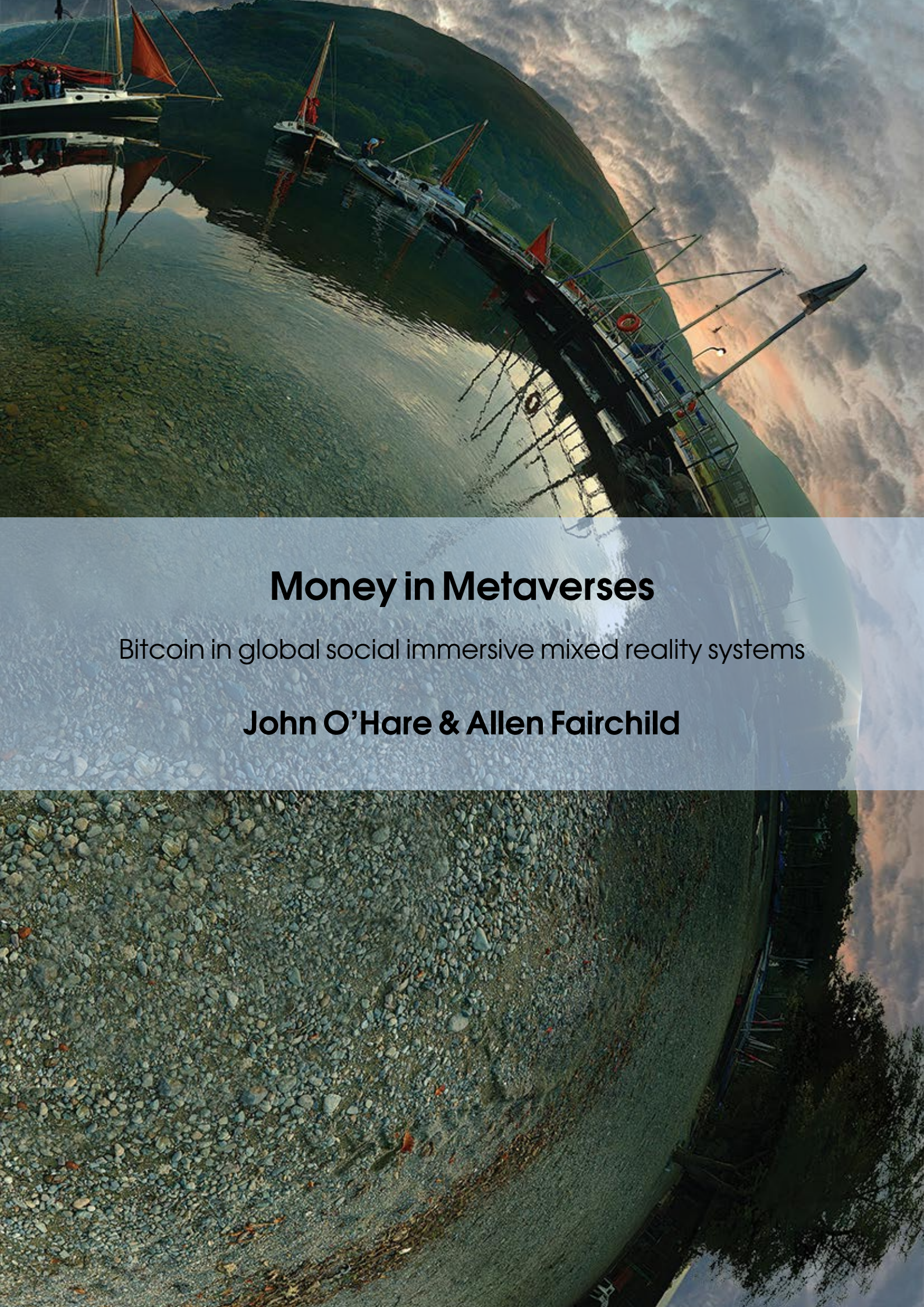


Money in Metaverses

Bitcoin in global social immersive mixed reality systems

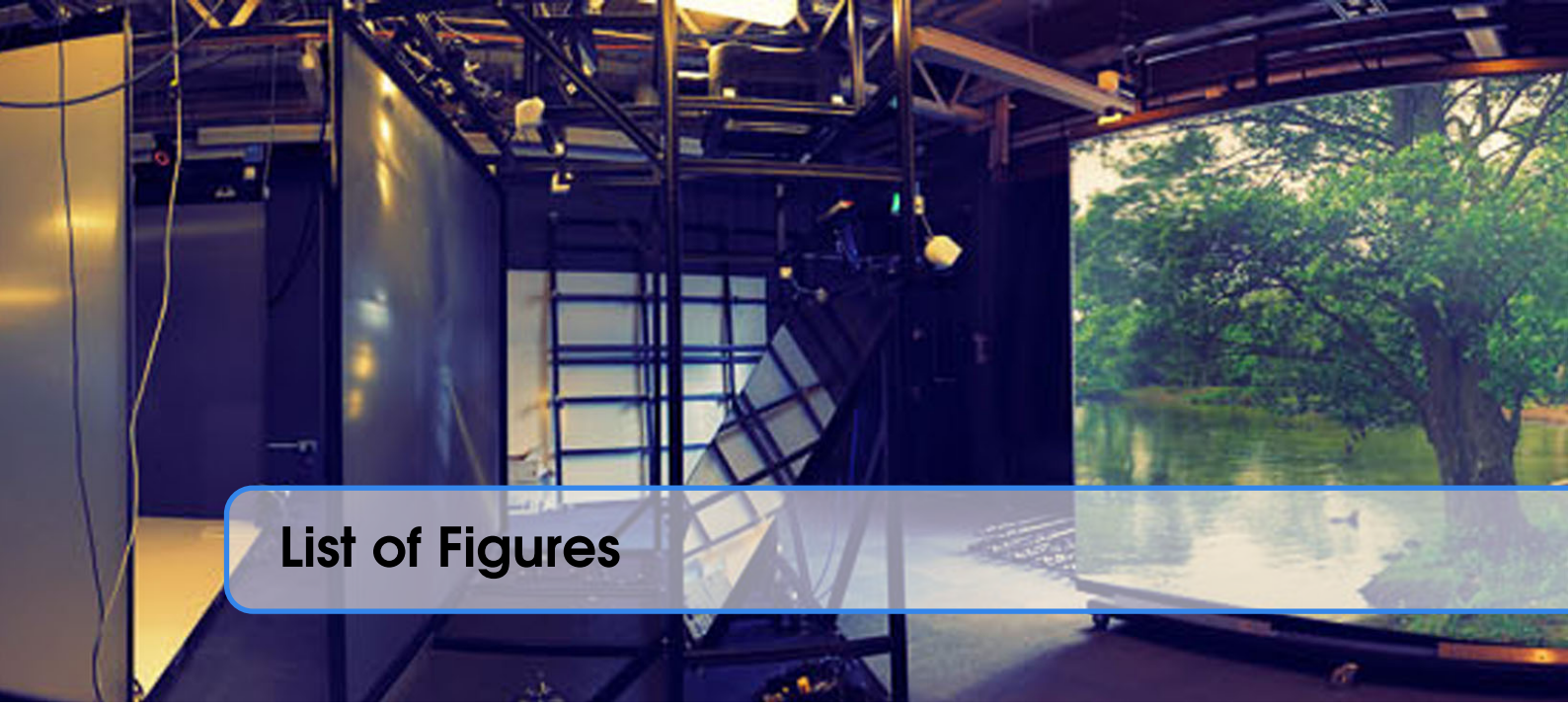
John O'Hare & Allen Fairchild

PUBLISHED BY J.OHARE@SALFORD.AC.UK FOR THE CYBER FOUNDRY PROGRAMME AT THE UNIVERSITY OF SALFORD

RAW GITHUB HYPERLINK

First printing, March 2022

Contents



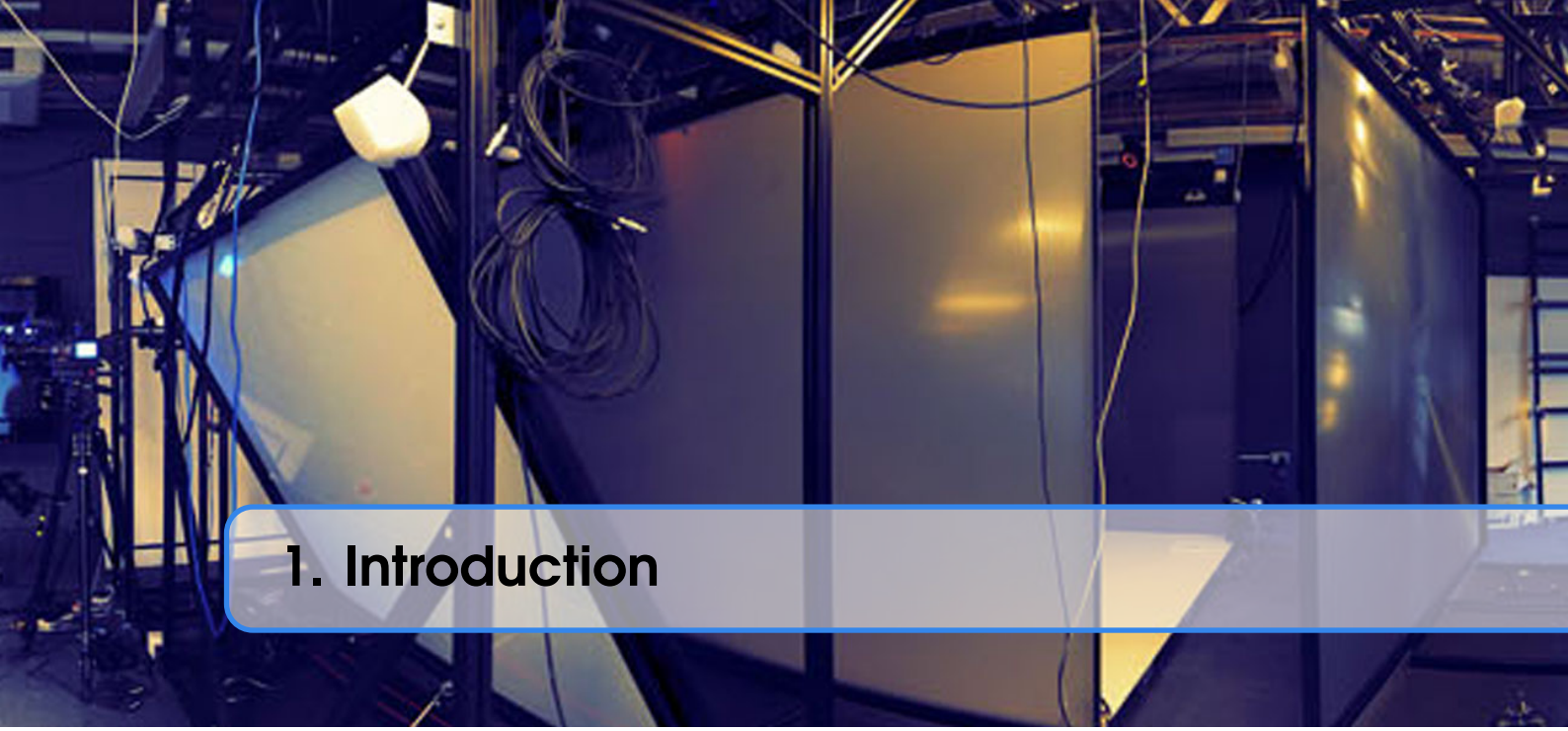
List of Figures

List of Tables

State of the art and proposal

0.1 Conflict of interest statements

The authors own small numbers of the various tokens referenced in the text for experimentation and/or investment purposes. This includes Solana, Ethereum, 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 Abstract

We present a state of the art and positioning book, about Web3, Bitcoin, and 'Metaverse'; describing the intersections and synergies. A high level overview of Web3 technologies leads to a description of blockchain, and the Bitcoin network is specifically selected for detailed examination. Suitable components of the extended Bitcoin ecosystem are described in more depth. Other mechanisms for native digital value transfer are described, with a focus on 'money'. Metaverse technology is over-viewed, primarily from the perspective of Bitcoin and extended reality.
Bitcoin is selected as the best contender for value transfer in metaverses because of it's free and open source nature, and network effect. Challenges and risks of this approach are identified. A cloud deployable virtual machine based technology stack deployment guide with a focus on cybersecurity best practice can be downloaded from GitHub to experiment with the technologies. This deployable lab is designed to inform development of secure value transaction, for small and medium sized companies. Next steps are touched upon in the conclusion.
This is an incomplete document and may frankly contain a bunch of errors. Usual v0.1 caveats apply. It's 100% open source (licensed under the Creative Commons Zero v1.0 Universal) so if something seems wrong pertaining to your project, or you have a suggestion for an improvement, then submit a PR to GitHub.

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. The world's largest pension fund manager Blackrock is adding

these asset to their management engine which manages tens of trillions of dollars. 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".

Meanwhile 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. "

This is has immediate implications for (Small and medium-sized enterprises). It is timely then 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[29])*. Figure 1.1 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 are numeric, while opinion pieces, grey statistics, and pertinent news articles are hyperlinked in blue from the text. As the book develops the veracity of the citations should improve. It is likely that this document is incomplete as you are reading it as it's designed to be an open ended and open source resource. It is an experiment in a living document and repository.

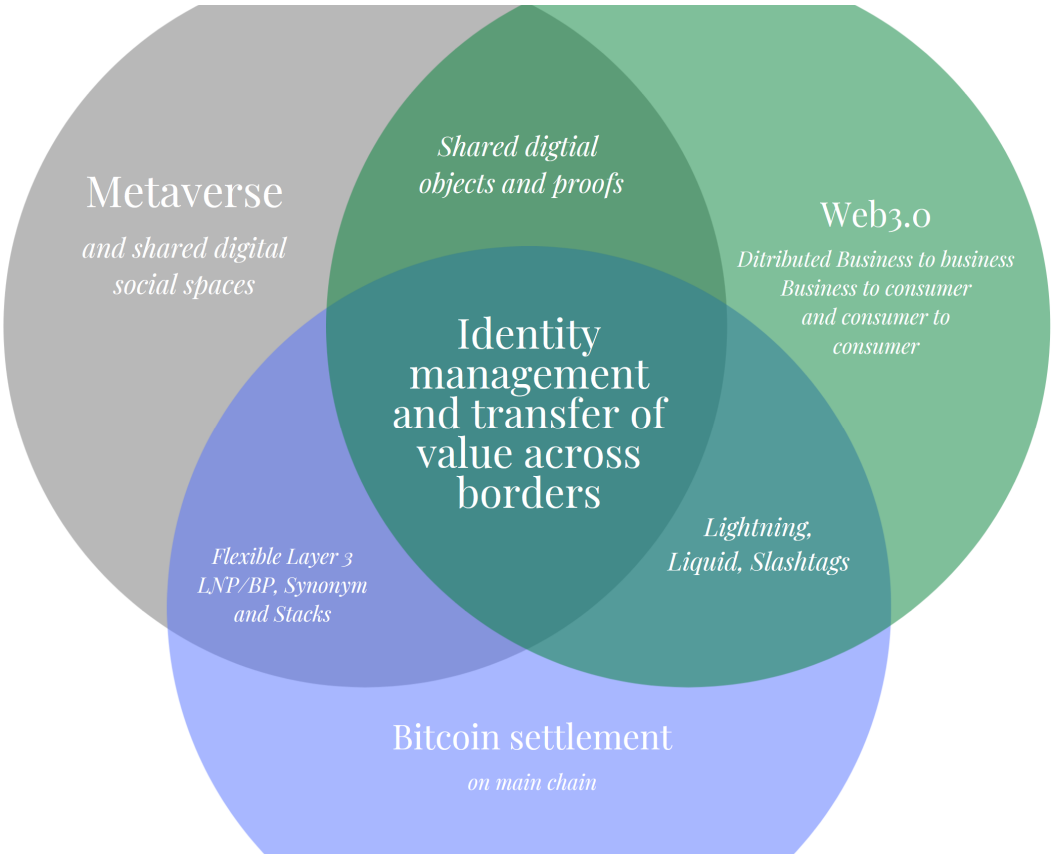


Figure 1.1: Web 3, Metaverse, and Bitcoin are inter-sectional technologies.

2. Web3 / decentralised web

Web3 is a rapidly evolving set of technologies and specifications which are drifting further from their origin. Decentralised web is perhaps a more useful name, but focus in this section will be on the evolution of the popularised term Web3.

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 [6].

“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 [15]. This is as odds with Berners-Lee’s vision.

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 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 cyptographers, and this will be described later.

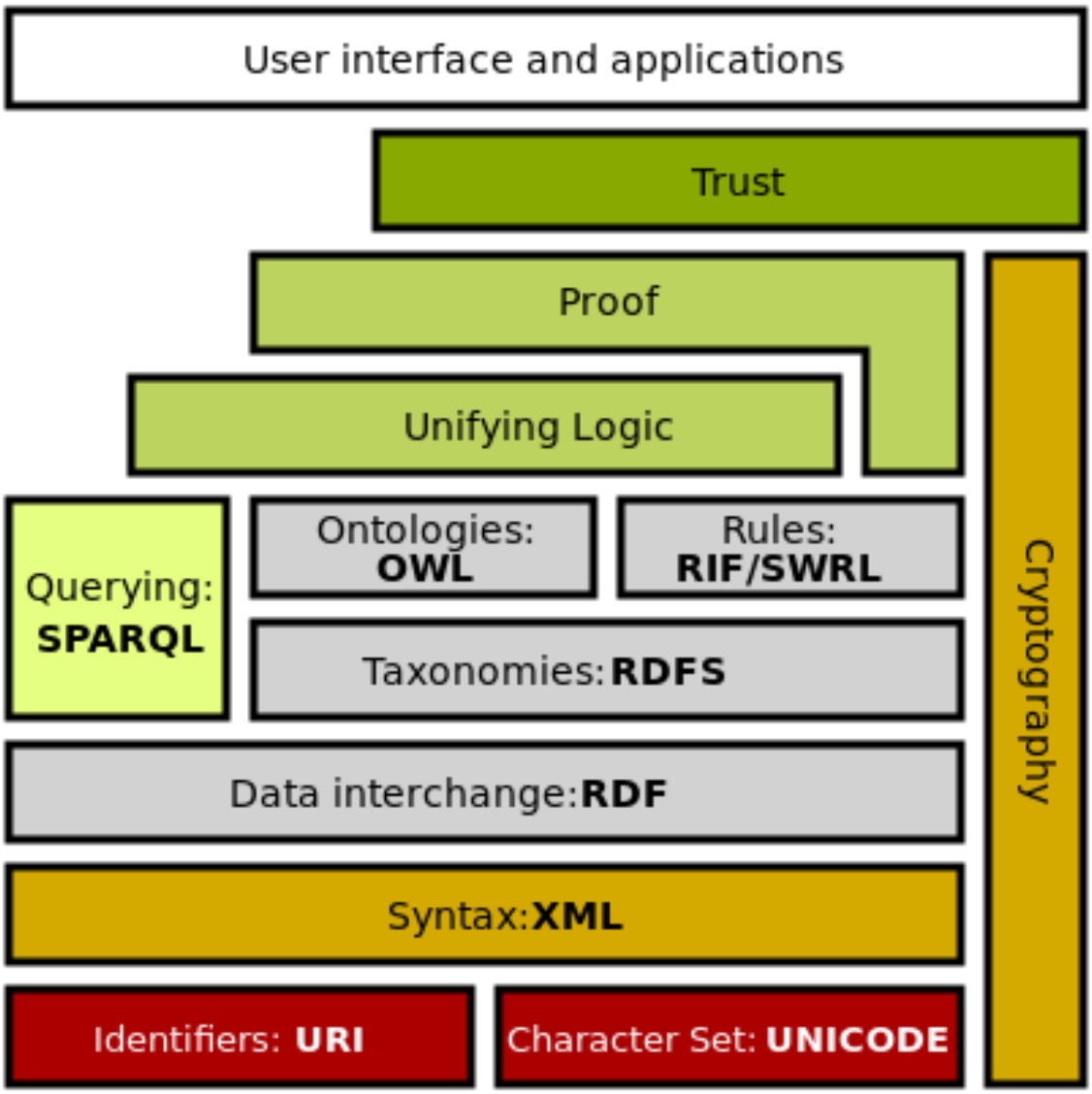


Figure 2.1: Semantic Web Stack [CC0 image]

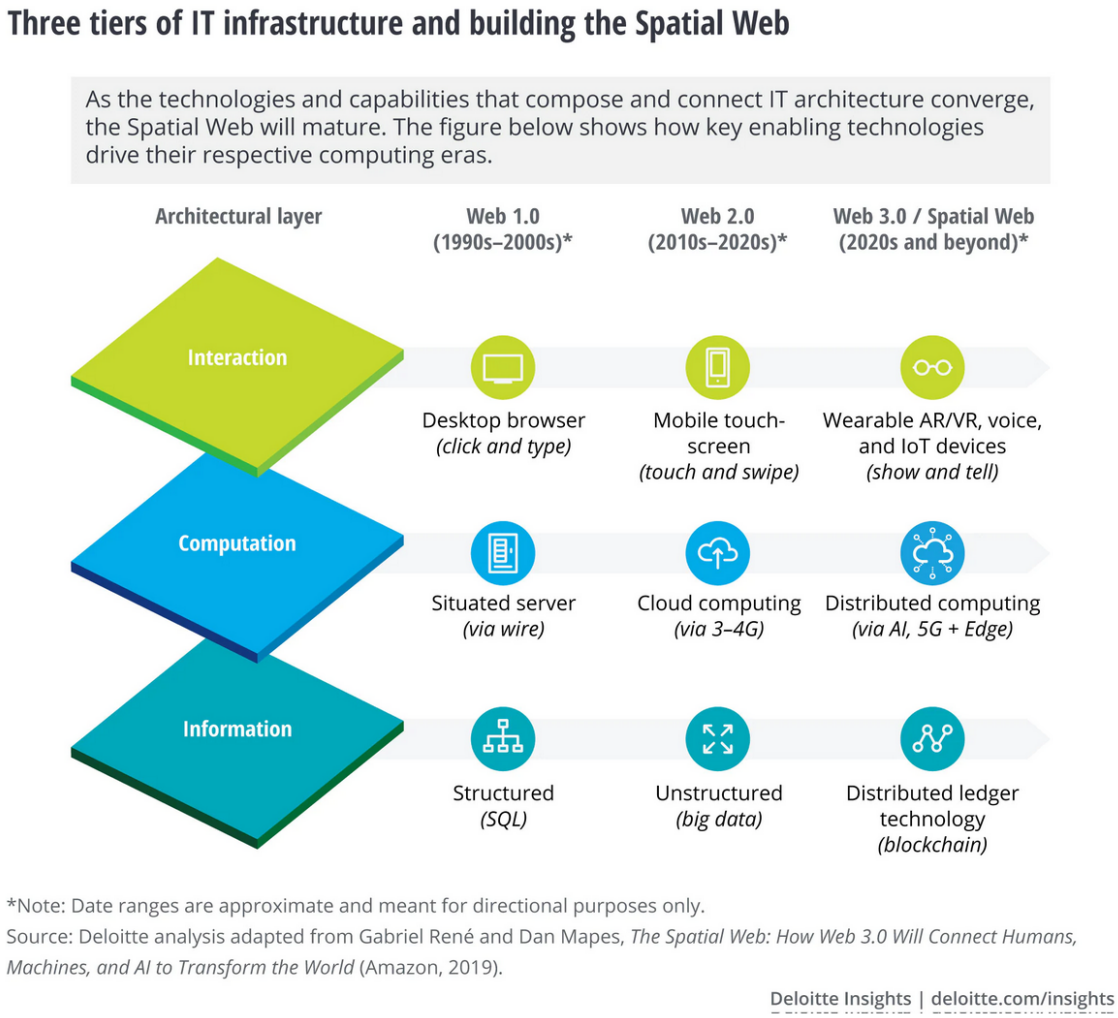


Figure 2.2: Deloitte Spatial Web Overview Reused with permission.

2.2 Spatial web

"The Spatial Web", a blurring of the boundaries between digital and geospatialised 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.

2.3 Webs of trust

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 meta-data, 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

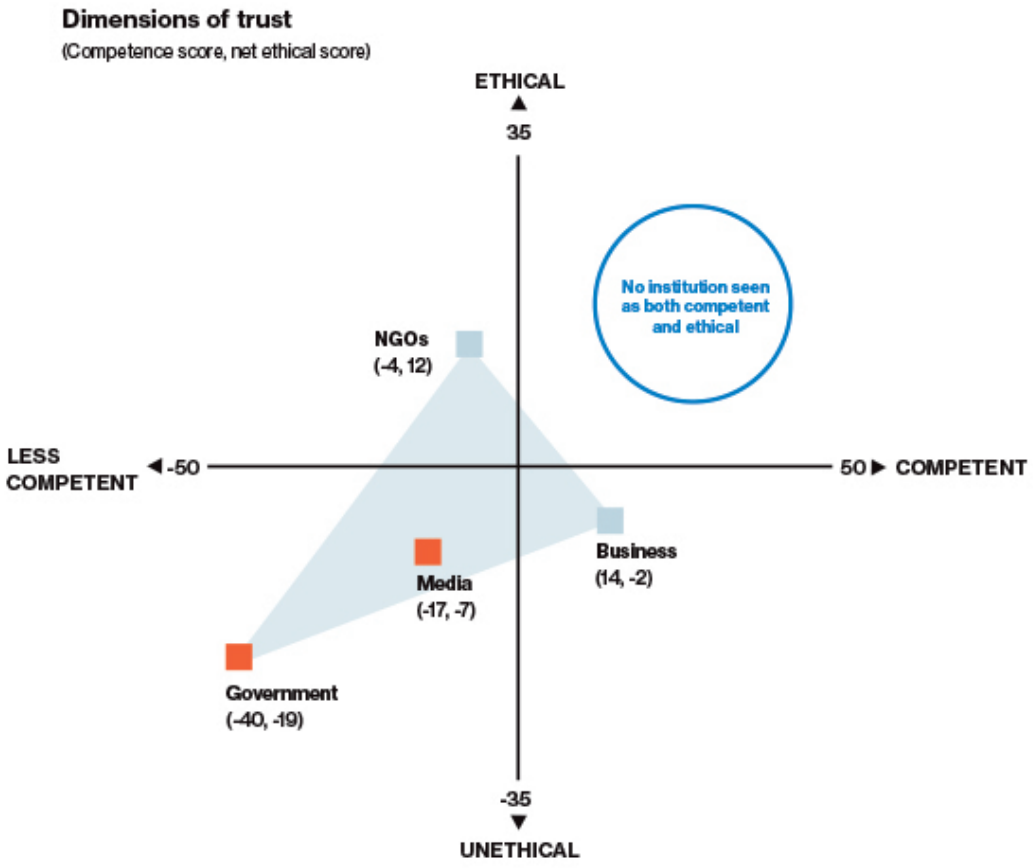


Figure 2.3: Edelman 2020 trust barometer [rights requested]

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 (Figure 2.3), 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.

2.4 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 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 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. 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'

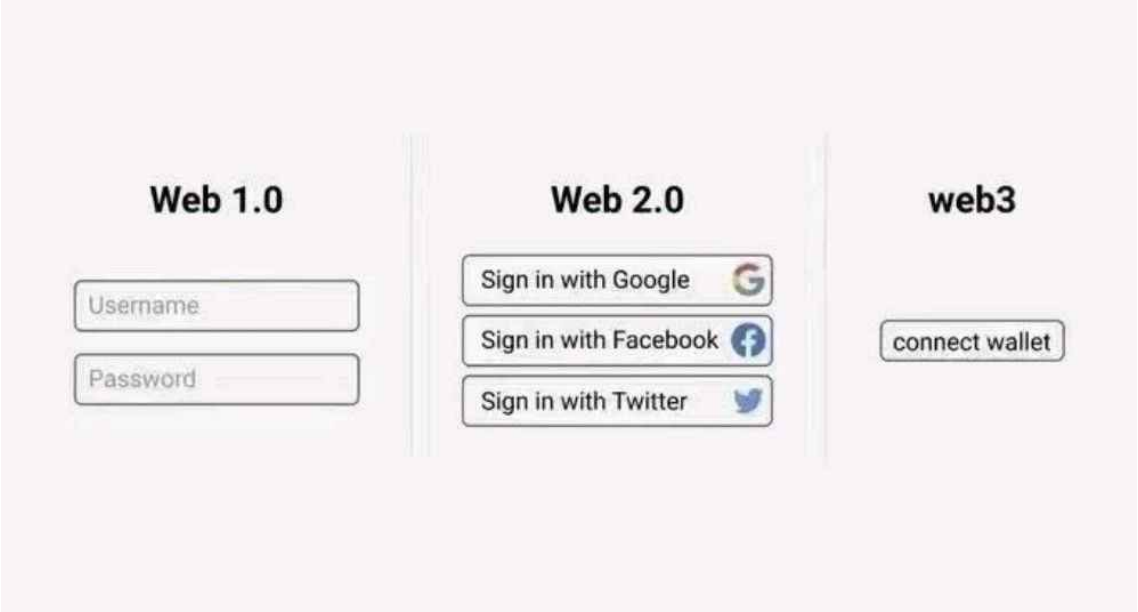


Figure 2.4: A meme showing differing approached to logging in on a website.

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

Many of the mentioned components here will be described later in the book. 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.

Dante Disparte, chief strategy officer of Circle, said in testimony to 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. The suggestion is that this is happening regardless of a decent use case or definition.

It’s a complex evolving narrative, and clearly contradictions are common. Into this confusion this book advances a narrow take, and toolset, which might extract some value from the technologies, while maintaining a low barrier to entry.

2.5 Example applications

2.5.1 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.

2.5.2 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.

2.5.3 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, within the distributed blockchains. This makes them extremely hard to ban, and as a result they operate in a legal gray 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.

2.5.4 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.

2.5.5 Slashtags / Hypercore

Slashtags is a web of trust model decentralised peer to peer 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 metadada managed by the user. It is new and has 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 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. It 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[23]. The first application by the affiliated Hyperdivision team is an open source pear to peer live video streaming app called Dazaar. Once again, it's not clear yet who wants or needs this bit-torrent style service.

2.5.6 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. The authority around naming is centralised in ICANN. There has been talk for many years about 'properly' distributing this database using decentralised/blockchain technologies[30]. 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.

2.5.7 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, 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 be kickstarted.

2.6 The common thread

One feature which persists throughout all of these interpretations of Web3 is the need for decentralised trust. If there is to be no central controlling party(s) as in the Web 2 model then nothing can happen without a cryptographically secure underpinning, which favours no party beyond the terms of their collectively agreed rights and privileges. 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 $13B of capital investment in 2021 alone. At time of writing the industry is a over 2 trillion dollar market. According to Nathaniel Whittemore, a journalist for Coindesk, "The Web3 moniker positions this industry in opposition to big tech". In practice it seems that this is just another avenue for existing players to experiment with new models of control, and is rife with scams.

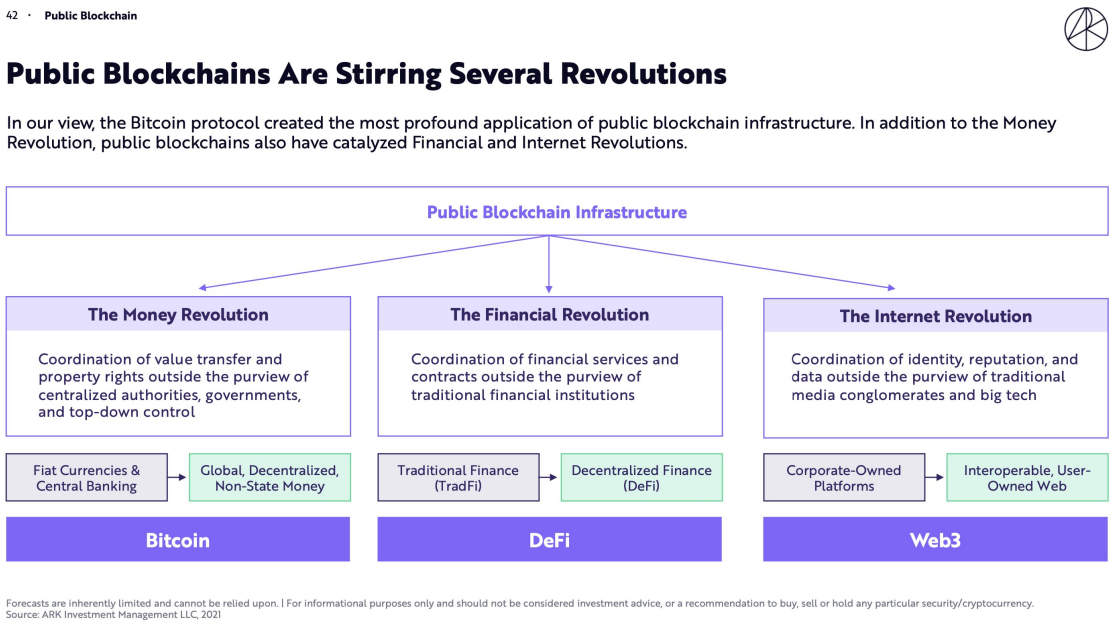


Figure 2.5: ARK slide on Web3. Rights requested

Of their 2022 'Big Ideas' report, ARK investment LLC (who manage $50B tech investment) said the following (Figure 2.5), 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 [44]. 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 figured out how to send messages online without a trusted third party [20, 40].
Soon after the 1980s saw the emergence of the cypherpunk activist movement, as a reaction to the emerging surveillance state [9, 14]. These early computer scientists in the USA saw the emerging intersectionality between information, computation, economics, and personal freedom [33]. Online discussion in the early nineties foresaw the emergence of trans-national digital markets, what would become the WWW [45, 51]. 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' [2] paved the way for later work by introducing the concept of 'proof of work'. This was built upon by Dai [17], Szabo [50], Finney [11], and Nakamoto amongst others. In all it took 16 years of collaboration on the mailing lists to attack the problem of trust minimised, distributed, digital cash. The culmination of these attempts were Bitcoin [41]. This is illustrated by Dan Held in Figure 3.1.
This is now a wider ecosystem of technologies.

There is enormous complexity and scope, as seen in Figure 3.2, and yet genuinely useful products are elusive. It can be argued that the whole concept of crypto/blockchain is somewhat flawed, as the vast majority of the technology offerings are not properly distributed, and "there are many scenarios where traditional databases should be used instead"[13].
It is surprising hard to pin down a simple explanation for the features which define blockchain. These "key takeaway" from Investopedia are a neat summary however.

- Blockchain is a specific type of database.

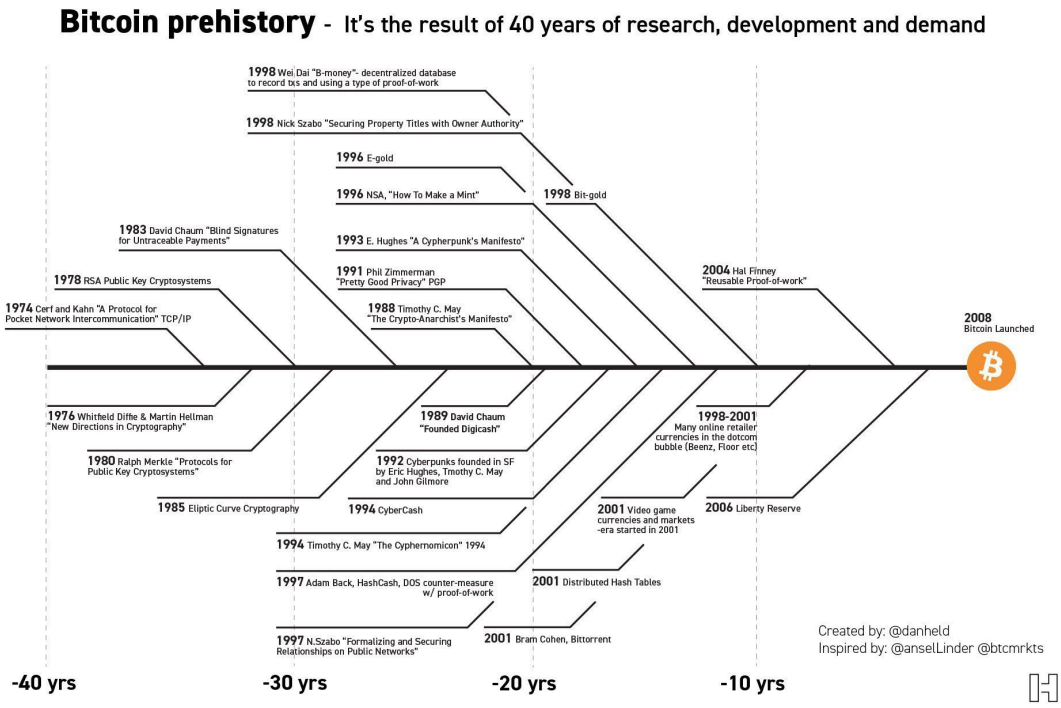


Figure 3.1: Dan Held: Bitcoin prehistory used with permission.

- 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 blockchain can be considered "trust minimised". This is important for some, but not all people. 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. Thanks to a natural fit with strong encryption, and innate resistance to censorship by external parties, these systems lend themselves well to 'borderless' applications. Finally, a host of well engineered open source code repositories makes the cost of adoption relatively low.

Within DLT/blockchain there seem to be as many opinions on the value of the technology as there are implementations. 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

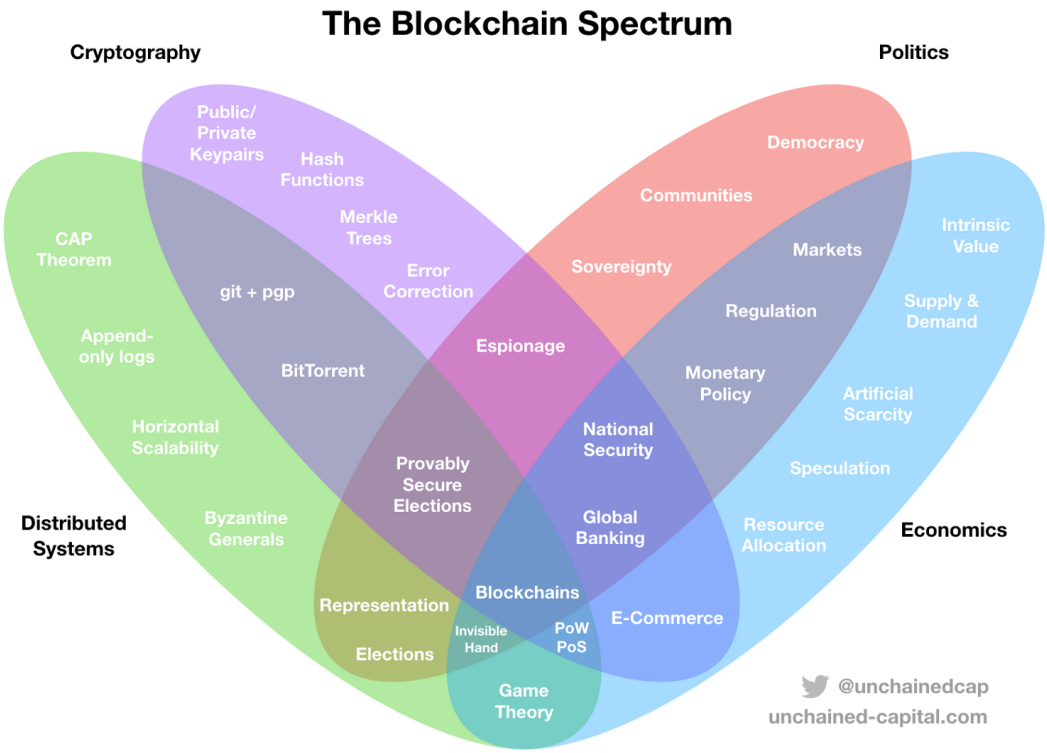


Figure 3.2: Intersecting disciplines. Reused with permission Dhruv Bansal

'scams', and this happens very often [26].
The following sections give an overview of the major strands of the technology. First is Ethereum, mainly to discount it's use and get to more accessible offerings.

3.1 Ethereum

Ethereum [10] is the second most secure public blockchain (by about 50%), and second most valuable by market capitalisation (though this comparison is somewhat strained). It is the natural connection from Web3 to the rest of the paper, so it will be considered first.
It is touted as 'programmable money'. It, unlike bitcoin, is Turing complete, 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 makes 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. Even partial nodes are run chiefly by one specialist cloud provider (Infura), which has recently been forced to exclude Venezuela from the network. 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.
With that said there are many talented developers doing interesting work on the platform, and

Figure 3.3: Ethereum is thought to look like a speculative bubble. Rights requested

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 tradable 'ERC20' tokens, which can accrue value or demonstrate smart contract utility. 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. Most of this money is pure market speculation speculation (as is the case across blockchain). 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 3.3. 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.

Such is the level of nefarious activity on these networks that they have a poor reputation, and are difficult to audit, launch, and maintain. The overriding problem of using a blockchain for utility applications 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

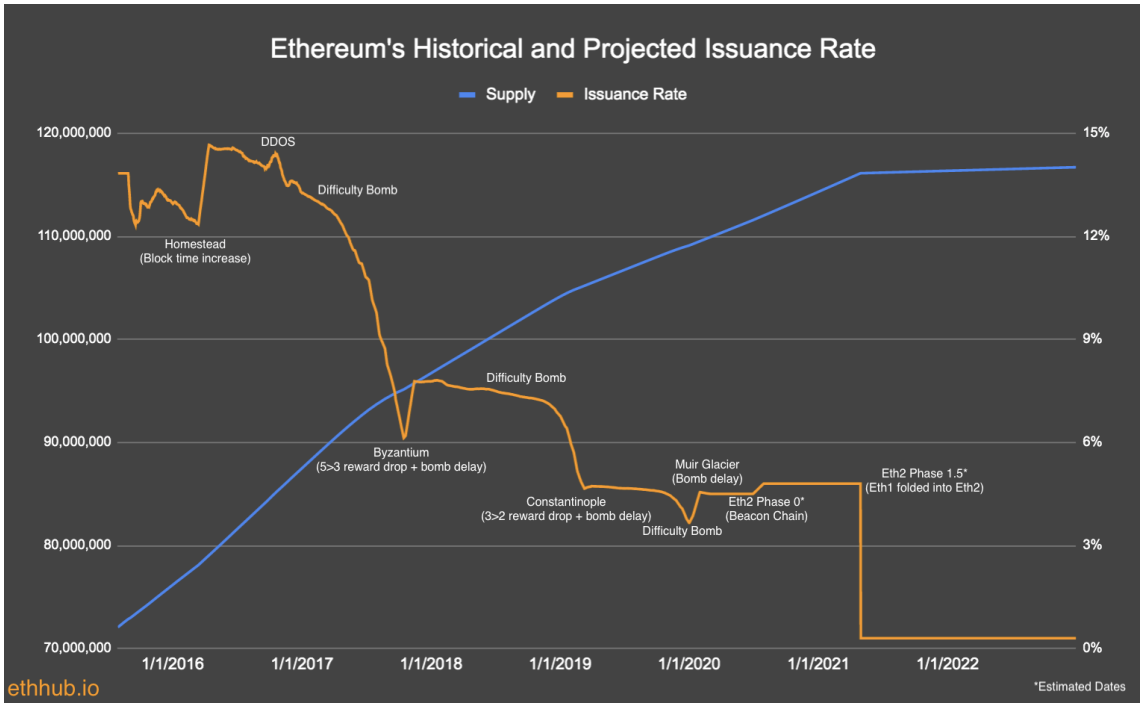


Figure 3.4: The rate of token generation has changed unpredictably over time. Rights requested

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."

3.1.1 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 while 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 hundreds of dollars to do a single transaction, though it is more normally just a few tens of dollars. 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 huge 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.

3.1.2 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 3.4. In addition a recent upgrade called EIP-1559 means that tokens are now 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. [34]. Addionally, 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. 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.

3.2 Bitcoin

The first practical blockchain was the Bitcoin network [41], some two decades after Haber et al. first described the idea [27]. It can be considered a triple entry book keeping system [21, 28], the first of it's kind, integrating a 'provable' timestamp with a transaction ledger. Some see this as the first major innovation in ledger technology since double entry was codified in Venice in fourteen seventy five[46].
It was created pseudonomously in 2009 as a direct response to the perceived mishandling of the 2008 global financial crisis, 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, with no barrier to access, and equality of opportunity to accumulate and save over long periods. 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. The "genesis block" which was hard coded at the beginning of the 'chain' contains text from The Times newpaper detailing the second bank bailout.
Satoshi Nakamoto (the name of the publishing entity) disappeared from the forums forever in 2010. Although there were some earlier experiments (hashcash, b-money etc), Bitcoin is the first viably decentralised 'cryptocurrency'; the network is used to store economic 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 $12 trillion Dollars in 2021, though Makarov et al. contest this, citing network overheads, and speculation [36]. 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 3.5.
Only around 7 transactions per second can be settled on Bitcoin. The native protocol does not scale well, and moreover this in an inherent trade-off as described by Croman et al. in their positioning paper on public blockchains [16]. 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 ever to move again [19].
Bitcoin has developed quickly, with a faster adoption than even the internet itself. It is now a mature

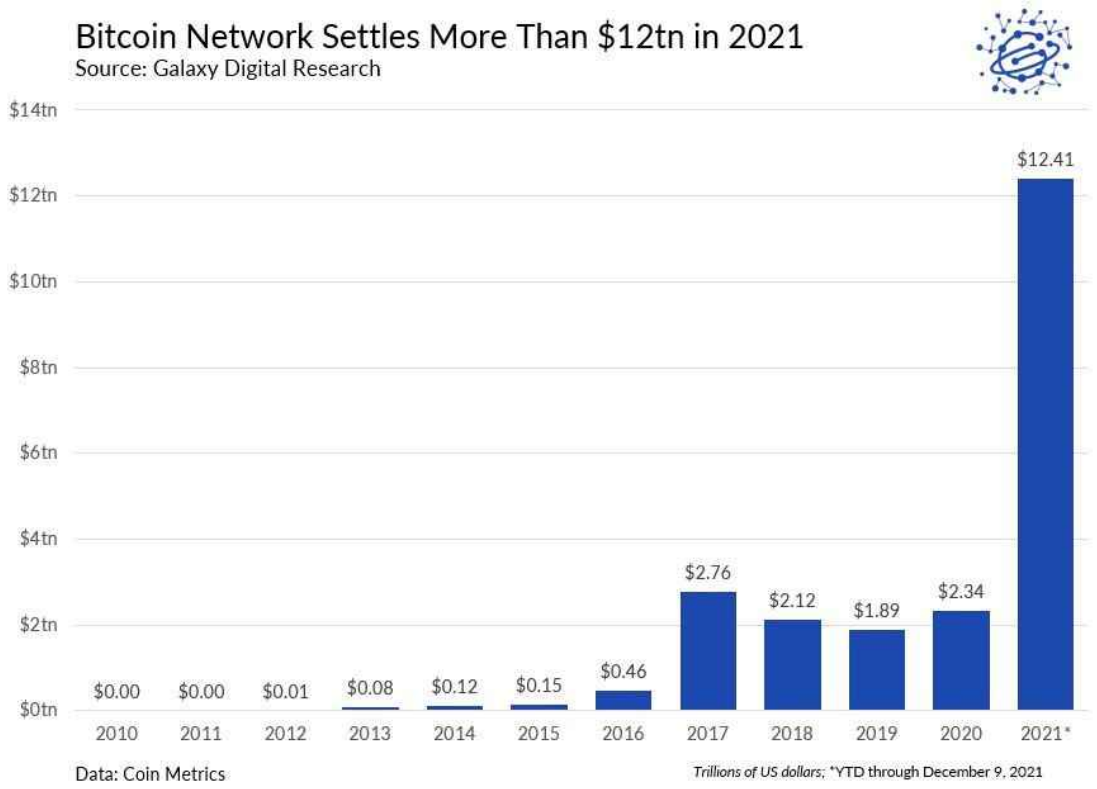


Figure 3.5: Growth in settlement value on the Bitcoin network.

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. Many city treasuries have added it to their balance sheet. The Swiss city of Lugano is launching a huge initiative alongside Tether. It is already legal tender in the country of El Salvador[1]. This will be explored more later. 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."

3.2.1 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 400 developers out of a wider 'crypto' pool of around 9000 contributors. Development and innovation continues but there is an empahasis 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 3.6.

Bitcoin core is the main historical effort, but there are alternatives (LibBitcoin in C++, BTCD in Go, and BitcoinJ in Java).

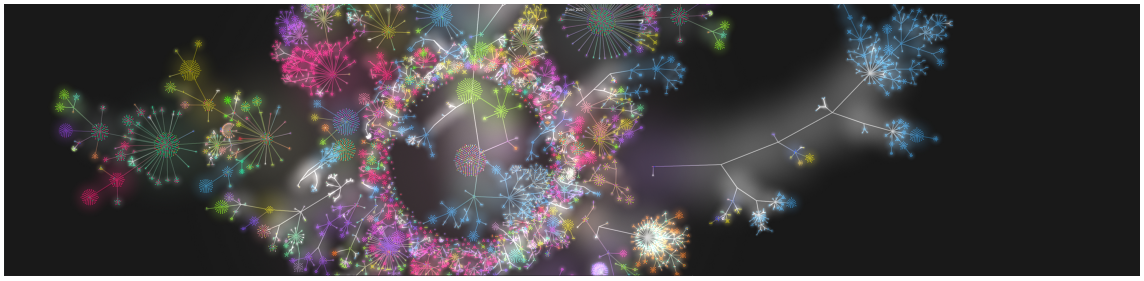


Figure 3.6: Bitpaint: Contributions to the Bitcoin ecosystem. Reused with permission.

3.2.2 What are ECDSA, addresses and UTXO's

All these technologies use the same underpinning elliptic curve cryptography, but it makes sense to unpack this here just once, and only in the context of Bitcoin, as this will be the main focus of our attention. To that end we will not consider solutions which us the "integer factorization problem". In Bitoin 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 [20]. In this 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 simplify 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 3.7 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 was as the Diffie-Hellman approach, and the security of this system is very sensitive to the randomness which is applied to the operation. ECDSA has already been replaced by the more efficient Schnorr signature method, but this will take so time for organic adoption, and ECDSA will never be deprecated.

3.2.3 Mining and Energy concerns

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 "magicnumber" resulting from a hash function, and upon finding it, they can take their pre-prepared 'block' of transactions sources 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.
Bitcoin uses a staggering amount of energy to secure the blockchain, and this has climate repercussions. 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 Adam Back's "proof of work", and is essential to the technology. The Cambridge Bitcoin Energy Consumption Index

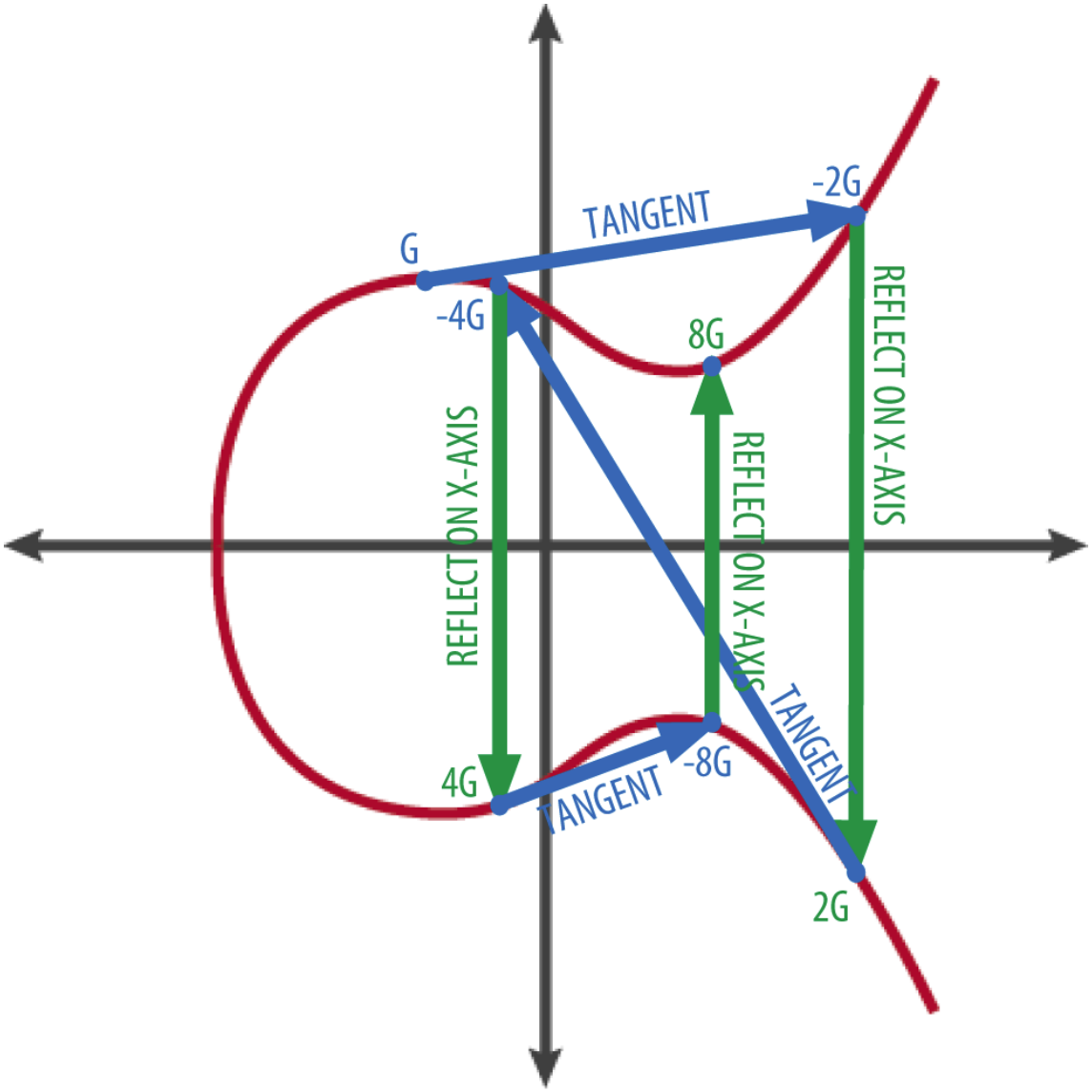


Figure 3.7: Given a start point on the curve and a number of reflection operations it's trivial to find a number at the end point, but impossible to find the number of hops from the two end points alone.


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 3.8: Intimate tie between energy and money, Henry Ford

monitors this energy usage.
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 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 as can be seen in Figure 3.8. Henry Ford proposed an intimate tie between energy and money to create a separation of powers from government.

Nic Carter newsweek

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.
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 away from 'dirty coal' as seen in Figure 3.9. Some analysts propose mitigations, or even suggest that 'ending financialisation' through use of Bitcoin may be net positive for the environment. Recently for example 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."*[4]. 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 argue that economic pressures mean that most of the 'hashrate' is generated by renewable energy[7]. Certainly 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 [3]. The most cited example of this is El Salvador's 'volcano mining' which is supporting their national power infrastructure plans. 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. Critics highlight the potential impact of mining on local energy prices[5]. The debate whether this consumption is 'worth' it is complex and rapidly evolving. Is

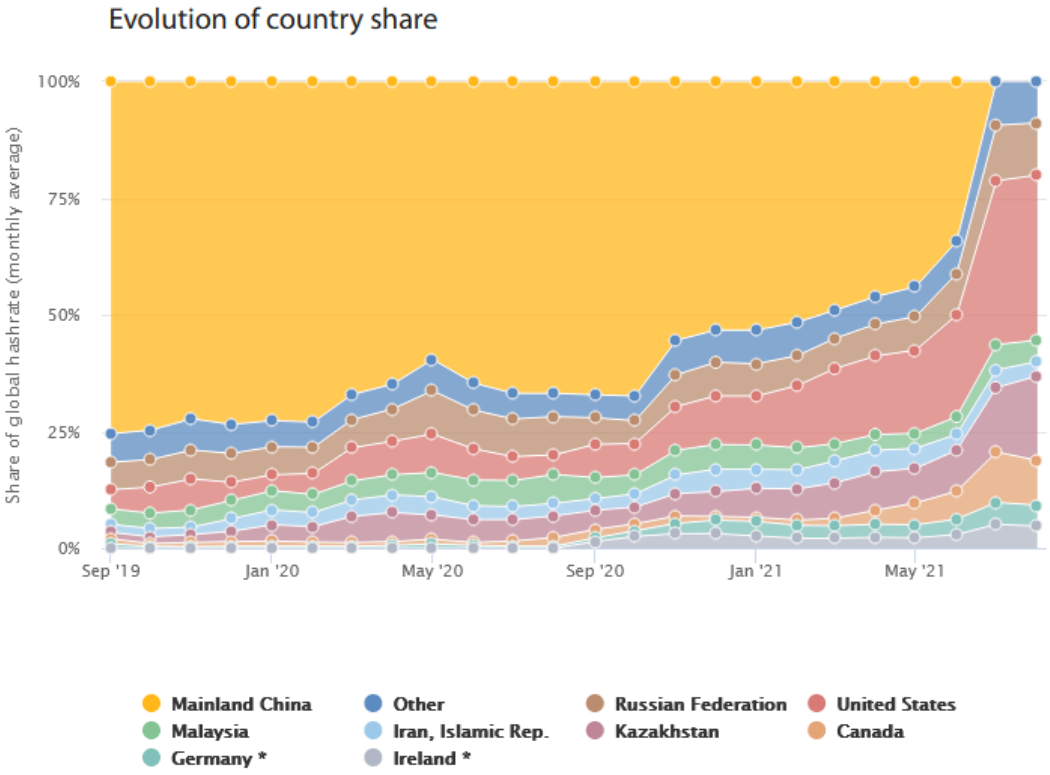


Figure 3.9: Hash rate suddenly migrates from China [Reuse rights requested]

a trillion dollar asset which potentially replaces the money utility of gold, but doesn't need to be stored under guard in vaults (Figure 3.10), 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. This book offers no firm opinion.

3.2.4 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.
- Miners, who profit from creation of new UTXOs, and receive payments for adding transactions to the chain. In return they secure the network.
- Node operators, who enforce the consensus ruleset 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 ths network from changes which might undermine their speculation and use of the tokens.

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 the following open source distributions, with the most noteworthy explained alongside their standout featureset:

- Raspiblitz offers fully opensource lightning focused functionality with a touchscreen display
- Mynode focuses on easy of use through a web interface and has many modules which users can try out.

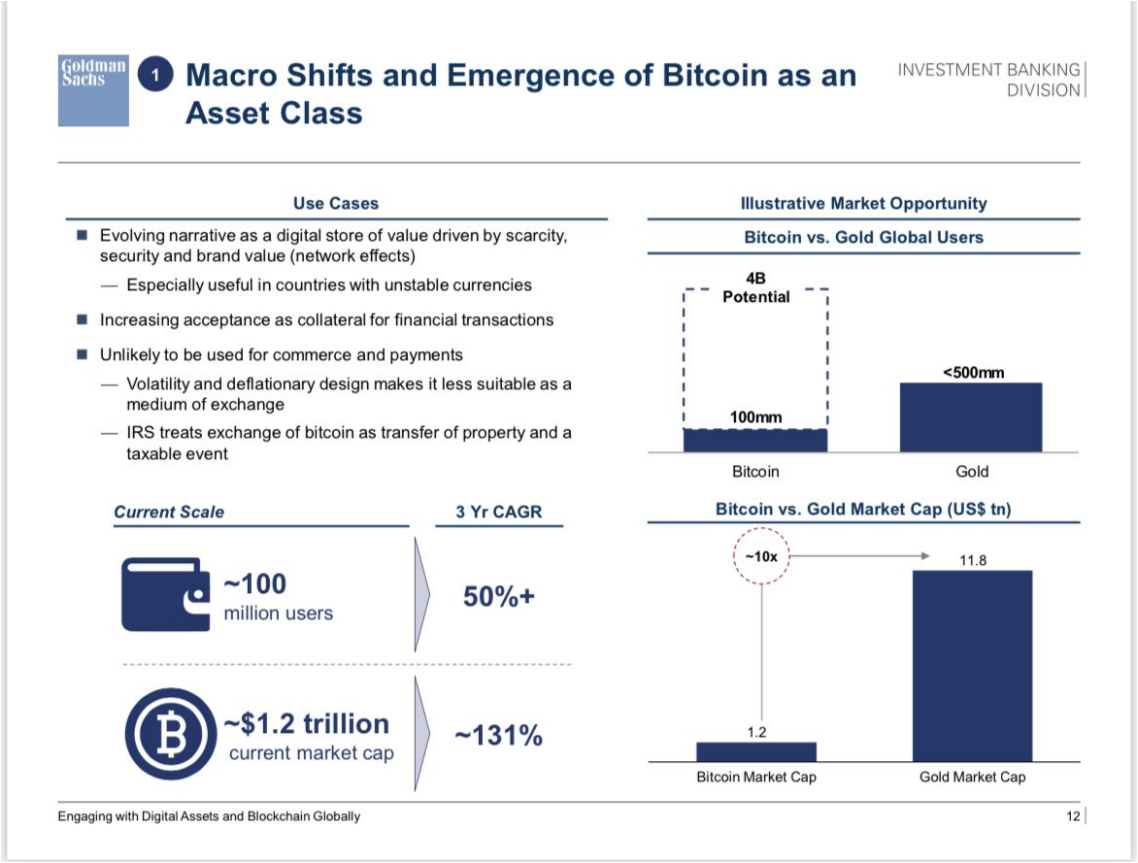


Figure 3.10: Goldman suggest growth opportunity and potential demonetisation of gold?

- 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.

Rather than using one of these distributions we plan to support a new metaverse focused suite of these tools based around the nix distribution. Consider mining the NYDIG primer for information

3.2.5 Upgrade roadmap

Taproot, schnorr signatures replace ECDSA
BIP-119

3.2.6 Risks

- 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.
- 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.
- The 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 tech 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 own their own Bitcoin address (with it's associated underpinning UTXO).

3.3 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.

3.3.1 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.
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 developer to add lightning functionality to apps and wallets. It is a useful contender for our metaverse applications. They also fund external open source development.

3.3.2 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.

check the roadmap

3.4 Lightning (Layer 2)

Lightning was a 2016 proposal by Poon and Dryja [42], and is a community driven liquidity pool which enables scaling and speed improvements for the Bitcoin network. 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 [52]. 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 3.11). The popular payment app "Cash App" integrates the technology, and 'Lightning Strike' services the USA, El Salvador, and Argentina with zero exchange and tranmission 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 main Lightning network git is the Daemon here but it's worth knowing that Lightning itself really needs access to both a Bitcoin full node, and the Tor private network layer. Both Donner Labs

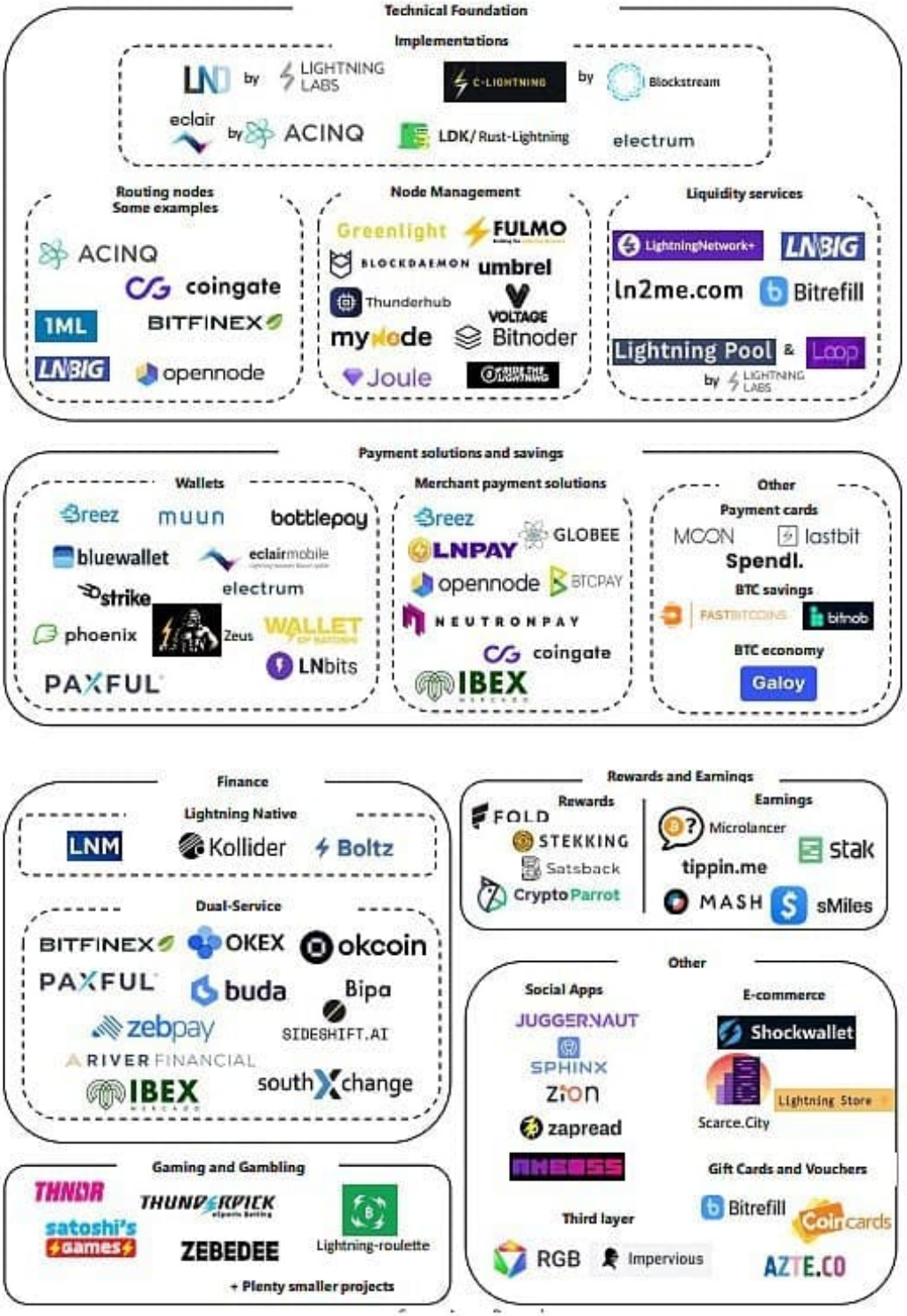


Figure 3.11: Arcane research lightning adoption overview.

and Zebedee have code packages which allow interaction with the lightning network within Unity. In all likelihood users would have to run a lightning / Bitcoin node and have their users interact with it. This would allow instantaneous transactions of Satoshis (the Bitcoin unit of account) between users. It would not resolve how to move money into Bitcoin or lightning. This could be handled through a web store (BTCPay Server). This is another overhead which would need weighing but opens the door to real value transacting at scale and with high security.
Setting up and running a lightning node is even more difficult. It is recommended to buy a third party hosted BTC / Lightning / BTCPayserver stack.

3.4.1 Micropayments

Possibly the most important affordance of the Lightning network is the concept of micropayments, 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.

3.4.2 BOLT12 and recurring payments

BOLT12 is a new and developing 'standard' which simplifies and extends the capability of the network for recurring payments.

3.4.3 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 3.12).
- 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.

3.4.4 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

Figure 3.12: Two of the many prebuilt and kit options for Lightning 'point of sale'

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.

3.4.5 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 and Juggernaut. To be clear, this is considered by some to be a misappropriation of the function of the network. Once 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.

3.5 Liquid federation (layer 2)

Liquid is part of the open source development contribution of Blockstream, the company started by Adam Back (of proof of work fame). 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 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. This is 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 C-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.

El Salvador volcano bonds stuff
launching in March 20th

3.6 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. 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 bring.

3.6.1 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
- 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 future version of the Lightning network, significantly lowering the barrier to entry for this whole technology. This is slated for release later in the year.
- RGB22 may provide a route to identity proofs. This is covered in detail later.

3.6.2 Synonym & Omnibolt

Omnibolt github

3.6.3 DLCFD

Discrete log contracts are a form of externally arbitrated smart contract. Work is being done to extend this primitive to lightning.

Marty Bent “This particular contract allows (currently) one party to lock in a stable amount of USD value in BTC to avoid bitcoin price volatility while their counterpart takes a long position on BTC. As bitcoin’s price moves, the contract allocates sats to one party to make sure the individual who is engaged in the contract to lock in a USD value of bitcoin is doing just that. If the price of bitcoin goes up, sats are allocated to the individual who is taking the long position. If the price of bitcoin goes down, sats are allocated to the party looking to lock in a stable USD value. All of this happens on the Bitcoin blockchain and the Lightning Network. No obscure governance token, DAO, or central third party holding USD in a bank account necessary. All that is needed are sats and a willing counter-party.”

3.7 Bitcoin adjacent chains

In order of preference for functionality for Metaverse the following framework can be adopted. BitcoinL2>BitcoinL1>LiquidL2>Adjacentchains>Altchains

The reasons are:

- Free and open source network
- Network effect
- Security model
- Development community
- Transaction speed

This section is in early development.

3.7.1 Stacks and STX

“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.

3.7.1.1 Citycoins

These are actually slightly interesting.

3.7.2 Sovryn and RSK

Ingamar | Top of the Block: Lightning <> Rootstock Bridge for lnBTC <> Stablecoin swaps

Exchange
Repo 1
Repo 2
Repo 3
Bridge aggregator
Rest API docs

3.7.3 Sidechains

3.7.4 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 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.

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

3.7.5 Drivechain

3.7.6 Softchains

3.7.7 Statechains

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. They are all hypothetical with the exception of sidechains.

3.8 Other chains and networks

It's useful to make some 'honourable mentions' of other options as this technology is moving so fast.

Figure 3.13 shows the allocations of proportions of value within different chains.

3.8.1 Layer 1 chains

- 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 .
- Polkadot There is much hype within the invested public blockchain community about "cross-chain" protocols which can 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.
- Luna is a relatively new stablecoin offering with DeFi built in. It is currently in ascendance and seems to have a stable and useful underpinning, but is far too new to judge with any certainty.
- Avalanche AVAX is a newer, 'faster' and more eco friendly DeFi ecosystem which promises

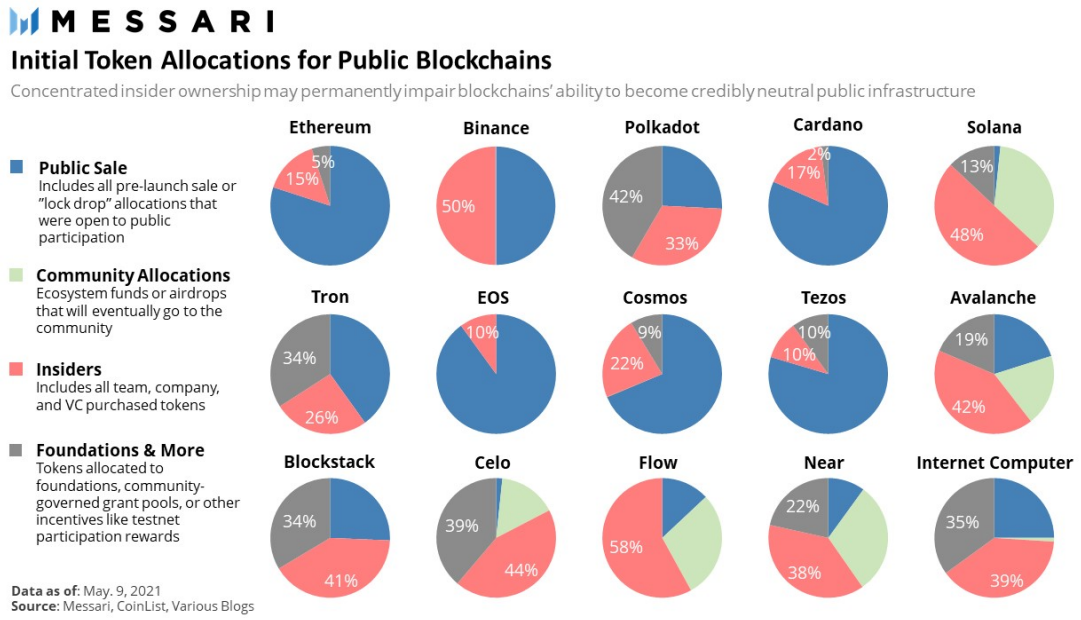


Figure 3.13: Allocations given at the beginning of public blockchain, by Messari.

returns within it's own framework of permissionless money. It is one of the relative success stories of the DeFi narrative. It's unclear what the value proposition, and sustainability of this token actually are.

- Tezos is an 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 uncertainly 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 the '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 to discuss in the same basket as the other ideas.
- 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 assertion that immutable global ledgers of real work asset tracking somehow protect from fraudulent behaviour. It's perhaps useful, but mainly in a highly automated industry 4.0 environment of minimal human interaction. it's also unclear what is added
- 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 nontheless 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 warchest of bitcoin which they still hold. The onus is on them to deliver some kind of product, and with a multi billion dollar investment in their own promises they can likely deliver something.

3.8.2 Crosschains

RUNE? lots of hacks and unmanageable complex logic. Who is moving across chains anyway?

3.8.3 Decentralised data

Nick Grossman blog piece on adversarial open data might inform how we should specify the open data layer for the metaverse. Something about Filecoin? ARWeave? IPFS etc

3.9 Risks and mitigations

3.9.1 ESG

3.9.2 Legislative

The partial regulatory capture of these technologies, and the potential for 'jurisdictional arbitrage', 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.

3.9.3 Crime and santion busting

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.

4. Money in the real world

It is necessary here to briefly examine what money actually is. 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. Indeed this has long been one of the assertions of the community and it finds favour in law. 'Money' though is a far more slippery concept to grasp. It seems very likely that Bitcoin is evolving as a 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

It is hard to find a universally accepted definition of what money is. The best approach is 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" [18].
Stroukal examines Bitcoins' likely value as a money from an Austrian economics perspective and identifies "portability, storability, divisibility, recognizability, homogeneity and scarcity" [49].
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.

4.2 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 [24, 25]. 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 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.
Strike is a possible the most interesting 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 application 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, 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 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. The caveat here 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.

It seems like the primary intersection Current state of the art Libre, Mark Carney synthetic hedgemonic currency, and Keynes baskets

USDF bank issued private dollar stablecoin

Paypal

Whatsapp, Novi, USDP etc Crypto dollarisaton (myanmar) USDC on Bitcoin?

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 (CDBC). CDBCs would likely not exist without the 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 currencies. This text from the thinktank VoxEU highlights the pressure on central banks 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."

CDBCs are wholly digital representations of national currencies, and as such are centralised database entries, endorsed and potentially issued by national governments. It is a rapidly evolving space, and many nations are now scrambling to catch up.

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. The debt is 'destroyed' on the balance sheet to remove currency through the reverse mechanism. They also facilitate government debt [22], and work (theoretically) outside of political control to adjust interest rates, in order to manage growth and flows of money.

Many things which cannot be done with traditional nation state money systems are possible with CDBCs, 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 [8, 12].
- 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 CDBCs 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." [43]
- 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 CDBC 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."
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 CDBC. It is far more likely that a blend of stablecoins, private bank issued digital currency (with a yield incentive) and some limited CDBC, 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.

US CDBC whitepaper

4.4 Bitcoin as a money

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. 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.
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

Mallers further identifies the attributes of the ideal global money.

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

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. 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[38].
"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

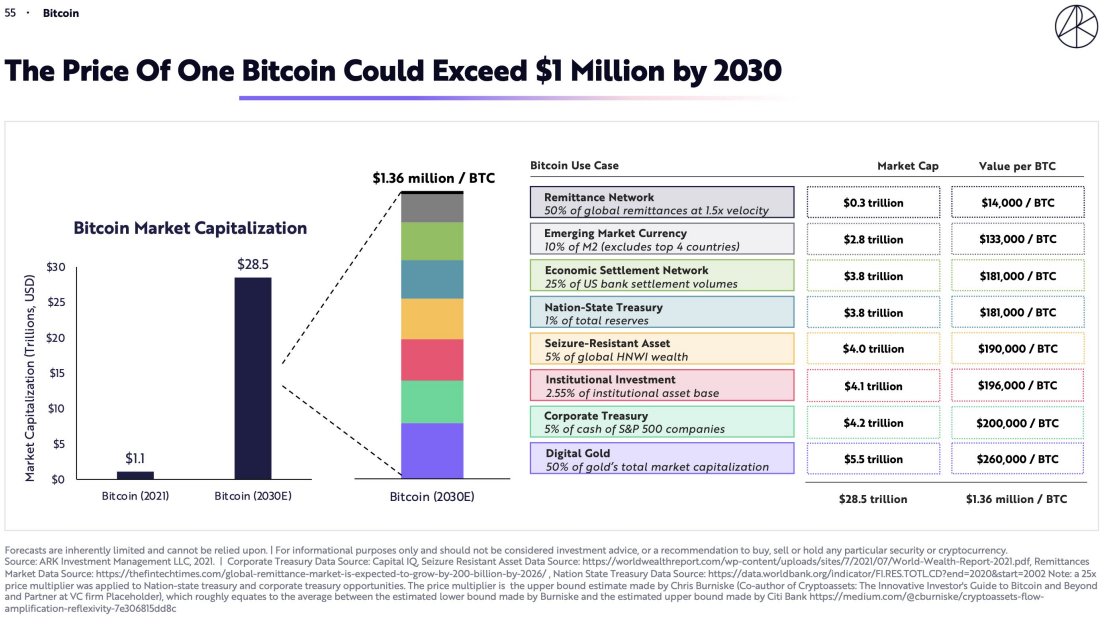


Figure 4.1: Potential market exposure to Bitcoin as a money

existed."

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 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."

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"*

The 2022 ARK Big Ideas report again provides some useful market insight. The 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 4.1.

Bitcoin is only a viable money when viewed in the layers described in this book. The base chain layer is the ultimate store of secure 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.

4.4.1 Hyperbitcoinization

Hyperbitcoinization is a term coined in 2014 by Daniel Krawisz [32]. 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 backed by a game theoretic analysis of both Bitcoin and current

macro economics. Fulgur Ventures (a venture capital firm) provide a blog post series about the route this might take. It's beyond the scope of this paper to look at the implications of this possibility, but they are clearly significant if true.

4.5 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 few years. It enables trading of value, loans, and interest (yield) without onerous KYC.

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. In addition access to DeFi is 'usually' through Web2.0 centralised portals (websites) which are just as vulnerable to legal takedown orders and any other centralised technology.

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.

5. Distributed Autonomous Organisations

A DAO is an organistion 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.
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

5.1 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.”

5.2 Risks

6. Distributed Self Sovereign Identity

This section need to point out that DID/SSI is broken, ION is untested, and everyone's kinda given up. Webs of trust are viable so this means Nostr or Slashtags. Maybe LNURL-Auth can do it.

This is where an external contributor can add information about DID and SSI Distributed self sovereign identity has a great elevator pitch. 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.

6.1 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 a 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, 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.

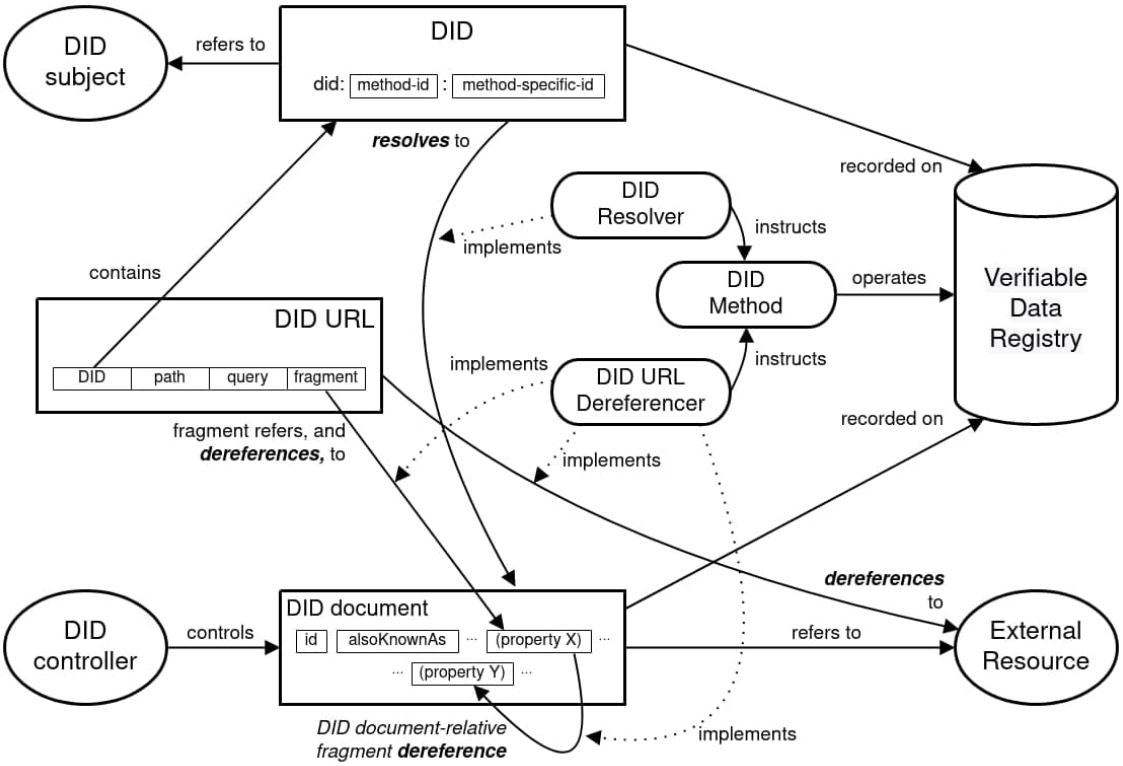


Figure 6.1: Part of the DID SSI specs

6.2 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 6.1.

.

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 [35] 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?

6.2.0.1 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.

6.2.0.2 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 contact the minimum about of information to accomplish the specific task required of them.

6.3 Newer Technologies

6.3.1 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.

6.3.2 LNURL-Auth

6.3.3 Sovrin

Sovrin foundation are established global players in distributed identity and we wish to apply to join their federation of credential issuers.

6.3.4 Keri

6.3.5 Atala Prism

6.3.6 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.

6.3.7 Atala Prism (ADA Ecosystem)

This Medium post lists the pre-requisites required for interaction with Eth within Unity. At this stage this hasn't been expanded out. It's based around the .NET 'nethereum' library which can be found on their github.

6.4 Risks & Challenges?

Classic DID/SSI risks fragmentations In all DID 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 user simple, and only caring about 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 off of their digital interactions with a trust metric.

7. Non Fungible Tokens

Nonfungible tokens allow digital and new media artists to connect with audiences without gatekeepers. This is an important supporting innovation for something so recently recognised as valuable art in it's own right. 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. This is a compounding, and disrupting paradigm change.

Users of NFT markets have injected around $30 billion into the tokens during 2021. While it is likely that there is currently a speculative bubble, it seems certain that the technology is here to stay. Samsung for instance have announced that their TVs will support not only display of NFTs with artist defined settings in the metadata, but also an integrated marketplace for browsing and purchasing.

Notable examples Mega Mutant Serum.

Wikipedia list

Beeple scam

Peter Thiel, the billionaire venture capitalist who founded PayPal has invested in expanded NTF use cases. The first is 'Royal' which is experimentally selling selling limited NFT tokens which contractually entitle the holder to a portion of music artist royalties. The other is a political funding NFT from Blake Masters to support his senate ambitions.

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.

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.

7.1 Energy concerns

It is under discussed within the community that 'minting' non fungible tokens, predominantly on Ethereum, is energy wasteful, on an already energy inefficient platform. As a random example this single collector of a few images accounts for nearly 10 kilotonnes of carbon emissions. This is a subtly different problem to the security of the Bitdooin economic network in that these tokens are clealy non fungible, so cannot be reused again and again in order to reduce the unit environmental impact.

7.2 NFTs and games

7.3 Is any of this useful?

7.4 User stories / behaviours

- As a user I want to select a digital asset I find in a metaverse and then be offered an option to purchase the asset so I can look at it in my own spaces.
- As a user I want to click on a digital asset I find in a metaverse and be given the opportunity to buy it as a rare digital representation so that only I and a few others are provably certified to own.
- As a metaverse 'land' holder (stakeholder) I would like to reward winners of competitions with real money or digital assets to foster and gamify the system
- As a user I would like to interact with a virtual marketplace where I could swap and trade digital assets with other users so that I continue to feel engaged.
- As a user I would like to create content so I can take it to metaverse locations and monetise it.

7.5 Comparing the technologies

Figure 7.1 on the next page compares the technologies discussed so far in the context of the behaviours in section 8.6.
Looking at these row by row it can be seen that:

- Bitcoin layer 1 is too slow. Additionally the technical challenge of interacting with the network are considerable, and the fees are both high and likely to rise.
- Ethereum ERC721 non fungible tokens might be a possibility for supporting limited edition digital assets. A web interface could be built on cloud servers to handle the shop and back end commitments to the Ethereum network. While fully committed transactions would take a few minutes to process the shop itself could inform the users immediately then email out a certificate of ownership. It would be possible to trade these items on other platforms, and conceivably within an app. Prizes (digital assets) could be issued to users for competition activity. The system would be expensive to use, the fees might vary wildly, and the ecological costs might be enormous. Batching transactions could overcome this, but that would rely on substantial take-up of the service, and management overhead.
- Building and issuing and Ethereum based token, in an ICO process or similar seems a disproportionate amount of investment and would be expensive to use.
- A custom private blockchain offers no advantages over a database. It is a difficult thing to implement, but would have better performance and use cost to the users.
- BTC pay server is an interesting open source project which allows companies to host a simple lightning / BTC web shop. It's not clear what the use case is here, but it is well engineered and scalable and should be born in mind when thinking about the other problems and systems.
- Lightning network has open source connectivity into Unity, works well with QR codes, is fast, and has low transaction latency. The only issue is that it offers nothing but marketing hype over and above more traditional digital point of sale layers, and is more difficult to connect to money rails in the UK.
- New layer 3 solutions like RGB, stacks, or Synonym might allow cheap and fast in

7.6 User stories / behaviours

- As a user I want to.
- As a user I want to.

- As a user I want to.

7.7 Comparing the technologies

Figure 7.1 on the next page compares the technologies discussed so far in the context of the behaviours in section 8.6.
Looking at these row by row it can be seen that:

- Bitcoin is too slow. Additionally the technical challenge of interacting with the network are considerable, and the fees are both high and rising.
- Ethereum ERC721 non fungible tokens might be a possibility for supporting limited edition digital asset sales. A web interface could be built on cloud servers to handle the shop and back end commitments to the Ethereum network. While fully committed transactions would take a few minutes to process the shop itself could inform the users immediately then email out a certificate of ownership. It would be possible to trade these items on other platforms, and conceivable within the app. Prizes (digital assets) could be issued to users for competition activity. The system would be expensive to use, the fees might vary wildly, and the ecological costs might be enormous. Batching transactions could overcome this, but that would rely on substantial take-up of the service, and management overhead.
- Building and issuing and Ethereum based token, in an ICO process or similar seems a disproportionate amount of investment and would be expensive to use.
- A custom private blockchain offers no advantages over a database. It is a difficult thing to implement, but would have better performance and use cost to the users.
- BTC pay server is an interesting open source project which allows companies to host a simple lightning / BTC web shop. It's not clear what the use case is here, but it is well engineered and scalable and should be born in mind when thinking about the other problems and systems.
- Lightning network has open source connectivity into Unity, works well with QR codes, is fast, and has low transaction latency. The only issue is that it offers nothing but marketing hype over and above more traditional digital point of sale layers, and is more difficult to connect to money rails in the UK.
- Coloured coins would allow all of the desirable functionality, but it would be a substantial development challenge, using old open source code, and have high use fees.
- RGB MyCitadel stack seems highly appropriate and is open source but is in development and will not be available until later in the year.

7.8 What are the options

ETH, SOL, ADA, STX, RGB, Liquid?, RSK, so many others, this is gonna be exhausting to write about.

7.9 Risks

7.10 Why choose bitcoin again

because it's the true opensource money option, the cost / barrier to entry is far lower than ethereum, and with new technology such as NFT integration directly with DIBA on RGB this integrates.

	Likely dev time	Cost of Use	Speed of Use	Energy Cost	Open source	Bank connect	Buying things	Prizes	Trading Peer 2 Peer	Arbi to issu
Bitcoin	N/A	~£10 per use	~H	High	Yes	Maybe (Strike)	Yes	Yes	Maybe	Y
Eth ERC721	N/A	~£10 per use	Mins	Very High	Yes	No	No	Yes	Maybe	Y
Eth token	Weeks Months	~£10 per use	Many Mins	High	Maybe	No	Maybe	Yes	Yes	Y
Custom chain	Months	Very low	Secs	Moderte	Maybe	Maybe	Yes	Yes	Yes	Y
BTC pay server + LND	Days but operational overheads	~£10 per use	Secs	Lower	Yes	Yes	Yes	Yes	No	N
BTC L2 and L3	Months	Very Low	Secs	Low	Some	Maybe	Yes	Yes	Yes	N
Colour coins	Months	Very Low	Secs	High	Maybe	Maybe	Yes	Yes	Yes	Ma

Table 7.1: This table is basically broken and out of date and will be sorted out soon!

8. Metaverses

8.1 History and market need

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 [39].
There were clear precursors such as VRML in the 1990's which laid much of the groundwork for 3D content over networked computers. The author used to create commercial 3D scenes on Silicon Graphics systems back in the late 90s.
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. The concept of the Metaverse is extremely plastic at this time (Figure 8.1). This section will attempt to frame the context, and explain the increasingly polarised options looking forward.

Both Second Life and more recently the game Fortnite can be seen as precursors. Second Life should rightly be viewed as the first serious attempt at a metaverse, and was being described as such by users as early as 2002/2003. It broke through into academic research and several Universities

Figure 8.1: Elon Musk agrees with this on Twitter

bought ‘digital land’ and started talking about using the platform for education [**emp2006putting**, 31, 47, 48]. Businesses began to develop and showcase virtual products. Interest in the platform waned by 2010, although the platform is still operational and under development with around 40k median concurrent users. Surprisingly this is similar to the 2007 peak use, but this is in the context of other platforms now boasting considerably faster growth (more later).
Epic games Tim Sweeney attaching the word metaverse to social events within fortnite in 2017.
“You’re seeing the beginning components of the Metaverse coming together now..” - Tim Sweeney
Clearly he ignored the extensive work of Second Life here, but fortnite demonstrated a new level of social engagement boasting millions of concurrent users in a single space for major events in the game. Most interestingly events outside of the game logic emerged, with concerts drawing over 10M users on occasion. This has kickstarted a new round of academic interest in the phenomenon [37]. A new era of microtransactions for in game assets has begun, thought this is constrained to the walled economic garden within Epic’s servers.

8.2 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. The second order hype is likely a speculative play by major companies on the future of the internet. There has been a reactive pushback against this by the wider tech community who are concerns about 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.
Meta,Disney plus, Sportswear manufacturers

Can enough be done to prevent abuse?

It seems like there are four major interpretations of the word.

Facebook have recently rebranding their parent company as ‘Meta’ and they are aggressively promoting “The Metaverse” as a shared social VR space, chiefly of their design. 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.
The Grayscale investment trust 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.

8.2.1 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?

8.3 Digital Land Metaverses

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.

8.3.1 Legacy Web2

8.3.1.1 Secondlife

8.3.1.2 Roblox

8.3.1.3 Minecraft

8.3.1.4 Fortnite

8.3.2 The new stuff

8.3.2.1 Decentraland

JPMorgan Chase, the investmemt bank, ahas just opened a ‘lounge’ in the Decentraland metaverse. This coincided with a major report on the potential opportunities.

8.3.2.2 Sonmiumspace

8.3.2.3 The Sandbox

8.4 Global enterprise perspective

Meta(Facebook)

Nvidia Omniverse is free for creators, Unity etc

Microsoft have just bought Activision / Blizzard for around seventy billion dollars. This is have 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.

8.5 NFT as metaverse narrative

Within the NFT community it is normalised to refer to ownership of digital tokens as participation in a metaverse. This CNBC article highlights the confusion, as this major news outlet refers to Walmart prepares to offer NFTs” as an entry “into the metaverse”.

8.6 MMORG games and NFTs

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 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.

- As a user I want to select a digital asset I find in the AR/VR world and then be offered an option to purchase the asset so I can look at it in my own spaces.
- As a user I want to click on a digital asset I find in the AR app and be given the opportunity to buy it as a rare digital representation so that only I and a few others are provably certified to own.
- As a user I would like to transfer economic value to people and entities I meet in the metaverse such that it is agreed by all parties quickly that value has been provably transferred.
- As a user I would like to access an online marketplace in the metaverse where I swap and trade digital assets with other users so that I continue to feel engaged.
- As a user I would like to create content (inside or outside of the metaverse) so I can take it to metaverse and monetise it.
- As a content creator or influencer I would like to engage with live audiences within the metaverse, and moneytise my opinions and knowledge in real-time. I would like to have a way to split this money with co-collaborators in real time.

8.7 Crypto metaverses

Report on Axie Infinity

Pavia Metaverse Probably the best example in the market at this time with connecting users with one another through blockchain is Satoshis Games 'Litenite'. Litenite is a 'battle royale' game which allows users to earn Satoshis through the Lightning network.
Similarly, and potentially more significantly, Zebedee have brought Lightning based micropayments

to Counter Strike, which adds a financial layer directly to eSport, itself a multi billion pound global industry.
The Zebedee model is interesting in that they provide simple onboarding, and management solutions, for gaming and metaverse application developers. There is doubtless an opportunity to utilise their business model in the proposed stacks in the paper, but it would be at odds with the free and open source product methodology in this paper. Their CTO said the following in a recent podcast:
"We all had very similar ideas around being able to put Lightning network capabilities into games. You're essentially putting real value inside of the game. So whether it's a point inside of the game or as a real end game economy, as a game developer, you don't have to worry about the mechanics around it.
You can use a real life currency: the money that exists in the world and that value carries regardless of which game you're in, regardless if you're in the real world or inside of a virtual world, like a game. We just think that vision is just sort of opening. Now there's so much more, if you extrapolate it into the Meatverse we would love for Zebedee to be a big platform provider and enabler for a lot of these."
Spells of Genesis is a long running card RPG trading game on mobiles which allows "ownership" of items and cards through non-fungible token ecosystems.
There are also hundreds of casinos which operate within and even on blockchain networks. These feel out of scope as they are a different and somewhat regulated offering.

8.8 Social VR software options

In considering the needs of business to business and business to client social VR is it useful to compare software platforms:

8.8.1 Second Life

Notable because it's the original and has a decently mature marketplace.

8.8.2 Spatial

- 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

8.8.3 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?

8.8.4 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

8.8.5 Mozilla Hubs

- 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

8.8.6 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

8.8.7 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

8.8.8 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

8.8.9 VRChat

8.8.10 NEOSVR

Notable becasue it's trying to integrate crypto marketplaces

8.8.11 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 changed in the underling business except Zuckerbergs well publicised shift to supporting a money losing gamble on the Metaverse. It is by no means that clear 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.

8.8.12 Vircadia

We have chosen Vircadia as our development platform for this investigation is it's a community supported free and open source project with some support for economic interaction.

8.8.13 WebXR/WebGL/WebGPU

8.8.13.1 Playcanvas

Monetisation of WebXR Playcanvas - Telefonica

8.8.14 Integration with web and game engines

(other integrations?)

8.9 User stories

8.10 Recommendations for value transfer

There are many claims about what blochchain technologies can enable. In the tens of thousands of attempts at utility over the last decade there are surprisingly few chains able to claim any value at all, and those that can often have significant problems in other areas. It is not the intention of this analysis to poke at problems. The primary use case within the context of a shared social space (metavserse) is low friction transmission of value. Remember that interlocutors and entities might have globally different physical locations outside of the real world. What is needed is instant "settlement" of digital bearer instruments within the context of the digital environement. This is fortunately what Bitcoin was designed to do. Additionally it is highly possible that exchange of

digital goods (art and objects and provable services) will be required. This is also in scope within this document.

8.11 Bitcoin market gap

Nobody is currently deploying the discussed technologies purely on Bitcoin because it's slower evolution is still catching up. This is a market gap and the following section shows how this might be done.

8.11.1 Money

8.11.2 Identity proofs

8.11.3 Digital object tracking

8.11.4 Object transfer and trading

8.12 Risks

Online regulations still apply

9. Hardware and software choices to support this

We propose that the software be deployable into a server based virtual network running on a single system. Our hardware recommendation to run a balanced selection of elements is a quad core 16GB system with two 1TB SSD drives. The system diagram can be seen in Figure 9.1.

9.1 Networking layer

9.1.1 Proxmox

Proxmox open source server virtualisation allows the deployment of several virtual machines within a hardware system. Each of these VMs can have a different balance of performance, ease of use, and security. The VMs are given only the access they need to perform the task which they are specialised for. This improves overall security. Resilience is improved since elements of the cluster can be shutdown, reinstanced, and upgraded, without impacting the whole. Snapshots and backups are simplified.

9.1.2 VyOS firewall

VyOS firewall is a Proxmox aware threat management gateway and firewall which allows more nuanced interfacing with corporate systems, while maximising the security of the VM network which sits behind it i the virtual cluster.

9.1.3 Privacy aspects and using TOR etc

Currently some compromises with privacy may be necessary. Power users vs standard users. KYC/AML. tor nodes

9.2 Bitcoin value management stack

9.2.1 Bitcoin Core on NixOS

9.2.2 Electrum server

Options on the Blockstream website

Figure 9.1: Proposed deployment of the software within the VMs on a single hardware system.

9.2.3 C-Lightning and CLBoss

9.2.4 LNBits with RGB and metaverse plugin

9.2.5 Backup & Watchtower

9.2.6 Object and media tracking: RGB

The world database in the shared rooms in the metaverse is the global object master, with RGB client side validation inheriting and validating against these objects.

9.3 Identity

9.3.1 nostr

User authentication and sideband communication will be through nostr. This allows completely private end to end encrypted chat sessions between participants.

9.4 Metaverse

9.4.1 Vircadia

9.4.2 Wolvic

"The goal of the Wolvic project is to create a full-featured browser exclusively for standalone AR and VR headsets."
Wolvic is a continuation of the now defunct Firefox Reality Browser project. It is open source.

9.4.3 WebM

Free open source web video player

9.5 Messengers and boards

9.5.1 Nostr

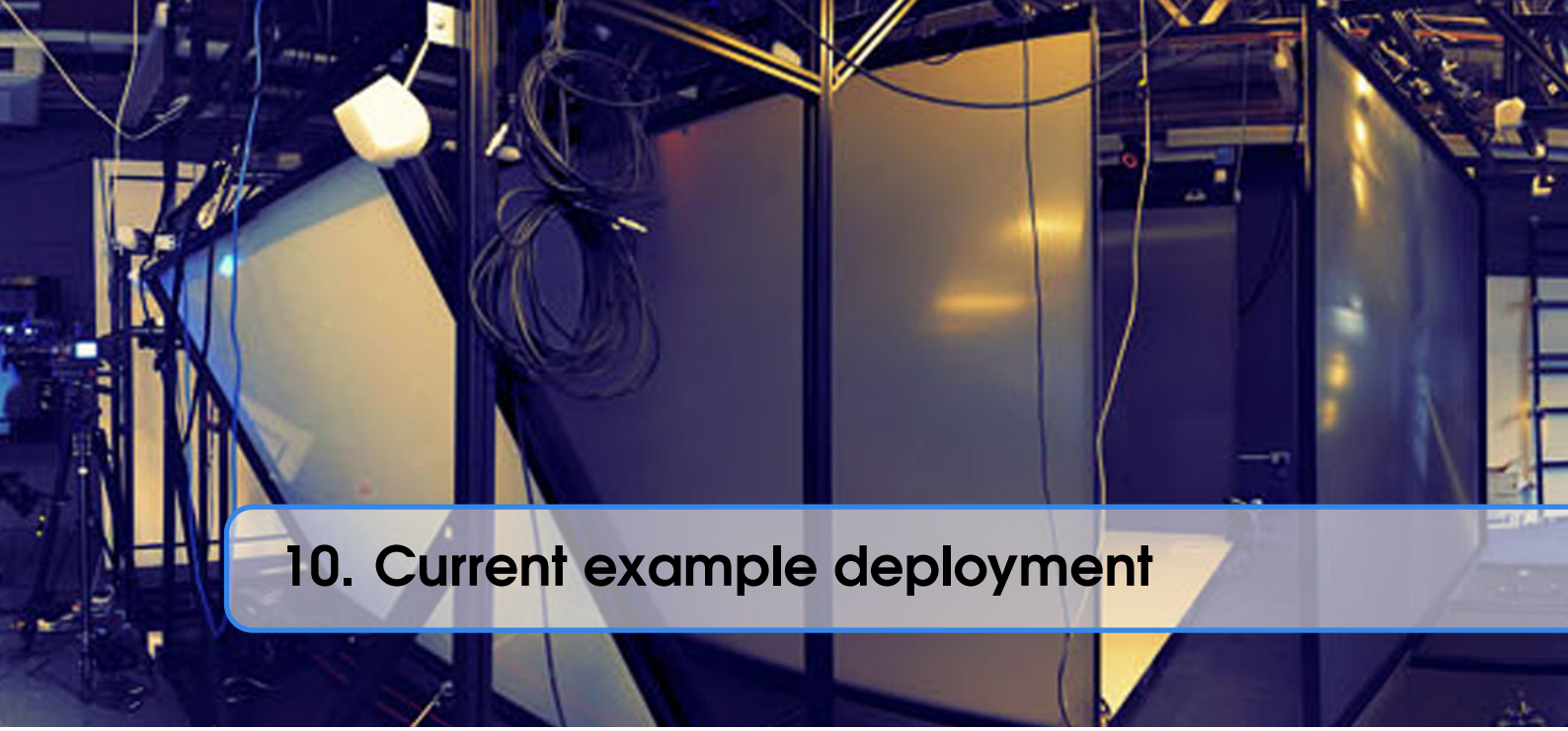
9.5.2 Cyperpost

Cyperpost is a social platform that uses ecdsa keys for e2ee. It's private first so no plain text on servers so no scope for censorship so it's okay to be centralized. All accounts are made with a single ID pubkey derived from a social Mnemonic, so you maintain uniform ID on all platforms.

9.5.3 Matrix

Matrix is the main self hosted solution for chat and also uses ecdsa keys.

9.6 Addressing identified risks



10. Current example deployment

10.1 GitHub

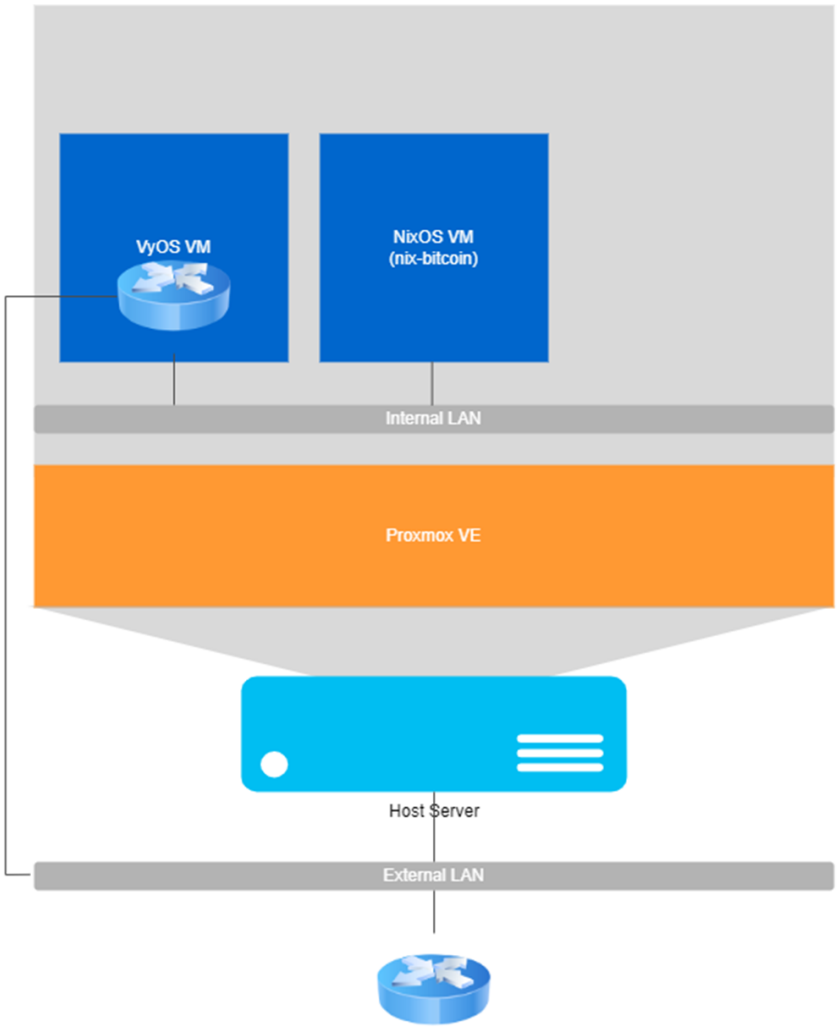
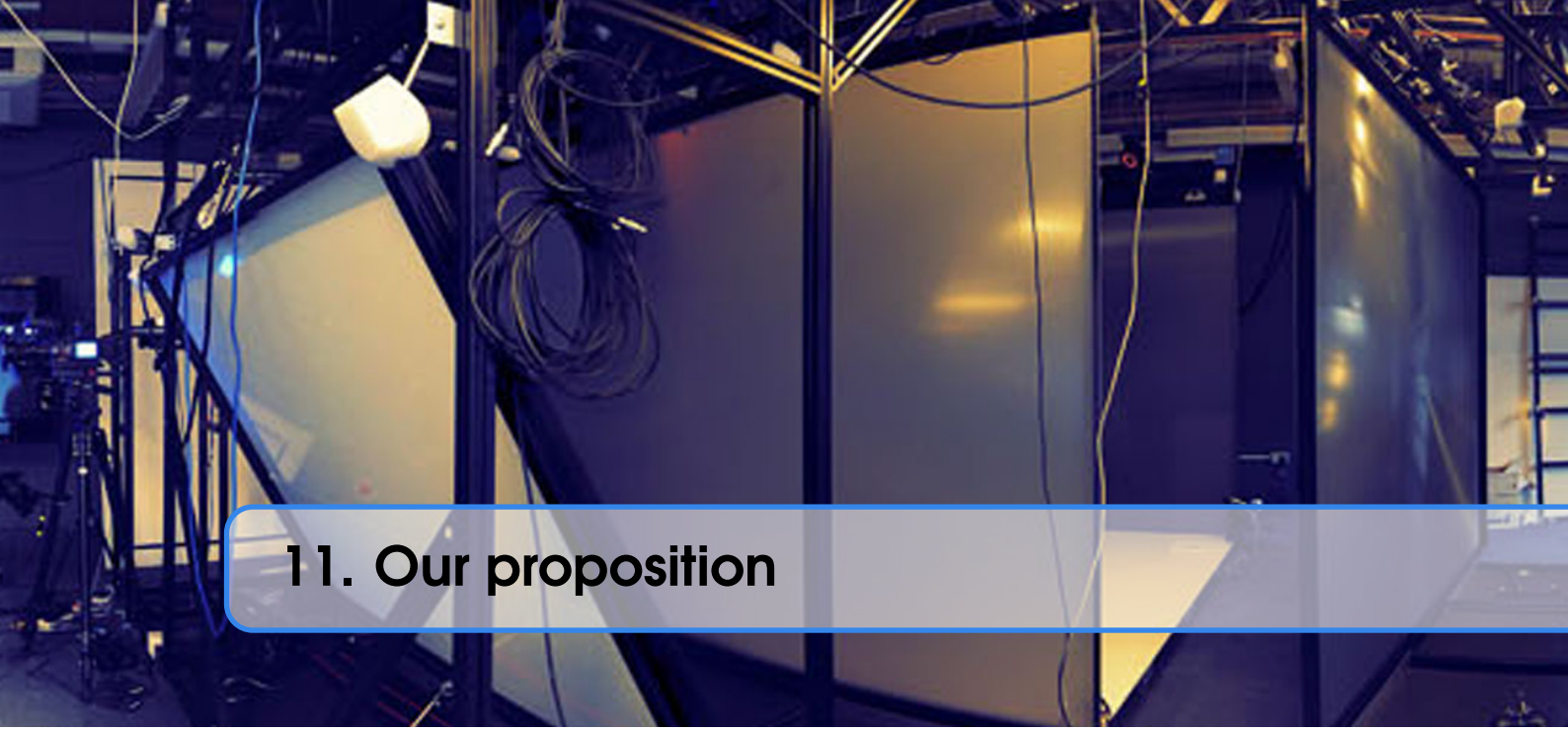


Figure 10.1: Current diagram of the proxmox as seen on the github.



11. 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.

11.1 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
  - 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
- 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

11.1.1 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 11.2.
- 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.

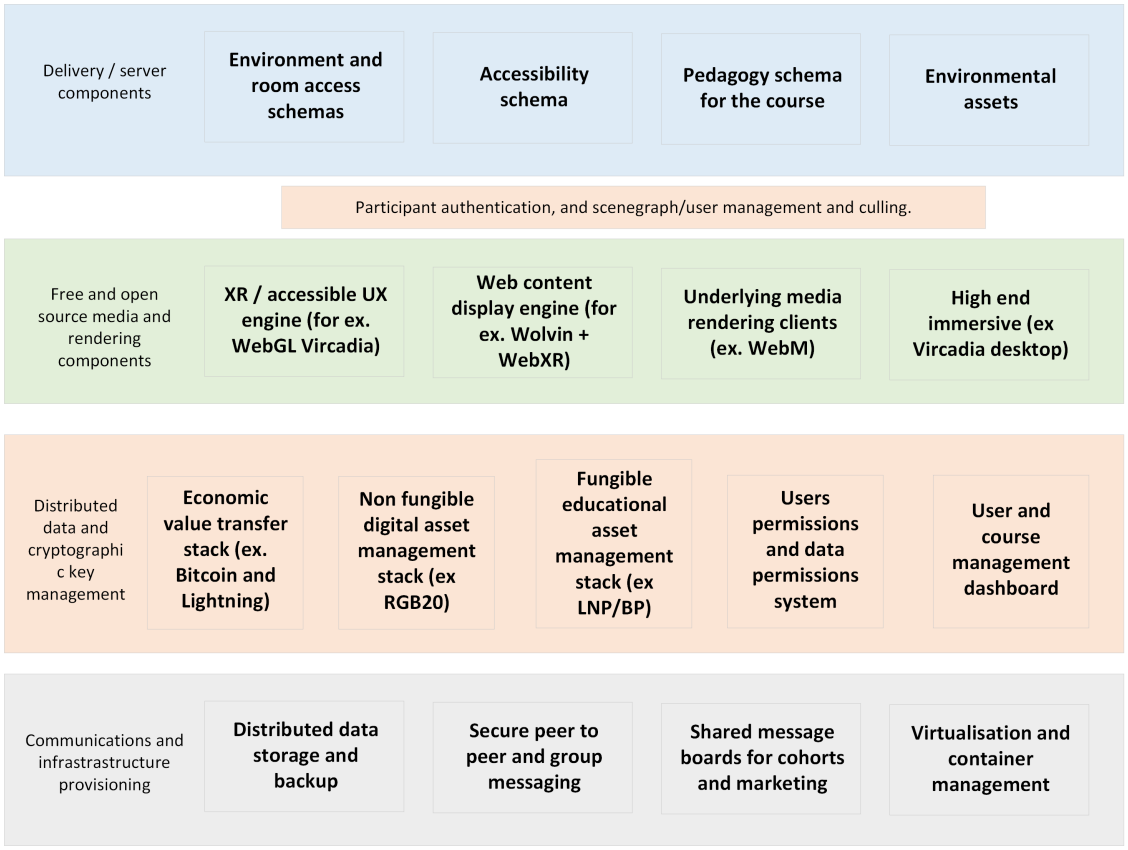


Figure 11.1: Functional elements for infrastructure.

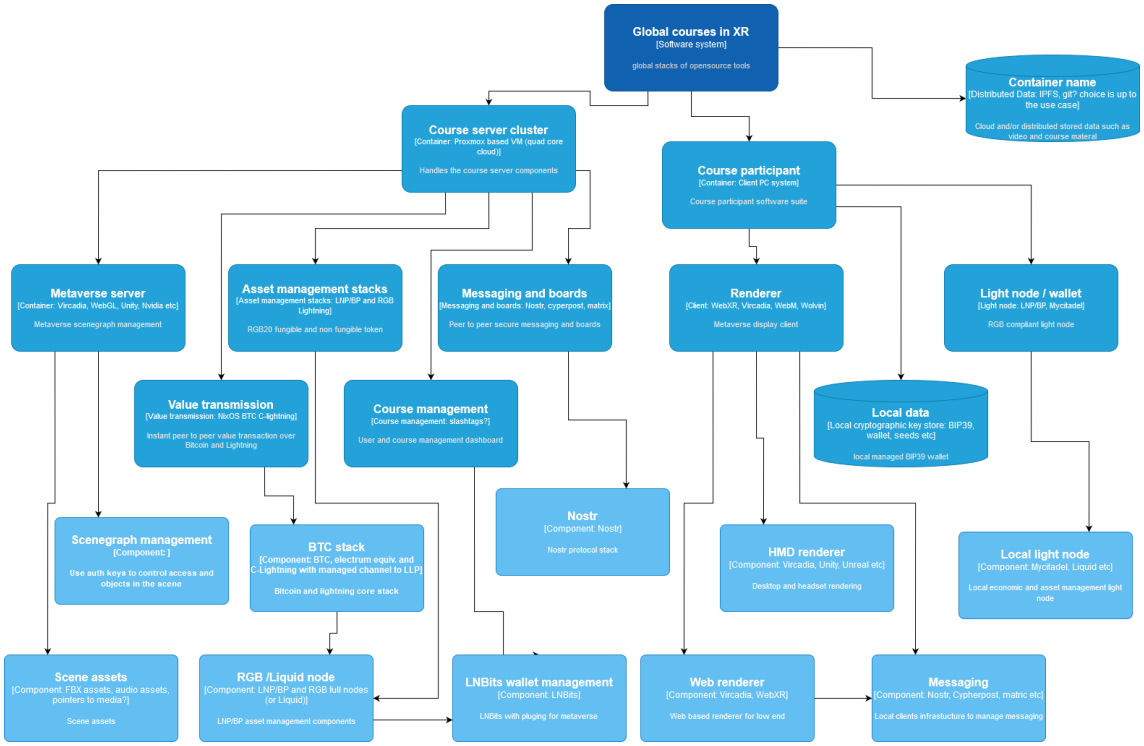
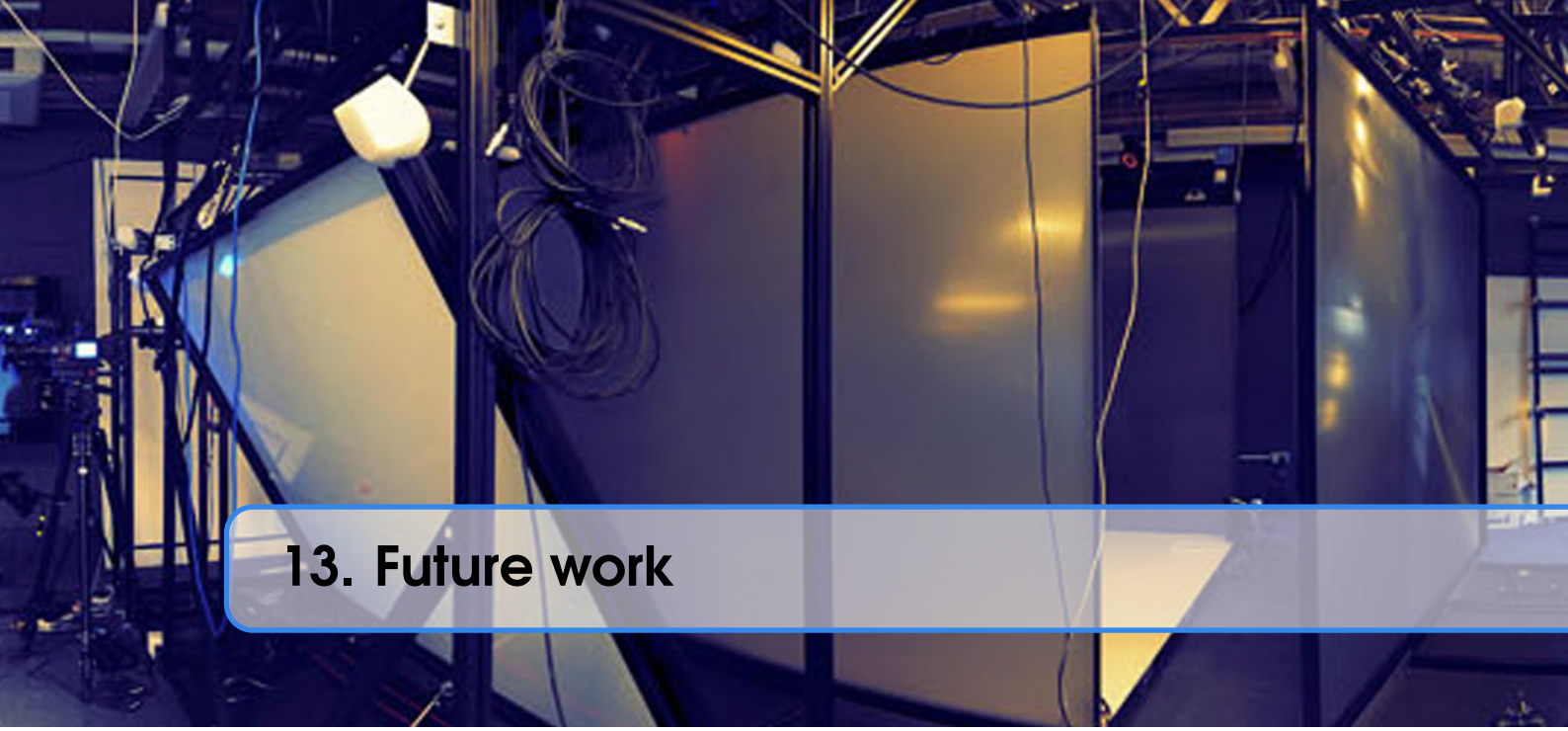


Figure 11.2: Client server C4 diagrams.

12. Conclusions



13. Future work

II Guides for deploying the software

13.1 Lab

13.1.1 Overview

This document details the process of creating the system detailed in the accompanying paper. It is intended to be complete. It is a how to guide.

13.1.1.1 Summary of software

Summarise the software and functionality

13.1.2 Prerequisites

Ensure that the BIOS / firmware / etc of the hardware you intend to use is up to date.

13.1.3 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).

13.1.4 Server configuration

13.1.4.1 Server hardware details

@todo

13.1.4.2 Disk configuration details

@todo

13.1.5 Proxmox VE

13.1.5.1 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).

13.1.5.2 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

13.1.5.3 Proxmox VE hardening

Links

@todo

Adding users

Add SSH keys and remove ability to login with password

13.1.6 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/

13.1.7 Install and configure Internet gateway server virtual machine

VyOS was selected (https://vyos.io/)

13.1.7.1 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:equuleus bash
```

Then in the Docker terminal run the following commands:

```
./configure --architecture amd64

sudo make iso
```

13.1.7.2 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

13.1.7.3 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/install.html)
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

13.1.7.4 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):

```
set interfaces ethernet eth0 address '192.168.x.221/24'
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

13.1.8 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.

13.1.9 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.

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.

13.1.9.1 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

13.1.9.2 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
```

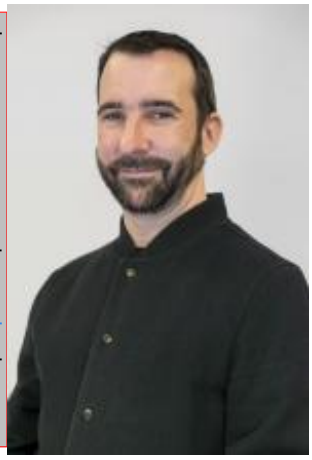
Once the above is complete and successful networking is verified
Run the following command:
`nixos-install`
and then reboot.

III Appendix

13.2 Acknowledgements and thanks

13.3 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'.



Bibliography

Articles

[1] Oxford Analytica. “El Salvador bitcoin experiment comes with risks”. In: *Emerald Expert Briefings* oxan-db (2021) (cited on page 35).

[2] Adam Back et al. “Hashcash-a denial of service counter-measure”. In: (2002) (cited on page 29).

[3] 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 38).

[4] 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 38).

[5] Matteo Benetton, Giovanni Compiani, and Adair Morse. “When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy”. In: *Available at SSRN 3779720* (2021) (cited on page 38).

[7] Apolline Blandin et al. “3rd global cryptoasset benchmarking study”. In: *Available at SSRN 3700822* (2020) (cited on page 38).

[8] 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 55).

[10] Vitalik Buterin et al. “Ethereum white paper”. In: *GitHub repository* 1 (2013), pages 22–23 (cited on page 31).

[13] 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 29).

[14] 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 page 29).

[17] Wei Dai. “b-money, 1998”. In: *URL http://www. weidai. com/bmoney. txt.(Last access: 08.04. 2019)* (1998) (cited on page 29).

[20] Whitfield Diffie and Martin Hellman. “New directions in cryptography”. In: *IEEE transactions on Information Theory* 22.6 (1976), pages 644–654 (cited on pages 29, 36).

[21] 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 34).

[22] 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 55).

[24] 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 53).

[25] Dror Goldberg. “Famous myths of" fiat money"”. In: *Journal of Money, Credit and Banking* (2005), pages 957–967 (cited on page 53).

[26] David Golumbia. “Cryptocurrency Is Garbage. So Is Blockchain.” In: *So Is Blockchain.(June 16, 2020)* (2020) (cited on page 31).

[28] Yuji Ijiri. “A framework for triple-entry bookkeeping”. In: *Accounting Review* (1986), pages 745–759 (cited on page 34).

[29] 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).

[30] 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 27).

[31] John Kirriemuir. “A Spring 2008 ‘snapshot’of UK higher and further education developments in Second Life”. In: *Eduserv Virtual World Watch* (2008), page 58 (cited on page 72).

[32] Daniel Krawisz. “Hyperbitcoinization”. In: *Online verfügbar unter: https://nakamotoin* (2014) (cited on page 58).

[33] Don Lavoie. “Prefatory Note: The Origins of" The Agorics Project”. In: *Market Process, v8, Spring* (1990), pages 116–119 (cited on page 29).

[34] 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 34).

[35] Mick Lockwood. “Exploring value propositions to drive Self-Sovereign Identity adoption”. In: *Frontiers in Blockchain* 4 (2021), page 4 (cited on page 64).

[37] Rick Marlatt. “Capitalizing on the craze of fortnite: Toward a conceptual framework for understanding how gamers construct communities of practice”. In: *Journal of Education* 200.1 (2020), pages 3–11 (cited on page 72).

[38] 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 57).

[39] Hilary McLellan. “Avatars, Affordances, and Interfaces: Virtual Reality Tools for Learning.” In: (1993) (cited on page 71).

[40] Ralph C Merkle. “Secure communications over insecure channels”. In: *Communications of the ACM* 21.4 (1978), pages 294–299 (cited on page 29).

[41] Satoshi Nakamoto. “Re: Bitcoin P2P e-cash paper”. In: *Email posted to listserv* 9 (2008), page 04 (cited on pages 29, 34).

[44] Michel Rauchs et al. “Distributed ledger technology systems: A conceptual framework”. In: *Available at SSRN 3230013* (2018) (cited on page 29).

[46] 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 34).

[47] Toni Sant. “Performance in Second Life: some possibilities for learning and teaching”. In: *Learning and teaching in the virtual world of Second Life* (2009), pages 145–166 (cited on page 72).

[48] Paul Sermon et al. “They live (in Second Life)”. In: (2008) (cited on page 72).

[49] 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 53).

[50] Nick Szabo. “Formalizing and securing relationships on public networks”. In: *First monday* (1997) (cited on page 29).

[52] Philipp Zabka et al. “Short Paper: A Centrality Analysis of the Lightning Network”. In: (2022) (cited on page 42).

Books

[9] David Burnham. *The rise of the computer state*. Random House Inc., 1983 (cited on page 29).

[12] Richard Cantillon. *Essai sur la nature du commerce en général*. éditeur non identifié, 1756 (cited on page 55).

[18] Glyn Davies. *History of money*. University of Wales Press, 2010 (cited on page 53).

[43] Eswar S Prasad. *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance*. Harvard University Press, 2021 (cited on page 56).