Challenges on the Way to a Secure and Decentralized Metaverse

Mykyta Skorokhod

Bachelor Thesis at the Department of Finance

Examiners:

Prof. Stefan Seidel

Dr. Katharina Drechsler

Submitted in the Bachelor program Information Systems at the Faculty of Management, Economics and Social Sciences of the University of Cologne

Cologne, August 11, 2023

Mykyta Skorokhod

Berrenrather Str. 348

50937, Cologne Germany

mskorokh@smail.uni-koeln.de

Student ID: 7345799

Table of contents

List of tables

List of figures

1 Introduction

Since the beginning of the computer era mankind was and is finding new ways to either transfer real-world processes into the digital world or augment them with digital technologies. This leads to a convergence of the real and virtual worlds into one interconnected reality.

The emergence of new disruptive technologies such as distributed ledger technology and especially blockchain has put us on the verge of a new era in digital technologies commonly proclaimed as Web 3.0. In a future driven by blockchain technology and empowered by smart contracts, coexistence within a system is determined through consensus among the majority of the system's participants, rather than being dictated by a minority of mega-corporations. Web 3.0 is imagined as a decentralized owned by everybody space that follows the motto “Can’t be evil” (Ball, 2022, p. 213; Dixon, 2021).

The occurrence and evolution of technologies also bring us closer to concepts exploited in science fiction for decades - virtual worlds and the Metaverse, a virtual world of virtual worlds (Nickerson et al., 2022), enabling immersive real-time experiences (Ball, 2022, pp. 35-40).

The notion of the Metaverse first appeared in science fiction and has gained significant attention recently after Facebook CEO Mark Zuckerberg announced to rename his company “Meta” thus claiming their interest in delivering the Metaverse.

According to Epic Games CEO Tim Sweeney the “Metaverse is going to be far more pervasive and powerful than anything else. If one central company gains control of this, they will become more powerful than any government and be a god on Earth”. To avoid such a dystopian outcome the intention of scholars around the globe is concentrated around the question of how to make the Metaverse into a place, owned and controlled by its participants. Distributed ledger-enabled decentralization is according to the current discourse one of the keys to it. However, there are several drawbacks of the technology to be overcome until it becomes a reality.

The worst thing about the Metaverse is also the best thing about it - it doesn’t yet exist, so it’s up to us to shape it and make it a reality (Ball, 2022, pp. 33-

34), hopefully fair, including and safe place for everyone not to escape or replace the real world but to complement and extend it.

This work suggests a point of view on the development of the Metaverse, where the emergence of interconnected virtual worlds that allow immersive experiences and seamless transition between them is seen not as a goal of the whole development, but rather as a far-off possible state of the co-existence of the two worlds. Furthermore, a model of possible development of the Metaverse is proposed, driven by the principle of optimizing the mutual enhancement of the real and virtual worlds. Finally, the core characteristics and principles underlying a possible implementation of the secure and decentralized Metaverse are grouped to form a framework that would facilitate the proposed development model.

The work is structured as follows. First, the background section provides an overview of the concepts crucial to the understanding of the analysis section. The analysis section starts with the motivation of the analysis conducted and proceeds with the results of the analysis. The discussion section summarizes the key findings of the work, and the conclusion section reiterates the research objective and summarizes the analysis conducted.

2 Background

This section provides an overview of the concepts referred to repeatedly in the work. First, the notion of the Metaverse and concepts related to it are discussed. The following sections elaborate on distributed ledger technology and blockchain, concepts enabled by distributed ledger technology, and novice frameworks and concepts deployed in blockchain networks.

2.1 The notion of “Metaverse”

Although the term Metaverse first appeared in Neil Stephenson’s 1992 dystopian novel “Snow Crash”, the idea of virtual worlds is reaching far in the past of science-fiction. For example, Stabley G. Weinbaum wrote a story in 1935 named “Pygmalion’s Spectacles” that described VR-like goggles, creating fully immersive and sensory realistic experiences. The movie industry has also contributed to science-fiction visions of the human-machine future in such classical pieces as “Tron” and “The Matrix”.

One thing in common for all the above-mentioned works of art is that they are all dystopian. “Pygmalion’s Spectacles” warned the readers of the potential escapism (Hirschman, 1983) arising from the beauty of the imaginary world. In “Snow Crash” the author’s point was that the Metaverse made real-world life worse (Ball, 2022, p. 12). In “Tron” the protagonist was trapped in cyberspace and “The Matrix” warns us of giving too much authority to a superior artificial intelligence.

Humanity’s concerns about what the future of two interwoven worlds may look like indicate first our fear of the unknown and second that humanity realized the potential dangers of such interconnection together with imaginaries of it. And while the virtual world possesses great power over the real one and that power is continually growing as we further shift to virtual interaction, we must keep in mind these precautions to be able to thoughtfully complement the real world with the virtual one, rather than replace or neglect it.

2.2 Different opinions about what the Metaverse is

There are many visions of what the Metaverse is. Microsoft CEO Satya Nadella (2021) for example imagines a metaverse as “made up of digital twins, simulated environments, and mixed reality” where “the entire world becomes your app canvas” (Nadella, 2021). Meta (former Facebook) CEO Mark Zuckerberg sees the Metaverse as “a vision” that is not going to be built by only one company but in a partnership between many other creators and developers (Newton, 2021). Furthermore, he believes it to be a successor of today’s internet, where instead of watching content on your screen you are actually in it (Newton, 2021).

Epic Games CEO Tim Sweeney sees the Metaverse as an evolution of users’ online interaction with brands, intellectual property, and each other (Park, 2021). According to Sweeney, the Metaverse should be an open space where users can freely incorporate with brands and each other in such ways that do not restrict self-expression and serve pleasure and joy, while users always can switch from one platform or provider to another, rather than being “trapped” in a “walled garden” of any of megacorporations (Park, 2021). Indeed, Big Tech companies offer more than one service or platform, switching between which is seamless and uncomplicated also providing users with the ability to transfer

their identity and credentials between them. But it is challenging if not impossible to use your information from one provider's platform on one of the other providers. The Metaverse if built by megacorporations may look like competing walled gardens, with no real interaction between different virtual worlds outside them. Furthermore, they may take their business models with them to the Metaverse, resulting in an uneven and unfair distribution of resources. For example, major gaming and software distribution platforms are currently charging the developers a 30% fee, while an average small-to-medium business in the USA gains only 10-15% profit from their products, meaning megacorporations owning these platforms usually gain more from creation and sale of digital assets than people who actually took the risk and created them (Ball, 2022, p. 174).

Epic Games is furthermore already operating a metaverse-like game called "Fortnite". Apart from offering a multiplayer battle arena, it also hosted a Travis Scott concert in 2020 and dropped a model of the Ferrari 296 GTB into the game that users can drive, creating a precedent of how industries may use the Metaverse for promoting their products (Park, 2021). Instead of just looking at an advertisement users may actually try the product in the Metaverse.

Moreover, Epic offers its game engine known as "Unreal Engine" which is a kit of software technologies and frameworks that are used to build virtual entities and worlds. A developer can use it to develop a game and must in turn provide Epic Games with 5% of the game's net revenue. According to Unreal Engine general manager Marc Petit, they are "trying to turn it [Unreal Engine] into a process that's very, very straightforward" to "power the metaverse and try to make it accessible to millions of people" (Park, 2021).

On top of that there also exists a so-called integrated virtual world platform (IVWP) based on Unreal Engine called "Fortnite Creative", where users can create new content with no coding needed, instead using graphical interfaces (Ball, 2022, pp. 104-108; Epic Games, n.d.).

Matthew Ball (2022) provides the following point of view on the Metaverse as being "a massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and

with continuity of data, such as identity, history, entitlements, objects, communications, and payments" (Ball, 2022, p. 35). He also addresses the question, of whether platforms such as "Fortnite" can be called Metaverses and states that they are rather Metagalaxies in what is to come as the Metaverse and a crucial point that will define the Metaverse is a level of interoperability between its different constituents (Ball, 2022, pp. 107-113). Another way to see it is as "an ecosystem of digital ecosystems, where each ecosystem can be conceived of as a universe with its own material and symbolic elements" (Nickerson et al., 2022).

But how to achieve interoperability between platforms, games, and experiences in general that are built on different programming languages, using different frameworks, and that usually even do not look alike? As pointed out by Ball (2022) in the Metaverse interoperability refers not to the question of whether services share information or not, but revolves around questions about who shares with whom, how much information is being shared, and at what cost (pp. 115-132). One way to achieve interoperability as presented by the scholars is standardization similar to that of the Internet (Seidel et al., 2022). However, a full standardization would mean neglecting some degree of diversity of the content, so instead the parties shaping the Metaverse would probably need to agree on "systems of systems" that could allow easier interpretation and contextualization of content by different platforms in the Metaverse (Ball, 2022, pp. 115-132), which also demands the involvement of every party contributing to the Metaverse (Nickerson et al., 2022).

2.3 Enabling technologies

For people to participate in immersive real-time virtual experiences there must be technologies to enable it. First, an extended reality headset (XR) offers a gateway to experiencing virtual worlds in a manner that the Metaverse visionaries imagine. However, the modern XR headsets, including virtual, augmented, and mixed reality headsets are either inferior to what would enable truly immersive experiences or are too costly, like the upcoming Apple's Vision Pro which would cost 3500 USD which is far more than a usual user could spend on a secondary device. A similar situation prevails on the market for other technologies that would enrich one's Metaverse experiences, like haptic

devices. There are however no doubts that technologies will evolve and as it happens to most consumer electronics these technologies will become more accessible in the future (Ball, 2022, p. 266).

More importantly, the Metaverse would enable real-time rendered experiences involving an effectively unlimited number of participants. For this to be possible system should have a way to stay synchronized throughout the users' devices, which poses a great challenge on the way to the Metaverse. There are two major characteristics of online connection to be considered, bandwidth, i.e., what amount of information the network can transfer, and latency, i.e., at what speed the information travels. In terms of bandwidth, the Metaverse poses an unprecedented case as the amount of information created by every user and which thus must be transferred to every other user in environments that should enable for an unlimited number of users to take part, is enormous.

Latency is even more crucial for the Metaverse. Currently, there are few services that need ultra-low latency connection, so the investments in these technologies are not high. Currently, information can take up to 1 second to travel between different points of the world. Imagine, how would you feel, if instead of practically instant receiving visual information that travels to us at the speed of light in the real world, you would see other users in a virtual world with up to 1-second delay. Usually, fast-paced games are unplayable with a delay of more than 150ms (Ball, 2022, p. 80).

Furthermore, no connection can be hundred percent secure, some unpredictable delays occur from time to time in every network, making it even harder to extend an experience to a scale of multiple thousands of users experiencing a virtual world simultaneously. Probably, we won't see the Metaverse as we imagine it until we explore new convenient ways to transfer information, for example using quantum particles (Röpke et al., 2021).

2.4 Ways to the Metaverse

In contrast to what the Metaverse could look like if owned by megacorporations, there exists a vision of a decentralized Metaverse. As pointed out by Xu et al. (2022) the Metaverse has a strong connection with the blockchain technology that enables interaction within the network of mutually

distrustful parties without a central authority using only encrypted identities that can be used directly for mutual authentication between actors in the Metaverse (Xu et al., 2022). Moreover, blockchain provides mechanisms, like DAOs and dApps, that enable participants to come together and aggregate resources in a more efficient way while relying not solely on participants' altruism but providing built-in incentives mechanisms that make it attractive for the users to participate thus providing the community with a mean to compete with trillion-dollar companies (Ball, 2022, p. 212). However, there is a challenge in how to efficiently use blockchain or generally distributed ledger technology in the Metaverse, given that reaching a consensus in a blockchain network requires extensive communication and computing (Xu et al., 2022).

The distributed ledger technology is however believed to provide more advantages to the Metaverse. First, it can be used to overcome the lack of computational resources inside the Metaverse. There already exist protocols, like Huawei's "Distributed Soft Bus" or in a network underlying an Otoy startup (Xu et al., 2022; Ball, 2022, pp. 204-205), that enable users to delegate their computing to other computers in the network. The latter operates on an Ethereum-based network named RNDR and issues its own cryptocurrency-like tokens. Every participant can send their computational tasks to other computers in the network without disclosing either their identity or the task being performed, while directly negotiating and paying for the service using RNDR tokens (Ball, 2022, pp. 204-205).

Moreover, blockchains are seen as the future of our online interaction as they provide transparency and immutability and are governed by the participants themselves, rather than by a central authority that can be flawed, biased, or simply persuading its own interests. In a decentralized organization people own the organization, govern it through democratic mechanisms, and profit when it's thriving. So, it may be useful for such a massive phenomenon like Metaverse to be owned by its inhabitants as they are more likely to maintain it to be able to profit from it.

2.5 IoT

The term "Internet of Things" refers to the concept of a network of interconnected smart devices that can communicate with each other, perform

their corresponding jobs and coordinate decisions in a shared environment or internet (Al-Fuqaha et al., 2015, pp. 2347–2376). The concept of IoT focuses on making the internet more immersive and pervasive (Zanella et al., 2014). So inherently this concept found numerous applications including home and industry automation, intelligent energy management, etc. (Zanella et al., 2014).

However, there exists yet no single broadly recognized implementation solution, because of the huge number of heterogeneous devices and environments to host IoT network or networks (Zanella et al., 2014), but also because there is no clear and widely accepted business model to attract potential investors (Laya et al., 2013).

As shown by Costidis & Devetsikiotis (2016) blockchain-based smart contracts network could be potentially used for automating a supply chain (Costidis & Devetsikiotis, 2016). Furthermore, a connected concept of applying IoT to an urban context, making better use of public resources, and increasing the overall quality of services provided to the citizens, while reducing cost of the public administration is usually referred to as a “Smart City” (Zanella et al., 2014). There are multiple areas of the city’s existence, such as monitoring of structural health of historical buildings, waste management, noise and air quality monitoring, traffic jam predicting and monitoring, and energy consumption monitoring, that can be automated or augmented by the use of digital technologies to create a win-win situation for citizens by increasing the quality of services and city administrations by decreasing cost of administration (Zanella et al., 2014).

Furthermore, the introduction of the concept of universal wallets, which are crypto wallets capable of storing or rather managing different data from cryptocurrency assets and tokens to identifiers and credentials opens possibilities for the IoT devices to authenticate each other and communicate in an IoT network (Jørgensen & Beck, 2022). Although, it should be pointed out that storing all the identifiers in a single wallet may create a single point of failure or attack (Hohenberger & Lysyanskaya 2005) so secure off-wallet data storage is needed (Gürsoy et al., 2020).

Although these challenges as well as the challenge of interoperability between different blockchain networks should be addressed before universal wallets

find wide usage not only by humans but also by any smart device, the concept is seen by scholars as playing a key role in digital transformation (Jørgensen & Beck, 2022).

2.6 What is Blockchain?

Though there are many uncertainties about what exactly the blockchain is - opinions vary from over-consumptive technology that is currently hyped through short-term speculations (Ball, 2022, p. 211) to technology with the capacity to bring up the next revolution to the Internet - it is generally believed to be an important technology (Beck et al., 2018).

First introduced by pseudonymous Satoshi Nakamoto in 2008 as a basis for the first cryptocurrency Bitcoin (Nakamoto, 2008) blockchain, more generally named distributed ledger technology, refers to a decentralized immutable log that includes all the transactions within a network of participants (called nodes) and is duplicated and stored by the members of the network. Each node in the network possesses a private/public key pair (Costidis & Devetsikiotis, 2016), is reachable via its public key, and can perform actions, such as signing a transaction, via its private key. The application of public-key cryptography makes it possible for the network to verify, if the action was performed using a specific private key based on the corresponding public key (Costidis & Devetsikiotis, 2016).

The characteristics of the blockchain that define to what extent the system is decentralized include how the coherence of the data among the nodes is reached, how the incentives are issued, who keeps track of nodes' private keys, and how the network is governed (Nabben, 2021b).

At this point, it is crucial to our understanding to differentiate between public and private blockchain. While in a public blockchain everybody can join and, dependent on the implementation of the network, participate in and contribute to it, in a private blockchain there is a central authority with the power to decide upon who may join the network, how the nodes may interact with the network and generally the state of the network and the underlying data structure, so the advantages of the private blockchain compared to a classical centralized database are quite limited. Furthermore, while in the public blockchain to

interact with the network nodes do not require to disclose any further information about themselves except their public key, in the private blockchain the central authority may require users' data before letting them participate in the network.

With this in mind let's examine why the public blockchain is seen as important for the future of the Internet.

First, it is essential to understand the main cryptographic function underlying the blockchain's data structure - the hash function. Put simply, the hash function is a way to transform data of arbitrary length into a fixed-length string called hash. The main feature of such transformation, besides the obvious impossibility to obtain the original data, used to form the hash, is the so-called collision resistance (Sobti & Ganesan, 2012, pp. 461-479), meaning that it is computationally impossible to find such a pair of different data that produces the same hash, i.e., given the state-of-the-art computers it is practically infeasible to change the data that was used to generate a hash so that the hash stays the same. So, every change to the data used to generate a hash, results in a completely different output of the hash function, as shown in Table 1.

Table 1. An example of the hashes produced by the SHA-256 hash function. The outputs of the slightly different inputs differ significantly.

Input data	Hash (hexadecimal)
Slightly different input	a6b5a6b180c14fb3638dc4400395760 21574690a4d31cdc5c0e1fe44f3b8ff36
Slightly different inputs	07d238311195017a94f39fa82811bbd 5ad8a34f624dd1f1f7edaac253fa46f63
slightly different input	ad2fdc1e4e86de27839e2285f1ac6faa b9aece6b1ded489ba81ca7ed9ce7b205
slightly different inputs	f14263f34c85e44d4819f8b9d7514524 145713772961fc0d8499df6060985e5c

With that understanding, we can proceed to examining the data structure underlying the blockchain. In the blockchain, the transactions are structured in

blocks of pre-defined size (in Bitcoin this is for example limited to 1 Mb). The block is usually structured as a Merkle tree (Figure 1) or its modifications (Ethereum Community, 2023, July 11) with the hash of the block being the root of the Merkle tree. Every block in the blockchain includes, along with the transactions, the hash of the preceding block, thus forming a chain constituted of blocks. Hence, if the hash of any block in a copy of the blockchain is altered, not only the hash of that block but also of all the following blocks become invalid. Given the fact that a copy of the complete blockchain is maintained by the set of nodes it can thus be restored.

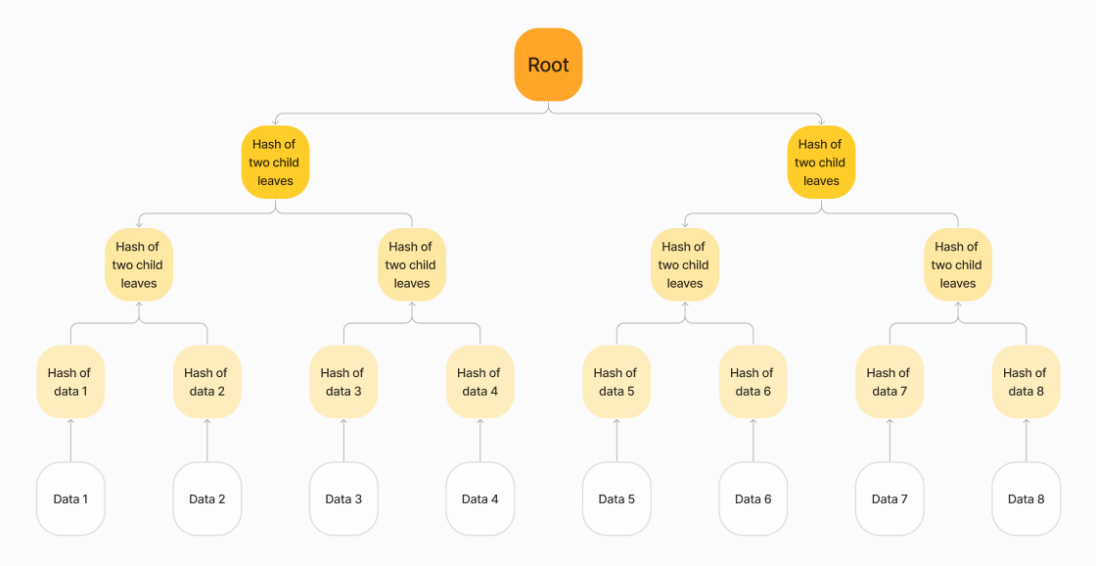

Figure 1. Example structure of the Merkle tree.

Furthermore, the decentralized maintenance of the blockchain makes peer-to-peer communication or transactions possible without a trusted third party or central authority. Since the whole history of the blockchain is stored in it every node that has access to the ledger can verify if the transaction made was valid. After verification, valid transactions are ready to be put in the new block of the blockchain.

To keep one consistent and shared truth about the system, thus averting chaos in such decentralized systems, the common single state of the system must be agreed upon by the nodes (Costidis & Devetsikiotis, 2016). The way nodes agree on the new state of the network and add new blocks to it is called consensus. The original problem behind the consensus is called the Byzantine Generals problem (Lamport et al., 1982). The problem describes the case of n

generals trying to agree upon a single common battle plan, while f of that n generals being traitors, trying to sabotage the agreement.

There exist multiple consensus mechanisms with their advantages and disadvantages.

The consensus mechanism used in the Bitcoin blockchain is called proof-of-work and adding a new block to the blockchain is called mining. Essentially, a basis for this consensus mechanism can be any task that is computationally difficult to solve but easy to verify (Tschorsch & Scheuermann, 2016). In the Bitcoin blockchain this task is represented by a random process of picking a series of numbers called nonce to include in the new block, so that the block's hash starts with a pre-defined number of zeros, i.e., the hash must be smaller than a predefined value. The first miner to find such nonce signs a newly created block and receives an incentive in the form of Bitcoin cryptocurrency. Since the operation of verification if the block meets the pre-defined condition involves a hash function, every node can hash the block itself verifying the pre-defined condition and thus confirming the new block's validity and adding it to their version of the blockchain.

The main disadvantage of the proof-of-work consensus mechanism is its exaggerated power consumption. While many nodes are trying to obtain an incentive for mining the new block, the amount of power their GPUs are consuming worldwide exceeds all conceivable limits: according to the 2018 estimates mining of new Bitcoin blocks has produced annual CO2 emissions comparable to 1 million transatlantic flights (Hern, 2018).

A widely used alternative to the proof-of-work consensus mechanism is proof-of-stake. While in the proof-of-work consensus mechanism the node with the most computational power is most likely to become the miner of the next block, in the proof-of-stake algorithm the creator of the next block, called the validator, is chosen randomly from the set of nodes that staked some of their funds to participate in the validation process. The higher the node's coin age is, i.e., the amount of funds staked multiplied by their holding period (King & Nadal, 2012), the higher is the node's chance to become a validator of a new block. After validating the block, the coin age is reset thus giving other participants the possibility to become validators (Tschorsch & Scheuermann, 2016). As pointed

out by one of the creators of the proof-of-stake algorithm in his interview (King, 2013), the risk of “rich getting richer” is balanced by the fact that “the poor also get richer”. The proof-of-stake mechanism requires furthermore much less computational power to validate the new block, thus making it far more sustainable than the above-mentioned proof-of-work mechanism.

The huge drawback as a result of maintaining decentralization of both of the beforementioned consensus mechanisms is their scalability, i.e., the number of transactions per second is heavily limited (Binance, 2023), because every transaction should be verified twice by the network, upon submitting and when added to the newly created block, thus making it highly time-consuming.

First proposed by the co-founder of Ethereum Dr. Gavin Wood the proof-of-authority consensus mechanism (Wood, 2015) is designed to tackle this drawback. The proof-of-authority consensus mechanism utilizes the node’s identity, instead of its funds or computational power. So, the validators are practically “staking” their identity while verifying new transactions and blocks (Binance, 2023). To be able to take advantage of this consensus mechanism it is crucial to give value to the identity itself, thus making this kind of consensus mechanism mostly unsuitable for most practically anonymous public blockchains.

To briefly summarize the keys to understanding blockchain, or more generally distributed ledger technology:

- The network of users called nodes engage with each other using public-key cryptography.
- Every node maintains its copy of the complete data structure, thus making it practically infeasible for the attacker to change it in their own benefit.
- The pieces of information (called blocks in blockchain) are furthermore connected to each other thus making it impossible to change one piece without changing the whole structure.
- Every change to the data structure must be validated by the majority of the network or by pre-trusted authorities, i.e., a consensus about the state of the data must be reached, thus maintaining one coherent truth about the network shared by everybody.

- Rules about what transactions, or more generally interactions, are valid are embedded into the system and are verified by other nodes upon interaction and upon adding information about them into the shared data structure (Costidis & Devetsikiotis, 2016).

The key feature of the public blockchain is its decentralization. So instead of having one central authority that keeps track of the transactions between the nodes and the state of the network, this function is delegated to the blockchain participants themselves. In other words, the network participants are the governors and maintainers of the network.

2.7 Important extensions of the blockchain technology

A crucial extension to the blockchain network is a concept of a so-called smart contract. Smart contracts are pieces of code that run on-chain and enable the autonomous execution of rules or actions embedded into them (Szabo, 1994). The blockchain architecture described above enables the transfer of digital resources in a peer-to-peer manner without a need for a trusted central authority, while blockchain with support of the smart contracts enables multi-part interactions to take place between users that do not trust each other (Christidis & Devetsikiotis 2016).

An important feature of smart contracts is that they are definite, i.e., the same inputs will lead to the same outputs (Christidis & Devetsikiotis 2016).

Furthermore, usually, smart contracts are also legally enforceable “as long as they follow the basic rules of contractual agreement” (Herpy, 2022). These rules include offer, acceptance, and consideration (Herpy, 2022). Offer means that the contract was proposed by one or more parties. Acceptance refers to the fact that all participants agree on the terms of the contract and consideration expresses the mutuality of value gained through the contract, i.e., the contract should be mutually profitable (Herpy, 2022).

The last building block of our understanding of the modern blockchain is non-fungible tokens or NFTs. These are cryptocurrency-like assets in the blockchain network. But unlike cryptocurrencies or traditional currencies that can be substituted by another asset with the same value, NFTs are unique (Ball, 2022, pp. 199-203). So, practically everybody can upload a unique piece

of code, art, or whatsoever as a NFT after which the right of ownership of this item can be traded similar to cryptocurrency (Ball, 2022, pp. 199-203).

Practically every unique item can be linked to a distributed ledger-based digital world by creating a token of it and thus connecting it to the real-world entity. Furthermore, dApps and DAOs (described in a further section) can issue their own tokens that can be traded in the same way as the cryptocurrency to people that contribute, maintain, or govern the dApp or DAO.

2.8 Blockchain security

To be able to use blockchain or distributed ledger technology we must guarantee that the users of the system are put in the center of the system's security, i.e., that the system's security is focused on the users' security, referred to as "people security" (Nabben, 2021b). But to design a system that is effectively secure when used by people is a very challenging task, as the designer may not be aware of users' actual desires and behaviors (Ferreira et al., 2014).

In the context of security, a new extension to the provided differentiation between public and private blockchains arises. In the private blockchain, there is a central authority that is given the power to alter the system without the actual agreement of the users (Nabben, 2021b). While public blockchain stimulates active participation of users in the development, governance, and maintenance of the system, in private blockchain these functions are concentrated in the hands of a central authority, thus minimizing the role of people in the system solely to "users", whereas in public blockchain they can be described as "participants" (Nabben, 2021b).

This is a crucial point to consider because in cases when users are not permitted to participate in shaping and defining the system, their security can be more easily put at risk (Nabben, 2021b).

2.9 Blockchain use-cases outside cryptocurrency

Although blockchain technology found its primary use in cryptocurrencies, there is much more it can offer than just this application. More generally, distributed ledger technology can be seen as a way to securely achieve

consensus in a peer-to-peer network (Greenspan, 2015) without a need for a central authority.

Blockchain technology has a crucial implementation in enabling more secure and decentralized ownership of personal data (Zyskind et al., 2015). In a framework proposed by Zyskind et al. (2015) blockchain technology is used to keep track of what information is disclosed to which service thus enabling more transparent and user-oriented data management.

The system functions as follows (Zyskind et al., 2015):

- There are three building blocks of the systems, users of the applications, services providing these applications, and nodes that maintain the system.
- When a user first downloads the service's application, a shared user-service identity is created, with the user being the owner of this identity. The service has restricted access to the identity based on the user's personal data access permissions, given to the service by the user. This information is sent to the blockchain.
- Whenever personal data is generated by the user, it is first encrypted using shared by the both user and service private key and then sent to the blockchain that sends it further to an off-chain data storage, leaving only a hash, i.e., pointer or identifier, of the data on-chain.
- Now both the service and user can retrieve data using its pointer, i.e., hash, and decrypt it using the shared key. Furthermore, the user can revoke access permissions granted to the service at any time.
- The off-chain data storage is proposed to be implemented via a distributed hash table. In this scenario nodes storing data, are still not able to access it, as the data itself is encrypted via an identity's private key.

One of the significant contributions of the proposed framework is that it illustrates how an a priori disclosed to everyone blockchain can be used to manage sensible data in a way that doesn't violate the data owner's interests and privacy (Zyskind et al. 2015) at the same time gaining advantage of the decentralized nature of the blockchain.

Another similar blockchain-based framework for personal data management was proposed by Onik et al. (2019). The framework however makes use of the smart contract technology, formalizing the relationships between data owners and services or processors of the data and furthermore suggests using the user's local storage as an off-chain data storage, so that every user practically owns and controls its data (Onik et al., 2019).

Technology communities echoed the idea of decentralization and giving more power to people, rather than central authorities. The application of blockchain and especially smart contracts technologies pushed this idea further and made the implementation of more complex "autonomous" systems possible. This led to the emergence of systems currently known as Decentralized Autonomous Organizations or simply DAOs as an innovative institutional structure for technology-driven governance (Nabben, 2021c). A DAO is a system implemented via smart contracts built on top of a blockchain network that enables coordination and governance of the system moderated by a set of rules embedded in smart contracts (Hassan & De Filippi, 2021). Such a constellation makes all imaginable applications of blockchain technology possible, it can be implemented as a ridesharing or crowd-funding platform, automated organization, or decision-making tool. This flexibility is enabled by the fact that a DAO refers to a concept, rather than a specific business model or organization type (Hassan & De Filippi, 2021).

DAOs can be also seen as automated decision-making systems, or ADMs (Nabben, 2021c), referred to as any system, software code, or model that uses computations to complement and/or replace government judgments and decisions (Richardson, 2021).

More generally, a DAO can be seen as a group of people, participating in a common goal, that operates as a single entity and uses a blockchain for governance (for example voting on decisions) and exchange or accumulating of value (Nabben, 2021c).

In any way, DAOs are a fascinating technical phenomenon that may shape the future of society and the ways we communicate online using digital mechanisms and can be also useful for further decentralization and democratization of governance (Nabben, 2021c; Hassan & De Filippi, 2021).

Although, after the infamous TheDAO Hack, during which a hacker utilized a bug in the DAO's underlying smart contract to drain millions of dollars in cryptocurrency from TheDAO and which also led to a split in the second largest cryptocurrency Ethereum (DuPont, 2017) the enthusiasm around and trust in DAOs as the future of the organization was shaken. The problem was in a poorly programmed smart contract that allowed the hacker to withdraw funds from the smart contract recursively until there were no funds left.

DAOs allow us to experiment with and explore the notion of "autonomy". Two important questions to be addressed in this discourse are who or what is made autonomous in such organizations and what is the actual meaning of "autonomy"? Former is rather a rhetorical question to be considered by the designers and developers of an autonomous organization that need to find a good balance between cost and desired autonomy for both people within the system and the system itself (Nabben, 2021c). The answer to the latter question is not obvious, is open for interpretation and can furthermore significantly shape the future of distributed ledger technology generally.

Usually, autonomy is referred to an ability of an entity to freely decide its own behavior and future free from external intervention or coercion. But in a system like DAO whose constituents are autonomous elements themselves, there is an inevitable tension between individual autonomy and autonomy of the whole (Nabben, 2021a). Furthermore, the autonomy of the whole is rather its ability to self-organization, self-reproduction, and self-governance, rather than being free from human intervention (Nabben, 2021a). The DAOs are created by humans and in human society, so their implementation cannot be truly free from the biases of their creators (Nabben, 2021c) and it is crucial to preserve the "creative core" of the individuals, as it is the essential "engine of evolution" (Principia Cybernetia, 1989).

Another crucial extension to blockchain technology is the so-called decentralized apps or dApps which are software applications that run on a distributed network thus profiting from the benefits that distributed ledger technologies provide.

So, DAOs and dApps provide us with a close-to-the-real-world but an open-to-imagination playground, where we can test and evolve our presumptions about how a decentralized, open, and secure Metaverse could look like. Together with assuring Metaverse's critical characteristics, like interoperability, scalability, and synchronicity, we must address the question of the right degree of its autonomy, i.e., find a right balance between trusting computer and AI, while preserving humans' "creative core" (Principia Cybernetia, 1989).

2.10 Zero-knowledge proof

Wide-accepted and used public-key cryptography also has its drawbacks. While the user in such systems possesses its own public-private key pair, encrypting messages using the private key discloses some portion of information about the private key. It is thus generally recognized that the most dangerous attack, among the natural ones, on the system that uses public-key cryptography is a so-called chosen-cipher-text-attack, when an attacker tries to break the system by asking and receiving decryptions of a cyphertext chosen by the attacker (Blum et al., 1988).

To address this drawback and to increase the overall privacy of user's private information the concept of a zero-knowledge proof system was introduced (Goldwasser et al.,1985; Blum et al. 1988) as a way to prove a statement without revealing the information used to proof the statement and it functions as follows:

- Two participants namely the verifier and the prover take part in a zero-knowledge proof system.
- The verifier inputs a statement that must be proved by the prover in a system's underlying protocol (e.g., the fact that the prover possesses a specific private key that can decrypt an encrypted message).
- The zero-knowledge protocol represents the statement as a problem that is solved only if the statement is true and will be unsolved else. Thus, it ensures that the verifier can verify a statement without a prover needing to disclose any information rather than the answer to the statement itself. Furthermore, it ensures that the probability of a malicious prover verifying a statement without possessing the information needed to verify it is minimized and approaches zero.

First zero-knowledge protocols were interactive, meaning the verifier and the prover needed to communicate back-and-forth repeatedly with a verifier picking random problems for the prover to solve thus minimizing the probability of the prover's "lucky guessing" and thus maximizing the probability of the trustfulness of the statement's answer. This property of the interactive zero-knowledge proof has limited its scalability and made independent verification impossible, because computing a new proof would require a new round of communication between the verifier and the prover (Ethereum Community, 2023, August 3). A non-interactive zero-knowledge proof protocol suggested by Blum et al. (1988) introduced a process of zero-knowledge verification of a statement requiring the verifier and the prover to communicate only once.

Two important instantiations of a non-interactive zero-knowledge proof are a ZK-SNARK protocol (Ben-Sasson, published 2013, last updated 2019) that is already being used in several blockchain systems and a ZK-SNARK's improvement ZK-STARK (Ben-Sasson, 2018). A major difference between them is that while ZK-SNARK requires a trusted initial setup for verification to be trustful, ZK-STARK makes use of collision-resistant hash functions to eliminate the need for a trusted initial setup, furthermore, making ZK-STARK protocol secure even in the face of potentially unlimited computational power provided by theoretical concept of quantum computers (Ben-Sasson, 2018).

Zero-knowledge proof can enhance distributed ledger technology in many ways. First, it can be used for transaction (interaction) verification in a way that enables more scalable solutions (Riabzev & Ben-Sasson, 2019). Furthermore, it can significantly simplify authentication mechanisms saving storage space for both parties of the authentication process, and reduce the risk of collusion, i.e., bribery, in on-chain voting mechanisms by hiding information about how nodes have voted (Ethereum Community, 2023, August 3). The main drawback of the zero-knowledge proof protocols is their computational intensity which makes them unsuitable for small or mobile devices (Ethereum Community, 2023, August 3).

2.11 Blockchain interoperability

Since the Metaverse is going to be constituted by many different worlds and platforms all built using different tools and frameworks interoperability as

mentioned before will be a big issue to overcome. If some of the separate worlds are going to be built using distributed ledger technology, we must consider a way of exchanging information between them that doesn't violate its underlying advantages. Zamyatin et al. (2019) stated and proved that there can be no cross-chain communication protocol that can operate without a trusted third party (Zamyatin et al., 2019). But the trusted third party could be centralized as well as decentralized, i.e., like a blockchain of blockchains, where nodes reach a consensus about the state of the global ledger using the consensus mechanism (Belchior et al., 2021). Besides, such a protocol was already proposed by Garoffolo et al. (2020) named Zendoo. Zendoo is a cross-chain communication protocol that proposes structuring the mainchain and sidechains constituting it into "a parent-child relationship", where the mainchain facilitates communication between different sidechains without revealing their corresponding internal structure or the transactions conducted enabling mainchain nodes to observe only "cryptographically authenticated certificates" that authorize transfers coming from the sidechains (Garoffolo et al., 2020, pp. 3-4). Authentication and validation via certificates are achieved by using the abovementioned ZK-SNARK protocol, while the sidechains are free to establish their own rules for both authentication and validation that still comply with the verification interface used by the mainchain thus giving the sidechains freedom in choosing and defining their own validation and authentication mechanisms.

3 Analysis

In this section, the actual analysis is conducted. The first part provides the motivation as well as an overview of the analysis results. Following sections present the findings of the work, a model of possible development of the Metaverse in a secure and decentralized open space, and a framework of the Metaverse that could facilitate the proposed development model.

3.1 Motivation

There are so many obstacles on the way to the Metaverse as described in the previous sections that it stays a rather far-off concept yet to be brought to life. There probably won't be a single point of emergence of a ready-to-connect-everything Metaverse but rather a way to it through different stages of

interwovenness between real and digital worlds. Lee et al. (2021) proposed a concept involving three stepping stones on the way to a synergy state of the two worlds. These are defined as digital twins, digital natives, and the co-existence of physical-virtual reality. The first step involves the development of the virtual copy of the real world capable of influencing the real world. Digital natives refer to a state of the Metaverse, where multiple virtual worlds are emerging and interconnecting. And finally, the third stage refers to the co-existence of two worlds in a merged and perpetual common state (Lee et al., 2021).

This work elaborates this vision of the possible development of the Metaverse further into a possible scenario of the co-existence steps of the real and virtual worlds.

To be able to propose a way it is crucial to first define the way's direction. From an interpretive standpoint, I suggest that the Metaverse refers to a rather unreachable utopian point in co-existence and immersion of real and virtual worlds, where the virtual world and digital technologies comprising it are optimally used to complement the real world at the highest achievable level. It is also a chance for humanity to define a new reality that could in perspective shape the real world of tomorrow, finding and showing a way to overcome drawbacks of the society.

The development of the Metaverse cannot thus be limited to any single perspective or field of study but is to be performed in a synergy between sciences and specialists. It is also extremely unlikely for an individual or a group of individuals to fully understand and realize the Metaverse in its whole complexity.

Driven by this definition following sections propose a model of the development of the decentralized Metaverse, driven by the principle of optimizing the mutual enhancement of the real and virtual worlds which is constituted from the following steps:

- DAOs as an operational ground to experiment with self-organization and self-governance.
- Real world's digital twin driven by the IoT.

- The Metaverse.

Finally, the core characteristics and principles underlying a possible implementation of the Metaverse are grouped to propose a framework that could facilitate the proposed development model.

3.2 A possible way to a decentralized and secure Metaverse

Decentralization is a core principle underlying the truly secure Metaverse. However, it isn't a ready-to-use framework that can be utilized while developing the Metaverse, but rather an overarching concept of distributing power over and responsibility for the commonly used resource. The prerequisites of deploying this concept are numerous and hard to define in advance. But the one thing commonly accepted is that an environment, whose participants are free to decide upon their individual and collective future, is far healthier and more desirable than current real-world society concentrated around a handful of big players. In the Metaverse as a not yet realized concept we are free to redefine the mechanisms that determine the distribution of various resources. It is also important to keep in mind that decentralization doesn't automatically mean solving all societal problems, the human core is still going to be irrational, but it can be rather seen as a means to involve as many participants as possible in the process of defining the common future.

The decentralized nature of the distributed ledger technology can assist greatly in realizing decentralization in a digital space. Blockchain isn't the only working adaptation of distributed ledger technology and hasn't moreover yet reached its full potential. And yet the underlying idea of decentralization, removing the need for a trusted third party to interact in a distrustful environment and giving the participants themselves the power to govern the whole system has gained so much attention that it became viral, which allowed digital assets issued in blockchain-based systems to attain a real market value.

Moreover, structures built on top of distributed ledger technology such as DAOs provide an operational arena for researchers and developers to experiment with different methods of organizing societies in a sustainable manner that enables self-governance and self-regulation. This may be seen as a first step towards the Metaverse from our standing point.

Many may refer to the blockchain as being overhyped. The value of cryptocurrencies based on this technology is indeed sometimes exaggerated through speculations and promises to earn “easy money”. But the underlying idea of the blockchain of removing trusted intermediary in interactions in the financial sector is so powerful that it became recognized as a payment method which is a strong precedent of the market’s flexibility to adapt itself to new ideas.

The Metaverse could potentially be designed based on the distributed ledger technology to realize decentralization and deeper involvement of different parties comprising it. It could also potentially issue its own tokens to incentivize people to take part in the greater whole. Driven by this acknowledgment the next stage of the development of the Metaverse is proposed as augmenting the real world with the IoT concept from within the Metaverse.

As described earlier multiple areas of urban life can be complemented and supported using smart technologies. Although research is needed to discover proper frameworks to create sustainable and coherent solutions in the field of IoT, the Metaverse based on distributed ledger technology could facilitate this process.

The IoT concept aims at augmenting as many processes as possible by connecting different processes and their constituent parts into a single network. This network will probably span beyond cities and even countries. Finding a way to construct such a network is a problem similar to defining the Metaverse as universal, connecting everything to everything network constituted from heterogeneous parties and environments, i.e., virtual worlds. The model proposed in this work uses this acknowledgment as a motivation to explore a structure that could enable the development of an immersive and omnipresent IoT network that could be experimented with and used as a basis for the Metaverse’s virtual world of virtual worlds.

The main motivation for creating an omnipresent IoT network is the possibility of making better use of resources and overall improving the services for the people. This includes many different applications of an even greater variety of heterogeneous smart devices, i.e., devices able to communicate with each other and coordinate in a shared network. The problem of bringing them all

together in a single network where they can exchange data at the same time not violating the privacy of their owners is comparable to the problem of bringing many virtual worlds in a single immersive Metaverse. This constitutes the second stage of the development of the Metaverse where bringing diverse devices and environments based on different protocols and frameworks to securely interact within a shared network presents a ground to experiment with different means to overcome interoperability issues. The findings of this development stage will be of further use while extending the Metaverse to multiple worlds owned by multiple parties.

The main driver of this stage could become the commonality of problems addressed by the development of the IoT network. It is of our common benefit to make the best use of the resources provided to us by our planet. It is of benefit to all coming generations all over the world if we find ways to sustainably expand and evolve together with our environment while not neglecting it. The universality of these benefits of the effective use of the IoT concept brings up the acknowledgment of its underlying inherent value that is shared by everybody on the planet. Augmentation of real-world processes like creating smart electricity grids, overall improvement of urban life, supply chain automation, and many more all contribute to the better use of the resources that are often limited. Given the young generations' growing concern about the environmental impacts of human activity (Jahns, 2021) these values will be shared by an ever greater number of people worldwide with generations to come. This can become the core of recognition of the value of the IoT in the Metaverse thus acquiring greater attention and investments, driving the development of the Metaverse further.

In addition to it, we are free to define actions and behaviors that are to be incentivized in such a network to direct its development as a self-governing organism. Some of the examples include contributing to a more complete digitized picture of the world, honest validation of interaction and honest interaction itself, storage and computational resources provided for common use, and many more. The full list is however not going to be defined by any one person or organization, but rather evolved through universal participation within the network. Another important question is how to avoid or punish

undesired actions and behaviors. The Metaverse is more likely to be a space open for collaboration and composition of experiences in new unpredictable ways thus creating new experiences (Nickerson et al., 2022) rather than a space free from malicious or antisocial behavior. One way one could consider is a social network-like process that enables users to report undesired behaviors and hiring moderators (possibly AI-based) that track and ban such behavior. But first, these mechanisms haven't managed to transform social networks into a bullying-free space and second heavy reliance on such mechanisms at deciding individuals' socioeconomic statuses could lead to unpredictable outcomes where people are judging each other too harshly based on their own subjective beliefs. Thus, we would need to explore new ways of managing interactions within the system.

The crucial point to be considered in the IoT network comprising this stage of the Metaverse are security issues. If the data collected from the ubiquitous network of devices is controlled and processed by one central authority it could create a potential point of misuse shifting the network towards quite a dystopian future of surveillance. Instead, as inspired and enabled by the distributed ledger technology every participant should be able to own and control their data. It can be accomplished using various techniques that are enabled by distributed ledger technology, such as smart contracts. Although it is important to keep in mind that hard-coded rules cannot fully depict the complex nature and randomness of real-world interactions and thus cannot be made into a single or final instance for decisions in the systems. Instead, the system should involve some degree of humanness to be able to adequately reflect and augment the real world.

Upon successful implementation of such a network, it may become a starting point for the Metaverse.

The Metaverse is furthermore to be designed in a way that assures its ability to self-govern, self-organize, and self-regulate. It would also provide different people with a way to persuade their dreams no matter what they are. It doesn't necessarily need to be creating or adding value to the Metaverse itself, but probably rather anything that doesn't endanger it. The Metaverse has the potential of becoming an environment where the skill and quality of the work

are given value (Park, 2021). How do we measure skill and quality throughout numerous heterogeneous domains of human activity? One answer to this question could be with the help of like-minded creators and connoisseurs. If appropriately designed the Metaverse could become a space of unlimited collaboration inside and between groups of like-minded individuals, a process which in turn would further drive innovations and progress. One should be able to find and connect with others seamlessly, at the same time preserving mutuality and privacy.

3.3 Proposed model of the Metaverse.

3.3.1 Structure

The proposed model is constituted of three interconnected layers.

- The first layer is the resource layer representing distributed and shared computational and storage resources.
- The second layer is the distributed ledger layer, needed for the participants to be able to reach the first layer and interact with each other. This layer is mostly constituted of the smart contracts between participants.
- The third layer is the operational layer, where the nodes are free to interact with each other based on the smart contracts in the second layer.

3.3.2 First layer

The first layer represents all the computational and storage power currently available to the participants. As soon as a participant joins the network, i.e., goes online, its computational resource connected to the system are becoming available in the first layer. This of course implies that the demand for the computational resource is lower than the shared resource because otherwise it would make no sense for participants to join the network where they cannot operate but must instead give their computational power to others. But this condition is addressed by the proposed development model of the Metaverse, where the first operational step of it is going to be the IoT. First, the city administrations, i.e., the governments are going to be interested in the IoT to succeed, simply because it would save them money, so they are likely to invest

existent computational resources to support the system. Second, there will be a built-in incentivization mechanism for the participants for sharing their resources, so it is also likely that participants will go online to share their resources to earn tokens. So, it is assumed that the participants will first use their local computational power and in case of the need for the additional computational power will access the shared resource.

As already outlined the first layer is going to include the shared storage resources. For it to work conveniently there should be well-thought-out rules for participants to share their storage resources. First, the data is going to be stored in an encrypted way, possibly using dynamic encryption (Knudsen, 2015) to enhance security. It must also be guaranteed that the storage is reachable around the clock with some margin for unreliable internet connection and that the storage moreover won't lose any information. There is also going to be a built-in incentivization mechanism for the participants for sharing the storage resources, as well as a reputation-based penalty for broken guarantees that would affect only the ability of the participant to share this resource.

3.3.3 Second layer

The second layer represents the distributed ledger layer, where the smart contracts between participants are written and stored. For the smart contracts to work the distributed ledger should run some kind of virtual machine (VM), i.e., an operational computer, so the second layer will also use computational resources from the first layer.

Furthermore, smart contracts are going to be concluded using zero-knowledge proofs of identity between participants and added to the distributed ledger via a consensus mechanism, which is going to be an adaptation of the proof-of-authority as the mechanism of reputation is already introduced to the system. However, it is crucial to design the reputation mechanisms so that they do not endanger autonomy in the system (Nabben, 2021c). Another possible issue with this setting is that due to the computational intensity of the zero-knowledge proof protocols, the proof by other nodes can create a computational bottleneck. Alternatively, a mechanism similar to the one from public-key cryptography can be used, where the participants both sign the smart contract,

and other nodes can verify the signatures using respective public keys. In both settings, however, it is also possible to change the conditions of the contract by repeating the process of mutual agreement and verification conducted to create the smart contract.

To enable provability of the content of the smart contract at the same time not disclosing the complete content of it only a hash of the content will be written on the distributed ledger, while the content itself is going to be stored on the participants' storage so that it can be accessed by the VM but not seen by other participants on the distributed ledger. The conditions of the smart contract are going to be enforced only if they hash to the same value stored in the smart contract. In case of unavailability of both participants, the conditions are going to be run as soon as one of them is online and the VM can successfully query the data. If stored by the participant conditions of the smart contract do not hash to the value stored in the smart contract the reputational sequences will follow. If conditions stored by both participants do not hash to the value stored in the smart contract thus making the contract unenforceable, it is terminated creating a disputing situation to be handled in the common space, while both participants receive reputational penalties.

The usage of shared resources is also going to be regulated via smart contracts. To use a shared computational or storage resource a smart contract is automatically generated, including only the public identities of the participants and incentive for the provider of the shared resource proportional to the resource usage.

3.3.4 Third layer

The third layer is going to be initially blank space where the interactions are conducted. Every participant has a pair of private and public keys and is addressable via their public key and utilizes the private key to authorize interactions. All the data is going to be stored locally or at the specified by the participant storage, like for example home PC in case of smart home devices or cloud storage if the participant wishes so so that the participants are in control of their own data.

There are unlimited possibilities of what this space could look like and will likely be shaped by collective efforts. Possibilities include plain internet-like space and real-world digital twin where other nodes are findable either at their respective real-world locations or via advertisements. It would depend on many creators and developers, as well as platforms that provide game engines and IVWPs, what the common interaction space will become and there are going to be built-in incentives also for enriching this space, as well as for providing means to enhance it.

3.4. General acknowledgments

The proposed system should also include space for collective decision-making and collaboration that affect multiple parties or the whole space itself similar to Cossack Rada (council) held in the center of the Sich (administrative center of Cossacks), where the important decisions concerning the common space, resources, and future were discussed and reached. The complexity of interactions is also going to rise together with the evolution of the system and its inclusion of further processes, so there are going to arise disputes that can also be resolved in a common space for example in the form of the jury where the jury can vote on different outcomes. Participation in these processes needs to be incentivized as it directly contributes to maintaining and governing the system and the more people participate in these processes, the fairer they become. The problem with this approach is the inability of a pseudonymous system to guarantee that people vote only once thus removing the risk of the Sybil attack (Douceur, 2002), in which one individual uses multiple identities within the system to attack it. To overcome this challenge, it is going to be eventually required to provide identity validation to join the system. However, with the help of zero-knowledge proofs and the fact that participants are in control of their own data, it is possible to guarantee that this personal information either stays known only to the user or is provided only once to generate a unique hash of it thus guaranteeing that the person if joining once more will be recognized as the same individual. The problem with this approach is that there can be collisions, that is two different sets of data can produce the same hash, which is extremely unlikely but possible. Increasing the number of bits used in the hash function could further minimize the probability of collision but not eliminate it completely.

Interaction model based on smart contracts also provides means to regulate interactions in the more distant Metaverse space, where there is going to be much more room for various interactions. One way to use it is to enable some primary interactions in the shared layer while giving participants the possibility to mutually agree on deeper levels of interaction that will be formalized in the form of a smart contract. Furthermore, there are going to be virtual worlds in the Metaverse, where the level of interaction will be mutually enhanced, like battlegrounds where participants can fight each other. The only problem with this model is how to guarantee that minors are excluded from participating in such worlds while maintaining the pseudonymous nature of the Metaverse. One possible solution could be the use of zero-knowledge proofs, as the data is controlled by the participants and thus does not get exposed in this scenario.

While designing and building the Metaverse we should consider that the Metaverse should be constituted with as few rules as possible. The same refers to the standards, the fewer standards there are the more variety will the Metaverse enable. And the variety of the real world is unprecedented and cannot be easily depicted but recreated by the human variety. The Metaverse must not restrict this variety from blooming.

4 Discussion

This work builds on the knowledge generated by scholars and technology enthusiasts in the fields of the virtual worlds, Metaverse, and distributed ledger technologies to propose a model of the possible development of the Metaverse into a decentralized space open for secure interaction and collaboration.

The proposed development follows through various steps of the evolvement of the commonly shared virtual world to assure its decentralization and security. First, it is proposed to experiment with the possible protocols and frameworks for realizing the Metaverse in blockchain-enabled environments like DAOs to explore characteristics, rules, and underlying structure of self-organizing, self-regulating, and self-governing decentralized social organizations owned by its participants.

Furthermore, the development of the ubiquitous Internet of Things network as a step towards a decentralized Metaverse is discussed and motivation for it is provided.

Finally, the framework of the Metaverse to facilitate this development path comprising three different interconnected layers is proposed. The framework utilizes state-of-the-art technologies proposed by the technology enthusiasts and scholars such as smart contracts and zero-knowledge proof protocols to introduce secure, decentralized, and privacy-preserving interaction mechanisms within the system. The framework also addresses the problem of uneven distribution of computational powers and storage resources by proposing the common pool of shared resources.

As discussed, it is crucial for the Metaverse as a space shared by the whole world to be decentralized, i.e., owned and governed by the people. The proposed model therefore assures the decentralized nature of the Metaverse at the same time not restricting other forms of governance to be utilized in the systems built in the shared space.

The most important characteristics, features, and considerations concerning the concept of the decentralized Metaverse are also outlined and motivated in the work, as well as technologies and concepts that will facilitate its development.

It is however important to note that the Metaverse cannot be defined by scholars and enthusiasts from the perspective of one field or science but will instead arise only as a result of ultimate collaboration between fields of knowledge. The same processes that enabled the emergence of astrophysics and the whole bunch of new sciences that enabled us to see a more complete picture of the universe in the 20th century will have to be repeated at an even larger scale to be able to define and develop the Metaverse. And its evolvement won't possibly stop with its emergence but will afterward proceed towards the synergy state of the real and virtual worlds.

The Metaverse is going to be a highly dynamic space interwoven with the real world. It is an unprecedented phenomenon from many points of view. The amount of data created and exchanged within it will exceed everything known

to humanity. Likely, we won't see the Metaverse coming to life in a form as imagined by its visionaries until we encounter breakthroughs in different fields in the future.

Further research must also be conducted to reflect the visions of the Metaverse of the coming generations. We should also define design principles to be considered in developing the Metaverse because as soon as it scales it won't be easy to redefine it (Nickerson et al., 2022). So, there is much work to be done before defining a ready-to-use Metaverse.

Many problems could potentially arise from a poorly designed Metaverse that would result in neglecting the real world. Environmental and societal issues arising from the introduction of such a massive project call once again for the universal participation of specialists from different fields to be able to realize this project at its full potential. Because do we need the immersive and feeling real Metaverse if it would neglect the real world?

5 Conclusion

This work elaborates a vision of the potential development of the Metaverse further into a possible scenario of its evolvement including motivation and outcomes of each step of co-existence of the real and virtual worlds. A framework is also presented that could facilitate the proposed development of the Metaverse and ensure the security and decentralization of the Metaverse. The analysis conducted builds upon the state-of-the-art accomplishments in technology and science to provide a framework realizable given the current achievements.

6 References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095

Ball, M. (2022) The Metaverse: And How it Will Revolutionize Everything. Digital edition. New York, NY Liveright Publishing Corporation, a division of W.W. Norton & Company.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and research agenda. Journal of the Association for Information Systems. https://doi.org/10.17705/1jais.00518

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: past, present, and future trends. ACM Computing Surveys, 54(8), 1–41. https://doi.org/10.1145/3471140

Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, 2018, 46. https://eprint.iacr.org/2018/046.pdf

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (Last updated 2019, February 5). Succinct non-interactive zero knowledge for a von Neumann architecture. Report, 781-796. Retieved August 8, 2023, from https://eprint.iacr.org/2013/879.pdf

Binance. (Published 2018, December 8, last edited 2023 February 1). Proof of Authority Explained. Retrieved August 3, 2023, from https://academy.binance.com/en/articles/proof-of-authority-explained

Blum, M., Feldman, P., & Micali, S. (1988). Non-Interactive Zero-Knowledge and its Applications (Extended Abstract). Symposium on the Theory of Computing, 103–112. https://doi.org/10.1145/62212.62222

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/access.2016.2566339

Dixon, C. (2021, November 19). Twitter post. Retrieved August 10, 2023, from https://twitter.com/cdixon/status/1461723922336915459

Douceur, J. R. (2002). The Sybil attack. In Lecture Notes in Computer Science (pp. 251–260). https://doi.org/10.1007/3-540-45748-8_24

DuPont, Q. (2017). Experiments in algorithmic governance. In Routledge eBooks (pp. 157–177). https://doi.org/10.4324/9781315211909-8

Epic Games. (n.d.). What is Creative mode in Fortnite? How does it work? Retrieved August 5, 2023, from https://www.epicgames.com/help/en-US/fortnite-c5719335176219/creative-c5719344003995/what-is-creative-mode-in-fortnite-how-does-it-work-a5720352367643

Ethereum Community. (Last edited 2023, July 11). Merkle Patricia Trie. Retrieved August 2, 2023, from https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie/

Ethereum Community. (Last edited 2023, August 3). Zero-knowledge proofs. Retrieved August 8, 2023, from https://ethereum.org/en/zero-knowledge-proofs/

Ferreira, A., Huynen, J., Koenig, V., & Lenzini, G. (2014). A conceptual framework to study Socio-Technical Security. In Lecture Notes in Computer Science (pp. 318–329). https://doi.org/10.1007/978-3-319-07620-1_28

Garoffolo, A., Kaidalov, D., & Oliynykov, R. (2020). Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. Technical Report. https://doi.org/10.1109/icdcs47774.2020.00161

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. STOC '85: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. https://doi.org/10.1145/22145.22178

Greenspan, G. (2015, July 19). Ending the Bitcoin vs Blockchain Debate. Retrieved August 2, 2023, from https://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/

Gürsoy, G., Brannon, C. M., & Gerstein, M. (2020). Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Medical Genomics, 13(1). https://doi.org/10.1186/s12920-020-00732-x

Hassan, S., & De Filippi, P. (2021). Decentralized Autonomous organization. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1556

Hern, A. (2018, January 17). Bitcoin's energy usage is huge – we can't afford to ignore it. Retrieved August 3, 2023 from https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

Herpy, J. (2022, March 17) Smart Contracts And The Law: What You Need To Know. Retrieved August 3, 2023, from https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/17/smart-contracts-and-the-law-what-you-need-to-know/

Hirschman, E. C. (1983). Predictors of Self-Projection, fantasy fulfillment, and escapism. Journal of Social Psychology, 120(1), 63–76. https://doi.org/10.1080/00224545.1983.9712011

Hohenberger, S., & Lysyanskaya, A. (2005). How to securely outsource cryptographic computations. In Lecture Notes in Computer Science (pp. 264–282). https://doi.org/10.1007/978-3-540-30576-7_15

Jahns, K. (Last edited 2021, August 11). The environment is Gen Z's No. 1 concern – and some companies are taking advantage of that. Retrieved August 9, 2023, from https://www.cnbc.com/2021/08/10/the-environment-is-gen-zs-no-1-concern-but-beware-of-greenwashing.html

King, S. (2013, Oktober 19). PeercoinTalk's Community Interview With Sunny King #1. Retrieved August 2, 2023, from https://talk.peercoin.net/t/peercointalks-community-interview-with-sunny-king-1-october-19-2013/1919/1

King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Technical Report. http://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

Knudsen, L. R. (2015). Dynamic encryption. Journal of Cyber Security and Mobility, 3(4), 357–370. https://doi.org/10.13052/jcsm2245-1439.341

Lamport, L., Shostak, R. E., & Pease, M. C. (1982). The Byzantine Generals problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401. https://doi.org/10.1145/357172.357176

Laya, A., Bratu, V. I., & Markendahl, J. (2013). Who is investing in machine-to-machine communications? Proceedings of 24th European Regional ITS Conference. https://www.econstor.eu/bitstream/10419/88475/1/774034017.pdf

Nabben, K. (2021a). Imagining Human-Machine Futures: blockchain-based "Decentralized autonomous organizations." Social Science Research Network. https://doi.org/10.2139/ssrn.3953623

Nabben, K. (2021b). Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology. Front. Comput. Sci., 2(599406). https://doi.org/10.3389/fcomp.2020.599406

Nabben, K. (2021c). Is a "Decentralized Autonomous Organization" a Panopticon? Algorithmic governance as creating and mitigating vulnerabilities in DAOs. Interdisciplinary Workshop on (De) Centralization in the Internet (IWCT'21). https://doi.org/10.1145/3488663.3493791

Nadella, S. (2021, May 25). Building the platform for platform creators. Retrieved August 5, 2023, from https://www.linkedin.com/pulse/building-platform-creators-satya-nadella/

Newton, C. (2021, July 22). Mark in the metaverse. Facebook's CEO on why the social network is becoming 'a metaverse company'. Retrieved August 5, 2023, from https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview

Nickerson, J. V., Seidel, S., Yepes, G., & Berente, N. (2022). Design principles for coordination in the metaverse. Proceedings - Academy of Management, 2022(1). https://doi.org/10.5465/ambpp.2022.15178abstract

Onik, M. H., Kim, C., Lee, N. Y., & Yang, J. (2019). Privacy-aware blockchain for personal data sharing and tracking. Open Computer Science, 9(1), 80–91. https://doi.org/10.1515/comp-2019-0005

Park, G. (2021, September 28). Epic Games believes the Internet is broken. This is their blueprint to fix it. Epic CEO Tim Sweeney and other executives detail their plan for the metaverse and how it differs from Facebook's vision. Retrieved August 5, 2023, from https://www.washingtonpost.com/video-games/2021/09/28/epic-fortnite-metaverse-facebook/

Principia Cybernetia. (1989). The Cybernetic Manifesto. Retrieved August 6, 2023, from http://pespmc1.vub.ac.be/MANIFESTO.html

Riabzev, M, & Ben-Sasson, E. (2019, February 5). STARK Math: The Journey Begins. Part 1. Retrieved August 8, 2023, from https://medium.com/starkware/stark-math-the-journey-begins-51bd2b063c71

Richardson, R. (2021). Defining and demystifying automated decision systems. Social Science Research Network. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3869753_code3361828.pdf?abstractid=3811708&mirid=1

Röpke, R., Kerker, N., & Stibor, A. (2021). Data transmission by quantum matter wave modulation. New Journal of Physics, 23(2), 023038. https://doi.org/10.1088/1367-2630/abe15f

Seidel, S., Berente, N., Nickerson, J. V., & Yepes, G. (2022). Designing the Metaverse. Proceedings of the 55th Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2022.811

Sobti, R., & Ganesan, G. (2012). Cryptographic Hash Functions: A Review. IJCSI International Journal of Computer Science Issues, 9(2), 2. http://ijcsi.org/papers/IJCSI-9-2-2-461-479.pdf

Szabo, N. (1994). Smart Contracts. Retrieved August 2, 2023, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys and Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/comst.2016.2535718

Wood, G. (2015) PoA Private Chains. Retrieved August 3, 2023, from https://github.com/ethereum/guide/blob/master/poa.md

Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., Kiayias, A., & Knottenbelt, W. J. (2019). SOK: Communication across distributed ledgers. IACR Cryptology ePrint Archive, 2019, 1128. https://dblp.uni-trier.de/db/journals/iacr/iacr2019.html#ZamyatinAZKMKK19

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32. https://doi.org/10.1109/jiot.2014.2306328

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE CS Security and Privacy Workshops. https://doi.org/10.1109/spw.2015.27