackson Hole Symposium*. Volume 23. 2019 (cited on page 74).

[83] Nadia Piffaretti. "Reshaping the international monetary architecture: lessons from Keynes' plan". In: *World Bank Policy Research Working Paper* 5034 (2009) (cited on page 74).

[84] Ronald-Peter Stoeferle and Mark J Valek. *Gold and the Turning of the Monetary Tides*. Technical report. Technical report, 2018 (cited on page 74).

[85] John A Mathews and Mark Selden. "China: The emergence of the Petroyuan and the challenge to US dollar hegemony". In: *The Asia-Pacific Journal* 16.22/3 (2018), pages 1–12 (cited on page 74).

[86] Yiping Huang. "Understanding China's Belt & Road initiative: motivation, framework and assessment". In: *China Economic Review* 40 (2016), pages 314–321 (cited on page 74).

[87] Joshua R Hendrickson and William J Luther. "The Value of Bitcoin in the Year 2141 (and beyond!)" In: *AIER Sound Money Project Working Paper* 2021-06 (2021) (cited on page 74).

[88] Peter Gainsford. "Salt and salary: were Roman soldiers paid in salt?" In: *Kiwi Hellenist: Modern Myths about the Ancient World. Retrieved* 11 (2017) (cited on page 74).

[89] Dror Goldberg. "Famous myths of" fiat money"". In: *Journal of Money, Credit and Banking* (2005), pages 957–967 (cited on page 74).

[90] Ryan Clements. "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins". In: *Wake Forest L. Rev. Online* 11 (2021), page 131 (cited on page 78).

[91] J. Wang. *Central Banking 101*. JOSEPH, 2021. ISBN: 9780999136744. URL: https://books.google.co.uk/books?id=nwoozgEACAAJ (cited on page 82).

[92] Andrew J Filardo, Madhusudan S Mohanty, and Ramon Moreno. "Central bank and government debt management: issues for monetary policy". In: *BIS Paper* 67d (2012) (cited on page 82).

[93] Richard Cantillon. *Essai sur la nature du commerce en général*. éditeur non identifié, 1756 (cited on page 83).

[94] Michael David Bordo. "Some aspects of the monetary economics of Richard Cantillon". In: *Journal of Monetary Economics* 12.2 (1983), pages 235–258 (cited on page 83).

[95] Eswar S Prasad. *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance*. Harvard University Press, 2021 (cited on page 83).

[96] Lyn Alden. *Bitcoin: Addressing the Ponzi Scheme Characterization*. 2021. URL: https://www.lynalden.com/bitcoin-ponzi-scheme/ (cited on page 87).

[97] Mathilde Maurel and Gunther Schnabl. “Keynesian and Austrian perspectives on crisis, shock adjustment, exchange rate regime and (long-term) growth”. In: *Open Economies Review* 23.5 (2012), pages 847–868 (cited on page 87).

[98] Nikhil Bhatia. *Layered Money*. Self Quoted, 1988 (cited on page 89).

[99] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. “Hijacking bitcoin: Routing attacks on cryptocurrencies”. In: *2017 IEEE symposium on security and privacy (SP)*. IEEE. 2017, pages 375–392 (cited on page 90).

[100] Nassim Nicholas Taleb. *Antifragile: how to live in a world we don’t understand*. Volume 3. Allen Lane London, 2012 (cited on page 90).

[101] Brett AS Martin et al. “Dark personalities and Bitcoin®: The influence of the Dark Tetrad on cryptocurrency attitude and buying intention”. In: *Personality and Individual Differences* 188 (2022), page 111453 (cited on page 94).

[102] Balaji Srinivasan. *The Network State: How To Start A New Country*. Amazon, 2022. URL: https://balajis.com/the-network-state-book-a-crosspost/ (cited on page 95).

[103] Daniel Krawisz. “Hyperbitcoinization”. In: *Online verfügbar unter: https://nakamotoin* (2014) (cited on page 95).

[104] J. Svanholm K. Booth, M. Shilling, and N. Laamanen. *Bitcoin: Everything Divided by 21 Million*. Amazon Digital Services LLC - KDP Print US, 2022. ISBN: 9789916697191. URL: https://books.google.co.uk/books?id=14onzwEACAAJ (cited on page 96).

[105] Leo Malherbe et al. “Cryptocurrencies and blockchain: Opportunities and limits of a new monetary regime”. In: *International Journal of Political Economy* 48.2 (2019), pages 127–152 (cited on page 96).

[106] Eric Budish. *The economic limits of bitcoin and the blockchain*. Technical report. National Bureau of Economic Research, 2018 (cited on page 96).

[107] Julien Piet, Jaiden Fairoze, and Nicholas Weaver. “Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value”. In: *arXiv preprint arXiv:2203.15930* (2022) (cited on page 96).

[108] Gordon A King et al. “Fisher, Franklin M., The Identification Problem in Econometrics”. In: *American Journal of Agricultural Economics* 48.4_Part_I (1966), pages 1039–1040 (cited on page 99).

[109] Mick Lockwood. “Exploring value propositions to drive Self-Sovereign Identity adoption”. In: *Frontiers in Blockchain* 4 (2021), page 4 (cited on page 100).

[110] Juliet M Moringiello and Christopher K Odinet. “The Property Law of Tokens”. In: *Florida Law Review (Forthcoming 2022)* (2021) (cited on page 105).

[111] Joshua Fairfield. “Tokenized: The law of non-fungible tokens and unique digital property”. In: *Indiana Law Journal, Forthcoming* (2021) (cited on page 105).

[112] Denis Dutton. “Authenticity in art”. In: *The Oxford handbook of aesthetics* (2003), pages 258–274 (cited on page 107).

[113] Chelsea Komlo and Ian Goldberg. “FROST: flexible round-optimized Schnorr threshold signatures”. In: *International Conference on Selected Areas in Cryptography*. Springer. 2020, pages 34–65 (cited on page 116).

[114] Stylianos Mystakidis. “Metaverse”. In: *Encyclopedia* 2.1 (2022), pages 486–497 (cited on page 119).

[115] Kim JL Nevelsteen. “Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse”. In: *Computer Animation and Virtual Worlds* 29.1 (2018), e1752 (cited on page 120).

[116] Cory Ondrejka. “Escaping the gilded cage: User created content and building the metaverse”. In: *NYL Sch. L. Rev.* 49 (2004), page 81 (cited on page 121).

[117] Hilary McLellan. “Avatars, Affordances, and Interfaces: Virtual Reality Tools for Learning.” In: (1993) (cited on page 121).

[118] Sang-Min Park and Young-Gab Kim. “A Metaverse: Taxonomy, components, applications, and open challenges”. In: *Ieee Access* 10 (2022), pages 4209–4251 (cited on pages 121, 145).

[119] William Gibson. “Neuromancer (1984)”. In: *Crime and Media*. Routledge, 2019, pages 86–94 (cited on page 121).

[120] Nicholas Bloom et al. “Does working from home work? Evidence from a Chinese experiment”. In: *Q. J. Econ.* 130.1 (2015), pages 165–218 (cited on page 123).

[121] Jose Maria Barrero, Nicholas Bloom, and Steven J Davis. *Why working from home will stick*. Technical report. National Bureau of Economic Research, 2021 (cited on page 123).

[122] Shiv Prakash et al. “Characteristic of enterprise collaboration system and its implementation issues in business management”. In: *International Journal of Business Intelligence and Data Mining* 16.1 (2020), pages 49–65 (cited on page 123).

[123] Adam Aiken. “Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think”. In: *Index on Censorship* 49.2 (2020), pages 24–27 (cited on page 124).

[124] R Wolff et al. “Communicating Eye Gaze across a Distance without Rooting Participants to the Spot”. In: *2008 12th IEEE/ACM International Symposium on Distributed Simulation and Real-Time Applications*. Ieee, #oct# 2008, pages 111–118 (cited on pages 124, 126).

[125] RS Oeppen, G Shaw, and PA Brennan. “Human factors recognition at virtual meetings and video conferencing: how to get the best performance from yourself and others”. In: *British Journal of Oral and Maxillofacial Surgery* (2020) (cited on page 124).

[126] C O’Malley and Steve Langton. “Comparison Of Face-to-face And Video-mediated Interaction”. In: volume 2. 1996, pages 177–192 (cited on page 125).

[127] Paul Dourish et al. “Your place or mine? Learning from long-term use of Audio-Video communication”. In: *Comput. Support. Coop. Work* 5.1 (#mar# 1996), pages 33–62 (cited on page 125).

[128] Criminisi et al. “Gaze manipulation for one-to-one teleconferencing”. In: *Proceedings Ninth IEEE International Conference on Computer Vision*. Nice, #oct# 2003, 191–198 vol.1 (cited on page 125).

[129] R van Eijk et al. “Human sensitivity to eye contact in 2D and 3D videoconferencing”. In: *2010 Second International Workshop on Quality of Multimedia Experience (QoMEX)*. #jun# 2010, pages 76–81 (cited on pages 125, 127).

[130] Milton Chen. “Leveraging the asymmetric sensitivity of eye contact for videoconference”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’02. Minneapolis, Minnesota, USA: Association for Computing Machinery, #apr# 2002, pages 49–56 (cited on pages 125, 127).

[131] David J Roberts et al. “Estimating the gaze of a virtuality human”. en. In: *IEEE Trans. Vis. Comput. Graph.* 19.4 (#apr# 2013), pages 681–690 (cited on page 125).

[132] Abigail Sellen, Bill Buxton, and John Arnott. “Using spatial cues to improve videoconferencing”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’92. Monterey, California, USA: Association for Computing Machinery, #jun# 1992, pages 651–652 (cited on pages 125, 135).

[133] Abigail J Sellen. “Remote Conversations: The Effects of Mediating Talk With Technology”. In: *Human–Computer Interaction* 10.4 (#dec# 1995), pages 401–444 (cited on page 125).

[134] Andrew F Monk and Caroline Gale. “A Look Is Worth a Thousand Words: Full Gaze Awareness in Video-Mediated Conversation”. In: *Discourse Process.* 33.3 (#may# 2002), pages 257–278 (cited on pages 125, 129).

[135] J Gemmell et al. “Gaze awareness for video-conferencing: a software approach”. In: *IEEE Multimedia* 7.4 (#oct# 2000), pages 26–35 (cited on page 125).

[136] Claudia Kuster et al. “Gaze correction for home video conferencing”. #nov# 2012 (cited on page 125).

[137] Ederyn Williams. “Experimental comparisons of face-to-face and mediated communication: A review”. In: *Psychol. Bull.* 84.5 (1977), page 963 (cited on page 126).

[138] C Edigo. “Videoconferencing as a technology to support group work: A review of its failure”. In: *Proceedings of the ACM conf. on Computer-Supported Cooperative Work*. 1988 (cited on page 126).

[139] Tomislav Pejsa et al. “Room2Room: Enabling Life-Size Telepresence in a Projected Augmented Reality Environment”. In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. CSCW ’16. San Francisco, California, USA: Association for Computing Machinery, #feb# 2016, pages 1716–1725 (cited on page 126).

[140] Jakob Bardram et al. “ReticularSpaces: activity-based computing support for physically distributed and collaborative smart spaces”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, #may# 2012, pages 2845–2854 (cited on pages 126, 138).

[141] Piotr D Adamczyk and Michael B Twidale. “Supporting multidisciplinary collaboration: requirements from novel HCI education”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’07. San Jose, California, USA: Association for Computing Machinery, #apr# 2007, pages 1073–1076 (cited on pages 126, 138).

[142] Hiroshi Ishii, Minoru Kobayashi, and Jonathan Grudin. “Integration of interpersonal space and shared workspace: ClearBoard design and experiments”. #oct# 1993 (cited on pages 126, 138).

[143] Dhanraj Vishwanath, Ahna R Girshick, and Martin S Banks. “Why pictures look right when viewed from the wrong place”. In: volume 8. Nature Publishing Group, 2005, pages 1401–1410 (cited on pages 126, 127).

[144] Stuart M Anstis, John W Mayhew, and Tania Morley. “The Perception of Where a Face or Television Portrait is Looking”. In: volume 82. JSTOR, 1969, pages 474–489 (cited on page 127).

[145] William Hyde Wollaston. “On the apparent direction of eyes in a portrait”. In: JSTOR, 1824, pages 247–256 (cited on page 127).

[146] Jack M Loomis et al. “Psychophysics of perceiving eye-gaze and head direction with peripheral vision: implications for the dynamics of eye-gaze behavior”. en. In: *Perception* 37.9 (2008), pages 1443–1457 (cited on pages 127, 131).

[147] Chris Fullwood and Gwyneth Doherty-Sneddon. “Effect of gazing at the camera during a video link on recall”. en. In: *Appl. Ergon.* 37.2 (#mar# 2006), pages 167–175 (cited on page 127).

[148] Samer Al Moubayed, Jens Edlund, and Jonas Beskow. “Taming Mona Lisa”. In: volume 1. 2012, pages 1–25 (cited on page 127).

[149] David Nguyen and John Canny. “MultiView: spatially faithful group video conferencing”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’05. Portland, Oregon, USA: Association for Computing Machinery, #apr# 2005, pages 799–808 (cited on pages 127, 140).

[150] Roel Vertegaal and Yaping Ding. “Explaining effects of eye gaze on mediated group conversations: amount or synchronization?” In: *Proceedings of the 2002 ACM conference on Computer supported cooperative work*. CSCW ’02. New Orleans, Louisiana, USA: Association for Computing Machinery, #nov# 2002, pages 41–48 (cited on pages 127, 129).

[151] Simon W Bock, Peter Dicke, and Peter Thier. “How precise is gaze following in humans?” en. In: *Vision Res.* 48.7 (#mar# 2008), pages 946–957 (cited on page 127).

[152] Norman P Jouppi and Michael J Pan. “Mutually-immersive audio telepresence”. In: *Audio Engineering Society Convention 113*. 2002 (cited on pages 127, 137).

[153] Paul M Aoki et al. “The mad hatter’s cocktail party: a social mobile audio space supporting multiple simultaneous conversations”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’03. Ft. Lauderdale, Florida, USA: Association for Computing Machinery, #apr# 2003, pages 425–432 (cited on pages 127, 145).

[154] Michael Argyle. *Bodily communication*. Methuen, 1988 (cited on pages 127, 129, 130, 132, 134, 135).

[155] Mattias Heldner and Jens Edlund. “Pauses, gaps and overlaps in conversations”. In: *J. Phon.* 38.4 (#oct# 2010), pages 555–568 (cited on page 128).

[156] C L Kleinke. “Gaze and eye contact: a research review”. en. In: *Psychol. Bull.* 100.1 (#jul# 1986), pages 78–100 (cited on pages 128, 130, 131, 143).

[157] Stella Ting-Toomey and Leeva C Chung. *Understanding intercultural communication*. Oxford University Press New York, NY, 2012 (cited on page 128).

[158] Kazuhiro Otsuka, Yoshinao Takemae, and Junji Yamato. “A probabilistic inference of multiparty-conversation structure based on Markov-switching models of gaze patterns, head directions, and utterances”. In: *Proceedings of the 7th international conference on Multimodal interfaces*. ICMI ’05. Torento, Italy: Association for Computing Machinery, #oct# 2005, pages 191–198 (cited on pages 128, 143).

[159] Yasuhiro Katagiri. “Aiduti in Japanese multi-party design conversations”. In: *Proceedings of the Workshop on Embodied Language Processing*. 2007, pages 9–16 (cited on page 128).

[160] Jack M Loomis, Roberta L Klatzky, and Nicholas A Giudice. “-Sensory Substitution of Vision: Importance of Perceptual and Cognitive Processing”. In: *Assistive technology for blindness and low vision*. CRC Press, 2012, pages 179–210 (cited on page 128).

[161] Charles Goodwin. “Action and embodiment within situated human interaction”. In: *J. Pragmat.* 32.10 (#sep# 2000), pages 1489–1522 (cited on page 128).

[162] Marco Gillies, Mel Slater, et al. “Non-verbal communication for correlational characters”. In: (2005) (cited on page 128).

[163] Michael Argyle and Mark Cook. *Gaze and Mutual Gaze*. en. Cambridge University Press, #jan# 1976 (cited on pages 129, 130, 132).

[164] Michael Argyle and Janet Dean. “Eye-contact, Distance And Affiliation”. In: JSTOR, 1965, pages 289–304 (cited on pages 129, 134).

[165] Michael Argyle and Roger Ingham. *Gaze, Mutual Gaze, and Proximity*. 1969 (cited on pages 129–131, 134).

[166] A Kendon. “Some functions of gaze-direction in social interaction.” In: *Acta Psychol.* 26.1 (1967), pages 22–63 (cited on pages 129, 143).

[167] B J Hedge, B S Everitt, and Christopher D Frith. “The Role Of Gaze In Dialogue”. In: volume 42. Elsevier, 1978, pages 453–475 (cited on pages 129, 135).

[168] D G Novick, B Hansen, and K Ward. “Coordinating turn-taking with gaze”. In: *Proceeding of Fourth International Conference on Spoken Language Processing. ICSLP ’96*. Volume 3. #oct# 1996, 1888–1891 vol.3 (cited on pages 129, 135).

[169] Roel Vertegaal, Gerrit Van der Veer, and Harro Vons. “Effects of gaze on multiparty mediated communication”. In: *Graphics interface*. Morgan Kaufmann, 2000, pages 95–102 (cited on page 129).

[170] Roel Vertegaal et al. “Eye gaze patterns in conversations: there is more to conversational agents than meets the eyes”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’01. Seattle, Washington, USA: Association for Computing Machinery, #mar# 2001, pages 301–308 (cited on page 129).

[171] S R Langton. “The mutual influence of gaze and head orientation in the analysis of social attention direction”. en. In: *Q. J. Exp. Psychol. A* 53.3 (#aug# 2000), pages 825–845 (cited on pages 129, 131).

[172] Alex Colburn, Michael F Cohen, and Steven Drucker. “The Role Of Eye Gaze In Avatar Mediated Conversational Interfaces”. In: 2000 (cited on page 129).

[173] C Neil Macrae et al. “Are you looking at me? Eye gaze and person perception”. en. In: *Psychol. Sci.* 13.5 (#sep# 2002), pages 460–464 (cited on page 129).

[174] Lawrence A Symons et al. “What are you looking at? Acuity for triadic eye gaze”. In: volume 131. 2004, pages 451–469 (cited on page 129).

[175] Nathan L Kluttz et al. “The effect of head turn on the perception of gaze”. en. In: *Vision Res.* 49.15 (#jul# 2009), pages 1979–1993 (cited on pages 129, 131).

[176] Hugh R Wilson et al. “Perception of head orientation”. In: volume 40. Elsevier, 2000, pages 459–472 (cited on pages 129, 131).

[177] Johann Schrammel et al. ““Look!”: using the gaze direction of embodied agents”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’07. San Jose, California, USA: Association for Computing Machinery, #apr# 2007, pages 1187–1190 (cited on page 129).

[178] Rainer Stiefelhagen, Jie Yang, and Alex Waibel. “Estimating focus of attention based on gaze and sound”. In: *Proceedings of the 2001 workshop on Perceptive user interfaces*. PUI ’01. Orlando, Florida, USA: Association for Computing Machinery, #nov# 2001, pages 1–9 (cited on pages 129, 135).

[179] R Stiefelhagen. “Tracking focus of attention in meetings”. In: *Proceedings. Fourth IEEE International Conference on Multimodal Interfaces*. #oct# 2002, pages 273–280 (cited on pages 129, 131, 135).

[180] W Steptoe et al. “Eye Tracking for Avatar Eye Gaze Control During Object-Focused Multiparty Interaction in Immersive Collaborative Virtual Environments”. In: *2009 IEEE Virtual Reality Conference*. #mar# 2009, pages 83–90 (cited on page 129).

[181] William Arthur Hugh Steptoe. “Eye tracking and avatar-mediated communication in immersive collaborative virtual environments”. PhD thesis. University College London (University of London), 2010 (cited on pages 130, 136).

[182] Mark Cook. “Gaze and mutual gaze in social encounters”. In: *Am. Sci.* 65.3 (1977), pages 328–333 (cited on pages 130, 143).

[183] Sascha Fagel et al. “On the importance of eye gaze in a face-to-face collaborative task”. In: *Proceedings of the 3rd international workshop on Affective interaction in natural environments*. AFFINE ’10. Firenze, Italy: Association for Computing Machinery, #oct# 2010, pages 81–86 (cited on pages 130, 135, 143).

[184] Leanne S Bohannon et al. “Eye contact and video-mediated communication: A review”. In: *Displays* 34.2 (#apr# 2013), pages 177–185 (cited on page 130).

[185] Holger Regenbrecht and Tobias Langlotz. “Mutual Gaze Support in Videoconferencing Reviewed”. In: *Communications of the Association for Information Systems* 37.1 (2015), page 45 (cited on page 130).

[186] Jim Steinmeyer. *The Science Behind the Ghost!: A Brief History of Pepper's Ghost*. Hahne, 2013 (cited on page 130).

[187] Adolph H Rosenthal. *Two-way television communication unit*. 1947 (cited on page 130).

[188] William Buxton. "Telepresence: Integrating shared task and person spaces". In: *Proceedings of graphics interface*. Volume 92. 1992, pages 123–129 (cited on pages 130, 132).

[189] Roel Vertegaal and Ivo Weevers. "GAZE-2: conveying eye contact in group video conferencing using eye-controlled camera direction". In: *Proceedings of the SIGCHI ...* 5 (2003), pages 521–528 (cited on page 131).

[190] N F Troje and U Siebeck. "Illumination-induced apparent shift in orientation of human heads". en. In: *Perception* 27.6 (1998), pages 671–680 (cited on page 131).

[191] Steven M Boker et al. "Something in the way we move: Motion dynamics, not perceived sex, influence head movements in conversation". en. In: *J. Exp. Psychol. Hum. Percept. Perform.* 37.3 (#jun# 2011), pages 874–891 (cited on page 131).

[192] M St John et al. "The use of 2D and 3D displays for shape-understanding versus relative-position tasks". en. In: *Hum. Factors* 43.1 (2001), pages 79–98 (cited on page 131).

[193] Jeremy N Bailenson, Andrew C Beall, and Jim Blascovich. "Gaze And Task Performance In Shared Virtual Environments". In: volume 13. 2002, pages 313–320 (cited on page 131).

[194] Rutger Rienks, Ronald Poppe, and Dirk Heylen. "Differences in head orientation behavior for speakers and listeners: An experiment in a virtual environment". #jan# 2010 (cited on page 131).

[195] David T Nguyen and John Canny. "More than face-to-face: empathy effects of video framing". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '09. Boston, MA, USA: Association for Computing Machinery, #apr# 2009, pages 423–432 (cited on pages 131, 132, 143).

[196] P Ekman. "Facial expression and emotion". en. In: *Am. Psychol.* 48.4 (#apr# 1993), pages 384–392 (cited on pages 131, 132).

[197] S Goldin-Meadow. "The role of gesture in communication and thinking". In: volume 3. 1999, pages 419–429 (cited on page 131).

[198] Nicole Chovil. "Discourse ?oriented facial displays in conversation". In: *Research on Language and Social Interaction* 25.1-4 (#jan# 1991), pages 163–194 (cited on page 132).

[199] Diane J Schiano, Sheryl M Ehrlich, and Kyle Sheridan. "Categorical imperative NOT: facial affect is perceived continuously". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '04. Vienna, Austria: Association for Computing Machinery, #apr# 2004, pages 49–56 (cited on page 132).

[200] K Ohba et al. "Facial expression space for smooth tele-communications". In: *Proceedings Third IEEE International Conference on Automatic Face and Gesture Recognition*. #apr# 1998, pages 378–383 (cited on page 132).

[201] Stefan G Hofmann, Michael Suvak, and Brett T Litz. “Sex differences in face recognition and influence of facial affect”. In: *Pers. Individ. Dif.* 40.8 (#jun# 2006), pages 1683–1690 (cited on pages 132, 134, 135).

[202] Jana M Iverson and Susan Goldin-Meadow. “Gesture paves the way for language development”. en. In: *Psychol. Sci.* 16.5 (#may# 2005), pages 367–371 (cited on page 132).

[203] Robert M Krauss, Yihsiu Chen, and Purnima Chawla. “Nonverbal Behavior and Nonverbal Communication: What do Conversational Hand Gestures Tell Us?” In: *Advances in Experimental Social Psychology*. Edited by Mark P Zanna. Volume 28. Academic Press, #jan# 1996, pages 389–450 (cited on page 132).

[204] A Kleinsmith and N Bianchi-Berthouze. “Affective Body Expression Perception and Recognition: A Survey”. In: *IEEE Transactions on Affective Computing* 4.1 (#jan# 2013), pages 15–33 (cited on page 132).

[205] Emanuel A Schegloff. “Body torque”. In: *Soc. Res.* (1998), pages 535–596 (cited on page 132).

[206] Jiazhi Ou et al. “Effects of task properties, partner actions, and message content on eye gaze patterns in a collaborative task”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’05. Portland, Oregon, USA: Association for Computing Machinery, #apr# 2005, pages 231–240 (cited on page 132).

[207] Norman Murray et al. “Eye gaze in virtual environments: evaluating the need and initial work on implementation”. In: *Concurr. Comput.* 21.11 (#aug# 2009), pages 1437–1449 (cited on page 132).

[208] Anthony Tang et al. “Three’s company: understanding communication channels in three-way distributed collaboration”. In: *Proceedings of the 2010 ACM conference on Computer supported cooperative work*. CSCW ’10. Savannah, Georgia, USA: Association for Computing Machinery, #feb# 2010, pages 271–280 (cited on page 132).

[209] Edward Tse et al. “How pairs interact over a multimodal digital table”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’07. San Jose, California, USA: Association for Computing Machinery, #apr# 2007, pages 215–218 (cited on page 132).

[210] Anthony Tang et al. “Collaborative coupling over tabletop displays”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’06. Montréal, Québec, Canada: Association for Computing Machinery, #apr# 2006, pages 1181–1190 (cited on page 132).

[211] James Norris, Holger M Schnädelbach, and Paul K Luff. “Putting things in focus: establishing co-orientation through video in context”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’13. Paris, France: Association for Computing Machinery, #apr# 2013, pages 1329–1338 (cited on page 133).

[212] James Norris, Holger Schnädelbach, and Guoping Qiu. “CamBlend: an object focused collaboration tool”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, #may# 2012, pages 627–636 (cited on page 133).

[213] Paul Luff et al. “Hands on hitchcock: embodied reference to a moving scene”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. Vancouver, BC, Canada: Association for Computing Machinery, #may# 2011, pages 43–52 (cited on page 133).

[214] Philip Tuddenham and Peter Robinson. “Territorial coordination and workspace awareness in remote tabletop collaboration”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’09. Boston, MA, USA: Association for Computing Machinery, #apr# 2009, pages 2139–2148 (cited on page 133).

[215] Izdihar Jamil et al. “The effects of interaction techniques on talk patterns in collaborative peer learning around interactive tables”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. Vancouver, BC, Canada: Association for Computing Machinery, #may# 2011, pages 3043–3052 (cited on page 133).

[216] Hans-Christian Jetter et al. “Materializing the query with facet-streams: a hybrid surface for collaborative search on tabletops”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. Vancouver, BC, Canada: Association for Computing Machinery, #may# 2011, pages 3013–3022 (cited on page 133).

[217] Edward Twitchell Hall and Edward T Hall. *The Hidden Dimension*. Volume 1990. Anchor Books New York, 1969 (cited on pages 133, 135).

[218] O Michael Watson and Theodore D Graves. “Quantitative Research in Proxemic Behavior”. In: *Am. Anthropol.* 68.4 (#aug# 1966), pages 971–985 (cited on page 134).

[219] Nicola Bruno and Michela Muzzolini. “Proxemics Revisited: Similar Effects of Arms Length on Men’s and Women’s Personal Distances”. In: *Universal Journal of Psychology* 1.2 (2013), pages 46–52 (cited on page 134).

[220] Gillian Slessor, Louise H Phillips, and Rebecca Bull. “Age-related declines in basic social perception: evidence from tasks assessing eye-gaze processing”. en. In: *Psychol. Aging* 23.4 (#dec# 2008), pages 812–822 (cited on pages 134, 135).

[221] Nick Yee, Jeremy N Bailenson, and Kathryn Rickertsen. “A meta-analysis of the impact of the inclusion and realism of human-like faces on user experiences in interfaces”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’07. San Jose, California, USA: Association for Computing Machinery, #apr# 2007, pages 1–10 (cited on pages 134, 141).

[222] Jeremy N Bailenson et al. “Equilibrium theory revisited: Mutual gaze and personal space in virtual environments”. In: volume 10. MIT Press, 2001, pages 583–598 (cited on page 134).

[223] Jeremy N Bailenson et al. “Interpersonal distance in immersive virtual environments”. en. In: *Pers. Soc. Psychol. Bull.* 29.7 (#jul# 2003), pages 819–833 (cited on page 134).

[224] Jim Blascovich. “A theoretical model of social influence for increasing the utility of collaborative virtual environments”. In: *Proceedings of the 4th international conference on Collaborative virtual environments*. CVE ’02. Bonn, Germany: Association for Computing Machinery, #sep# 2002, pages 25–30 (cited on page 134).

[225] Hiroyuki Maeda et al. “Real World Video Avatar: Transmission And Presentation Of Human Figure”. In: *Virtual Reality, 2004. Proceedings. IEEE*. 2004, pages 237–238 (cited on page 134).

[226] Joseph C Hager and Paul Ekman. “Long-distance of transmission of facial affect signals”. In: *Ethol. Sociobiol.* 1.1 (#oct# 1979), pages 77–82 (cited on page 135).

[227] Donal E Carlston. *The Oxford Handbook of Social Cognition*. en. Oxford Library of Psychology. OUP USA, #sep# 2013 (cited on page 135).

[228] Eva Deckers et al. “Designing for perceptual crossing: designing and comparing three behaviors”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’13. Paris, France: Association for Computing Machinery, #apr# 2013, pages 1901–1910 (cited on page 135).

[229] J J Gibson and A D Pick. “Perception of another person’s looking behavior”. en. In: *Am. J. Psychol.* 76.3 (#sep# 1963), pages 386–394 (cited on page 135).

[230] Gary Bente, W C Donaghy, and Dorit Suwelack. “Sex Differences In Body Movement And Visual Attention: An Integrated Analysis Of Movement And Gaze In Mixed-sex Dyads”. In: volume 22. 1998 (cited on page 135).

[231] Xueni Pan, Marco Gillies, and Mel Slater. “Male Bodily Responses during an Interaction with a Virtual Woman”. In: *Intelligent Virtual Agents*. Edited by Helmut Prendinger, James C Lester, and Mitsuru Ishizuka. Volume 5208. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2008, pages 89–96 (cited on page 135).

[232] Roel Vertegaal. “Catching the eye: management of joint attention in cooperative work”. In: 1997 (cited on page 135).

[233] D I Fels and P L Weiss. “Toward determining an attention-getting device for improving interaction during video-mediated communication”. In: *Comput. Human Behav.* 16.2 (#mar# 2000), pages 189–198 (cited on page 135).

[234] Amy Voida et al. “Cross-cutting faultlines of location and shared identity in the intergroup cooperation of partially distributed groups”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, #may# 2012, pages 3101–3110 (cited on page 135).

[235] Charles R Berger and Richard J Calabrese. “Some Explorations in Initial Interaction and Beyond: Toward a Developmental Theory of Interpersonal Communication”. In: *Hum. Commun. Res.* 1.2 (#dec# 1975), pages 99–112 (cited on page 135).

[236] Edward Ellsworth Jones and Richard E Nisbett. “The Actor And The Observer: Divergent Perceptions Of The Causes Of Behavior”. In: General Learning Press Morristown, NJ, 1971 (cited on page 136).

[237] Alaeddine Mihoub et al. “Learning multimodal behavioral models for face-to-face social interaction”. In: *Journal on Multimodal User Interfaces* 9.3 (#sep# 2015), pages 195–210 (cited on page 136).

[238] John Doerr. *Measure what matters: How Google, Bono, and the Gates Foundation rock the world with OKRs*. Penguin, 2018 (cited on page 136).

[239] T L Chartrand and J A Bargh. “The chameleon effect: the perception-behavior link and social interaction”. en. In: *J. Pers. Soc. Psychol.* 76.6 (#jun# 1999), pages 893–910 (cited on page 136).

[240] H M Parsons. “What Happened at Hawthorne?: New evidence suggests the Hawthorne effect resulted from operant reinforcement contingencies”. en. In: *Science* 183.4128 (#mar# 1974), pages 922–932 (cited on page 136).

[241] Evan F Risko and Alan Kingstone. “Eyes wide shut: implied social presence, eye tracking and attention”. en. In: *Atten. Percept. Psychophys.* 73.2 (#feb# 2011), pages 291–296 (cited on page 136).

[242] Glenn R Fox et al. “Neural correlates of gratitude”. In: *Frontiers in psychology* (2015), page 1491 (cited on page 136).

[243] Peter Kollock. “Social Dilemmas: The Anatomy of Cooperation”. In: *Annu. Rev. Sociol.* 24.1 (#aug# 1998), pages 183–214 (cited on page 136).

[244] Elisabeth Cuddihy and Deborah Walters. “Embodied interaction in social virtual environments”. In: *Proceedings of the third international conference on Collaborative virtual environments*. CVE ’00. San Francisco, California, USA: Association for Computing Machinery, #sep# 2000, pages 181–188 (cited on page 136).

[245] Jeffrey T Hancock, Jennifer Thom-Santelli, and Thompson Ritchie. “Deception and design: the impact of communication technology on lying behavior”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’04. Vienna, Austria: Association for Computing Machinery, #apr# 2004, pages 129–134 (cited on page 136).

[246] Håkan J Holm and Toshiji Kawagoe. “Face-to-face lying – An experimental study in Sweden and Japan”. In: *J. Econ. Psychol.* 31.3 (#jun# 2010), pages 310–321 (cited on page 136).

[247] Stephen Porter and Leanne ten Brinke. “Reading between the lies: identifying concealed and falsified emotions in universal facial expressions”. en. In: *Psychol. Sci.* 19.5 (#may# 2008), pages 508–514 (cited on page 136).

[248] D J Roberts et al. “withyou—An Experimental End-to-End Telepresence System Using Video-Based Reconstruction”. In: *IEEE J. Sel. Top. Signal Process.* 9.3 (#apr# 2015), pages 562–574 (cited on page 136).

[249] Dennis Beck et al. “Synthesizing presence: A multidisciplinary review of the literature”. In: volume 3. 2011 (cited on pages 136, 137).

[250] M J Schuemie et al. “Research on presence in virtual reality: a survey”. en. In: *Cyberpsychol. Behav.* 4.2 (#apr# 2001), pages 183–201 (cited on page 136).

[251] Mel Slater. “Measuring Presence: A Response to the Witmer and Singer Presence Questionnaire”. In: *Presence: Teleoperators and Virtual Environments* 8.5 (#oct# 1999), pages 560–565 (cited on page 136).

[252] Carrie Heeter. “Being There: The Subjective Experience of Presence”. In: *Presence: Teleoperators and Virtual Environments* 1.2 (#jan# 1992), pages 262–271 (cited on page 137).

[253] Frank Biocca. “The Cyborg Dilemma : Embodiment in Virtual Environments”. In: 1997, pages 12–26 (cited on page 137).

[254] Janet Fulk et al. “A Social Information Processing Model of Media Use in Organizations”. In: *Communic. Res.* 14.5 (#oct# 1987), pages 529–552 (cited on page 137).

[255] Caroline Haythornthwaite, Barry Wellman, and Marilyn Mantei. “Work relationships and media use: A social network analysis”. In: *Group Decision and Negotiation* 4.3 (#may# 1995), pages 193–211 (cited on page 137).

[256] Charlotte N Gunawardena and Frank J Zittle. “Social presence as a predictor of satisfaction within a computer ?mediated conferencing environment”. In: *Am. J. Distance Educ.* 11.3 (#jan# 1997), pages 8–26 (cited on pages 137, 138).

[257] Kristen Nowak. “Defining and differentiating copresence, social presence and presence as transportation”. In: *Presence 2001 Conference, Philadelphia, PA*. 2001, pages 1–23 (cited on pages 137, 138).

[258] Saniye Tugba Bulu. “Place presence, social presence, co-presence, and satisfaction in virtual worlds”. In: *Comput. Educ.* 58.1 (#jan# 2012), pages 154–161 (cited on page 137).

[259] Frank Biocca, Chad Harms, and Judee Burgoon. “Toward a more robust theory and measure of social presence: Review and suggested criteria”. In: volume 12. MIT press, 2003, pages 456–480 (cited on pages 137, 138).

[260] D Randy Garrison, Terry Anderson, and Walter Archer. “Critical Inquiry In A Text-based Environment: Computer Conferencing In Higher Education”. In: volume 2. Elsevier, 1999, pages 87–105 (cited on page 137).

[261] Yevgenia Bondareva and Don Bouwhuis. “Determinants of social presence in videoconferencing”. In: *AVI2004 Workshop on Environments for Personalized Information Access*. 2004, pages 1–9 (cited on pages 137, 138).

[262] Mel Slater. “How Colorful Was Your Day? Why Questionnaires Cannot Assess Presence in Virtual Environments”. In: *Presence: Teleoperators and Virtual Environments* 13.4 (#aug# 2004), pages 484–493 (cited on page 138).

[263] Martin Usoh et al. *Using Presence Questionnaires in Reality. (Usoh et al, 2000).pdf*. 2000 (cited on page 138).

[264] Joy Van Baren and Wijnand IJsselsteijn. *Measuring presence: A guide to current measurement approaches*. 2004 (cited on page 138).

[265] Chad Harms and Frank Biocca. “Internal consistency and reliability of the networked minds measure of social presence”. In: (2004) (cited on page 138).

[266] Jörg Hauber et al. “Social presence in two-and three-dimensional videoconferencing”. In: (2005) (cited on page 138).

[267] Jörg Hauber et al. “Spatiality in videoconferencing: trade-offs between efficiency and social presence”. In: *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*. CSCW ’06. Banff, Alberta, Canada: Association for Computing Machinery, #nov# 2006, pages 413–422 (cited on page 139).

[268] Peter Kauff and Oliver Schreer. “An immersive 3D video-conferencing system using shared virtual team user environments”. In: *Proceedings of the 4th international conference on Collaborative virtual environments*. CVE ’02. Bonn, Germany: Association for Computing Machinery, #sep# 2002, pages 105–112 (cited on page 139).

[269] Peter Kauff and Oliver Schreer. “Virtual team user environments-a step from tele-cubicles towards distributed tele-collaboration in mediated workspaces”. In: *Multimedia and Expo, 2002. ICME’02. Proceedings. 2002 IEEE International Conference on*. Volume 2. 2002, pages 9–12 (cited on page 139).

[270] H Fuchs et al. “3D Tele-Collaboration over internet 2”. In: *International Workshop on Immersive Telepresence (ITP ’02)*. Juan Les Pin, 2002 (cited on page 139).

[271] Andrew Jones et al. “HeadSPIN: a one-to-many 3D video teleconferencing system”. In: *ACM SIGGRAPH 2009 Emerging Technologies*. SIGGRAPH ’09 Article 13. New Orleans, Louisiana: Association for Computing Machinery, #aug# 2009, page 1 (cited on pages 139, 140).

[272] Yusuke Ichikawa et al. “MAJIC Videoconferencing System: Experiments, Evaluation and Improvement”. In: *Proceedings of the Fourth European Conference on Computer-Supported Cooperative Work ECSCW ’95: 10–14 September, 1995, Stockholm, Sweden*. Edited by Hans Marmolin, Yngve Sundblad, and Kjeld Schmidt. Dordrecht: Springer Netherlands, 1995, pages 279–292 (cited on page 139).

[273] Ken-Ichi Okada et al. “Multiparty videoconferencing at virtual social distance: MAJIC design”. In: *Proceedings of the 1994 ACM conference on Computer supported cooperative work*. CSCW ’94. Chapel Hill, North Carolina, USA: Association for Computing Machinery, #oct# 1994, pages 385–393 (cited on page 139).

[274] Daniel Gotsch et al. “TeleHuman2: A Cylindrical Light Field Teleconferencing System for Life-size 3D Human Telepresence”. In: *CHI*. 2018, page 522 (cited on page 140).

[275] Alexander Kulik et al. “C1x6: a stereoscopic six-user display for co-located collaboration in shared virtual environments”. In: *Proceedings of the 2011 SIGGRAPH Asia Conference*. Volume 30. SA ’11 Article 188. Hong Kong, China: Association for Computing Machinery, #dec# 2011, pages 1–12 (cited on page 140).

[276] Kazuhiro Otsuka et al. “MM+Space: n x 4 degree-of-freedom kinetic display for recreating multiparty conversation spaces”. In: *Proceedings of the 15th ACM on International conference on multimodal interaction*. ICMI ’13. Sydney, Australia: Association for Computing Machinery, #dec# 2013, pages 389–396 (cited on page 140).

[277] P-A Blanche et al. “Holographic three-dimensional telepresence using large-area photorefractive polymer”. In: volume 468. 2010, pages 80–83 (cited on page 140).

[278] Savaş Tay et al. “An updatable holographic three-dimensional display”. en. In: *Nature* 451.7179 (#feb# 2008), pages 694–698 (cited on page 140).

[279] Osman Eldes, Kaan Akşit, and Hakan Urey. “Multi-view autostereoscopic projection display using rotating screen”. en. In: *Opt. Express* 21.23 (#nov# 2013), pages 29043–29054 (cited on page 140).

[280] Tomohiro Yendo et al. “The Seelinder: Cylindrical 3D display viewable from 360 degrees”. In: *J. Vis. Commun. Image Represent.* 21.5 (#jul# 2010), pages 586–594 (cited on page 140).

[281] Chen Cao, Tomas Simon, Jin Kyu Kim, et al. “Authentic Volume Avatars from Phone Scans”. In: *ACM Transactions in Graphics* (2022). URL: https://drive.google.com/file/d/1i4NJKAggS82wqMamCJ1OHRGgViuyoY6R (cited on page 140).

[282] Masahiro Mori. “The uncanny valley”. In: *Energy* 7.4 (1970), pages 33–35 (cited on pages 140, 142).

[283] C Bartneck et al. “Is The Uncanny Valley An Uncanny Cliff?” In: *RO-MAN 2007 - The 16th IEEE International Symposium on Robot and Human Interactive Communication*. #aug# 2007, pages 368–373 (cited on page 141).

[284] Christoph Bartneck et al. “My robotic doppelgänger-A critical look at the uncanny valley”. In: *Robot and Human Interactive Communication, 2009.* 2009, pages 269–276 (cited on page 141).

[285] Wade J Mitchell et al. “A mismatch in the human realism of face and voice produces an uncanny valley”. en. In: *Iperception* 2.1 (#mar# 2011), pages 10–12 (cited on page 141).

[286] Chin-Chang Ho, Karl F MacDorman, and Z A D Dwi Pramono. “Human emotion and the uncanny valley: a GLM, MDS, and Isomap analysis of robot video ratings”. In: *Proceedings of the 3rd ACM/IEEE international conference on Human robot interaction*. HRI ’08. Amsterdam, The Netherlands: Association for Computing Machinery, #mar# 2008, pages 169–176 (cited on page 141).

[287] M Strait and M Scheutz. “Measuring users’ responses to humans, robots, and human-like robots with functional near infrared spectroscopy”. In: *The 23rd IEEE International Symposium on Robot and Human Interactive Communication*. #aug# 2014, pages 1128–1133 (cited on page 141).

[288] Stefan Marti and Chris Schmandt. “Physical embodiments for mobile communication agents”. In: *Proceedings of the 18th annual ACM symposium on User interface software and technology*. UIST ’05. Seattle, WA, USA: Association for Computing Machinery, #oct# 2005, pages 231–240 (cited on page 141).

[289] Sigurdur O Adalgeirsson and Cynthia Breazeal. “MeBot: a robotic platform for socially embodied presence”. In: *Proceedings of the 5th ACM/IEEE international conference on Human-robot interaction*. HRI ’10. Osaka, Japan: IEEE Press, #mar# 2010, pages 15–22 (cited on page 141).

[290] Min Kyung Lee and Leila Takayama. ““Now, i have a body”: uses and social norms for mobile remote presence in the workplace”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. Vancouver, BC, Canada: Association for Computing Machinery, #may# 2011, pages 33–42 (cited on pages 141, 142).

[291] Katherine M Tsui et al. “Exploring use cases for telepresence robots”. In: *Proceedings of the 6th international conference on Human-robot interaction*. HRI ’11. Lausanne, Switzerland: Association for Computing Machinery, #mar# 2011, pages 11–18 (cited on pages 141, 142).

[292] Eric Paulos and John Canny. “PRoP: personal roving presence”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’98. Los Angeles, California, USA: ACM Press/Addison-Wesley Publishing Co., #jan# 1998, pages 296–303 (cited on page 141).

[293] Annica Kristoffersson, Silvia Coradeschi, and Amy Loutfi. “A Review of Mobile Robotic Telepresence”. en. In: *Advances in Human-Computer Interaction* 2013 (#apr# 2013), page 3 (cited on pages 141, 142).

[294] M Desai et al. “Essential features of telepresence robots”. In: *2011 IEEE Conference on Technologies for Practical Robot Applications*. #apr# 2011, pages 15–20 (cited on page 141).

[295] Katherine M Tsui, Munjal Desai, and Holly A Yanco. “Towards measuring the quality of interaction: communication through telepresence robots”. In: *Proceedings of the Workshop on Performance Metrics for Intelligent Systems*. PerMIS ’12. College Park, Maryland: Association for Computing Machinery, #mar# 2012, pages 101–108 (cited on page 141).

[296] Annica Kristoffersson et al. “Sense of Presence in a Robotic Telepresence Domain: 6th International Conference, UAHCI 2011, Held as Part of HCI International 2011, Orlando, FL, USA, July 9-14, 2011, Proceedings, Part II”. In: *Universal Access in Human-Computer Interaction. Users Diversity*. Edited by Constantine Stephanidis. Volume 6766. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pages 479–487 (cited on page 141).

[297] Daisuke Sakamoto et al. “Android as a telecommunication medium with a human-like presence”. In: *Proceedings of the ACM/IEEE international conference on Human-robot interaction*. HRI ’07. Arlington, Virginia, USA: Association for Computing Machinery, #mar# 2007, pages 193–200 (cited on page 142).

[298] P Lincoln et al. “Animatronic Shader Lamps Avatars”. In: *2009 8th IEEE International Symposium on Mixed and Augmented Reality*. #oct# 2009, pages 27–33 (cited on page 142).

[299] Peter Lincoln et al. “Multi-view lenticular display for group teleconferencing”. In: *Proceedings of the 2nd International Conference on Immersive Telecommunications*. ICST, #may# 2010, page 22 (cited on page 142).

[300] Ramesh Raskar et al. “Shader Lamps: Animating Real Objects With Image-Based Illumination: Proceedings of the Eurographics Workshop in London, United Kingdom, June 25–27, 2001”. In: *Rendering Techniques 2001*. Edited by Steven J Gortler and Karol Myszkowski. Volume 20. Eurographics. Vienna: Springer Vienna, 2001, pages 89–102 (cited on page 142).

[301] Oyewole Oyekoya, William Steptoe, and Anthony Steed. “SphereAvatar: a situated display to represent a remote collaborator”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, #may# 2012, pages 2551–2560 (cited on page 142).

[302] Ye Pan and Anthony Steed. “A gaze-preserving situated multiview telepresence system”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’14. Toronto, Ontario, Canada: Association for Computing Machinery, #apr# 2014, pages 2173–2176 (cited on page 142).

[303] Y Pan and A Steed. “Preserving gaze direction in teleconferencing using a camera array and a spherical display”. In: *2012 3DTV-Conference: The True Vision - Capture, Transmission and Display of 3D Video (3DTV-CON)*. #oct# 2012, pages 1–4 (cited on page 142).

[304] Norman P Jouppi et al. “Bireality: mutually-immersive telepresence”. In: *Proceedings of the 12th annual ACM international conference on Multimedia*. 2004, pages 860–867 (cited on page 142).

[305] Arjun Nagendran et al. “Continuum of virtual-human space: towards improved interaction strategies for physical-virtual avatars”. In: *Proceedings of the 11th ACM SIGGRAPH International Conference on Virtual-Reality Continuum and its Applications in Industry*. VRCAI ’12. Singapore, Singapore: Association for Computing Machinery, #dec# 2012, pages 135–142 (cited on page 142).

[306] Kazuko Itoh et al. “Development of face robot to express the individual face by optimizing the facial features”. In: *Humanoid Robots, International Conference on*. 2005, pages 412–417 (cited on page 142).

[307] Nikita Drobyshev et al. “MegaPortraits: One-shot Megapixel Neural Head Avatars”. In: 2022 (cited on page 142).

[308] Ramesh Raskar et al. “The office of the future: A unified approach to image-based modeling and spatially immersive displays”. In: *Proceedings of the 25th annual conference on Computer graphics and interactive techniques*. 1998, pages 179–188 (cited on page 142).

[309] Diego Rivera-Gutierrez et al. “Shader Lamps Virtual Patients: the physical manifestation of virtual patients”. en. In: *Stud. Health Technol. Inform.* 173 (2012), pages 372–378 (cited on page 142).

[310] D Bandyopadhyay, R Raskar, and H Fuchs. “Dynamic shader lamps : painting on movable objects”. In: *Proceedings IEEE and ACM International Symposium on Augmented Reality*. IEEE Comput. Soc, #oct# 2001, pages 207–216 (cited on page 142).

[311] Peter Dalsgaard and Kim Halskov. “3d projection on physical objects: design insights from five real life cases”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. Vancouver, BC, Canada: Association for Computing Machinery, #may# 2011, pages 1041–1050 (cited on page 142).

[312] L O K Benjamin. “Shader lamps virtual patients: the physical manifestation of virtual patients”. In: *Medicine Meets Virtual Reality 19: NextMed* 173 (2012), page 372 (cited on page 142).

[313] Nannan Xi et al. “The challenges of entering the metaverse: An experiment on the effect of extended reality on workload”. In: *Information Systems Frontiers* (2022), pages 1–22 (cited on page 143).

[314] Verena Biener et al. “Quantifying the Effects of Working in VR for One Week”. In: *arXiv e-prints* (2022), arXiv–2206 (cited on page 143).

[315] Sascha Kraus et al. “Facebook and the creation of the metaverse: radical business model innovation or incremental transformation?” In: *International Journal of Entrepreneurial Behavior & Research* (2022) (cited on page 145).

[316] Thippa Reddy Gadekallu et al. “Blockchain for the Metaverse: A Review”. In: *arXiv preprint arXiv:2203.09738* (2022) (cited on page 148).

[317] Aziz Siyaev and Geun-Sik Jo. “Towards aircraft maintenance metaverse using speech interactions with virtual objects in mixed reality”. In: *Sensors* 21.6 (2021), page 2066 (cited on page 152).

[318] Alex Heiphetz and Gary Woodill. *Training and collaboration with virtual worlds: How to create cost-saving, efficient and engaging programs*. McGraw Hill Professional, 2010 (cited on page 152).

[319] Clark Aldrich. *Learning by doing: A comprehensive guide to simulations, computer games, and pedagogy in e-learning and other educational experiences*. John Wiley & Sons, 2005 (cited on page 152).

[320] Sophie J Nightingale and Hany Farid. “AI-synthesized faces are indistinguishable from real faces and more trustworthy”. In: *Proceedings of the National Academy of Sciences* 119.8 (2022), e2120481119 (cited on page 157).