The Future of The Metaverse

Creating Policies and Regulations for a Metaverse Built on a Blockchain

M.Sc. Engineering and Policy Analysis

Baris E. Yakali

Delft University of Technology

The Future of The Metaverse

Creating Policies and Regulations for a Metaverse Built on a Blockchain

by

Baris E. Yakali

Student Number:	4577078
Project Duration:	February, 2022 - August, 2022
Chair:	Marijn Janssen
First Supervisor:	Zenlin Roosenboom-Kwee
Second Supervisor:	Marijn Janssen
Place:	Faculty of Technology, Policy and Management, Delft

TUDelft

Preface

This thesis focuses on creating policies and regulations for a metaverse that is built on a blockchain. It is part of the M.Sc. program Engineering and Policy Analysis at the Delft University of Technology. I have been involved with the thesis from January to August of 2022.

Although the first time I heard about Bitcoin was in 2015, when a friend and I were exploring new technological innovations in the world, it was not until 2017 when I was genuinely interested in the technology. At this point, I was actively using blockchain technology and researching new projects to see what type of innovations they were bringing into the world as implemented in their new blockchains. Over the years, I have learned more about how blockchains work, the technology behind them and the type of applications that developers can build on blockchains.

The metaverse, however, is a much more recent interest of mine, as the development of the metaverse itself is also newer than blockchain technology itself. I would like to believe that my first interaction in the metaverse was when a good friend of mine loaned me his Oculus Rift virtual reality headset. This headset has a built-in game called ’Oculus Rooms and Parties’, where one can join and open lobby and interact with others. Even though the idea and execution were basic, it is essentially a metaverse where you can interact with other real people and play games with them.

Combining these two ideas, at least to me, would make ’the perfect’ metaverse, where no central authority controls the space, developers are free to build what they want, and users can jump from one metaverse to another. However, like anything in the world, nothing is perfect and there must be some regulations to make sure the space is safe for everyone, and people will not get scammed, but rather enjoy the space itself. This is when the idea of turning this idea into a thesis originated and I believed it worked out.

I would like to thank my two supervisors: Marijn Janssen and Zenlin Kwee for guiding me throughout this process and offering me their support and expertise. I also want to thank the interviewees who have shared their knowledge with me both in the blockchain domain, as well as the policy domain. I would also like to thank my family, friends and colleagues who have supported me from beginning to end. A special thanks to all the people that have stuck with me since the beginning of my bachelor’s degree.

With that being said, I truly hope that this thesis provides you with new insights on the metaverse, the technologies it can be built on and regulation/policies that could be implemented in the metaverse. I believe that the world will keep shifting to a more online environment, where the metaverse would be a medium in which meetings and events will be held.

Baris E. Yakali
Delft, August 2022

Summary

Blockchain is still a new development that must still undergo mass adoption for both businesses and users. There are already many applications built on blockchain, such as decentralized finance and marketplaces for non-fungible tokens (NFTs). With the recent increase in interest in NFTs, many companies have turned towards creating a ’metaverse’ around the NFTs for people to view them as more than just the picture alone, meetings and events, such as festivals can also be held in a metaverse. With the growth, many users will join the metaverse and a lot of wealth is expected to be transferred to it. For this to happen in a coerced manner, there must be some regulations and/or policies that ensure that the users and their data are protected. Additionally, blockchain might not be the best technology to build this digital world on, and thus a comparison between blockchain and cloud computing (CC) can perhaps find a better alternative and uncover the shortcomings of the technology. This will be done by discussing both (CC) and blockchain with respect to running a metaverse on them, which will be concluded by a comparison table for various aspects of the metaverse. Interviews will then be conducted with experts on both the policy and technical side to find out what they think should be regulated first out of 9 aspects of the metaverse and how they would do it. Taking all these interviews into consideration, a final list of most essential elements of the metaverse will be given together with how a regulatory framework and/or policy could potentially solve this.

The purpose of this research is to figure out what aspects of the metaverse should be focused on in terms of regulations and policy making. Most of the current studies that focus on blockchain simply mention that ’it should be regulated’ but provide little to no information on what they think should be regulated. The metaverse has even less studies done on it, with all the studies concluding the same as the studied for blockchain: ’it should be regulated’. This thesis will take that foundation and essentially go past that and suggest a few key areas that regulators should/could focus on for the first few regulatory frameworks. This will also aid future studies as they can use this thesis as a foundation and expand upon it in many different directions.

As mentioned before, the metaverse is a space that is likely going to grow significantly in the next couple of years. With this influx of users and money into the space, there are bound to be some individuals that will take advantage of others. For this reason, as well as others, such as building strong and reliable metaverses, ensuring user data is safe and solving IP rights issues, the research is extremely relevant for the modern day and near future. The relevance exceeds the societal perspective and extends to the academic perspective as well, allowing future researchers to use this thesis as a foundation for further exploratory studies.

For the first few chapters, the main methods that were used were a literature review and additional desk research. This was done to answer the first three sub-questions. Desk research goes past literature reviews and looks at other materials, such as information on blockchain costs, which have not been published as scientific articles. The last chapter, however, makes use of interviews to answer its sub-question. The interviewees were grouped into 3 categories: blockchain, cloud computing and policy advisor/analyst. The combination of these 3 categories allowed for multiple perspectives to be taken into consideration while aiming to answer the research question. The interviewees were asked to rank potential aspects of the metaverse that could be regulated, which was then used in the thesis itself.

Before going into the policy aspect, the results on the technical part must be discussed first. Although the thesis title mentions regulations for a metaverse on a blockchain, the comparison between blockchain and cloud computing found that there are some advantages of having parts of the metaverse run on the cloud, rather than on blockchain. Blockchain is making progress in these areas and keeps improving itself, but for the time being it is not ripe yet. Policy makers should keep this mind when creating new regulations/policies, so that their efforts are not for nothing. As for the regulations themselves,

when looking at the final rankings of all the interviewees, the following aspects are most important: data privacy, intellectual property and governance & legal documentation. The first are relatively self explanatory and the last one refers to descriptions of the technology and code given by developers and creators. However, this ranking is likely a reflection of the knowledge of the interviewees themselves, and all regulations in this space should be taken seriously.

The proposed regulations and policies were designed in such a way that they do not hinder the technology itself. This was a big worry for interviewees from the technical side and was understood by the policy interviewees as well. This harmony between the two groups that have different interest is a great example of why blockchain technology will keep developing and improving. For the data privacy, it is likely that an extra layer of encryption is needed before uploading data to the main chain. The IP rights of NFT holders should be very clearly outlines with what is and what is not allowed. NFTs can even be grouped into different categories to make different rules for an NFT representing a pet and one representing virtual land. For the last aspect, governance & legal documentation, a policy is proposed that would require developers to have a minimum number of comments and annotations to the code per line of code. While in this scenario it could take developers a longer time to develop certain projects, they will understand others' projects much faster and also be able to pick up old projects much quicker.

Contents

Nomenclature

Abbreviations

Abbreviation	Definition
AWS	Amazon Web Services
CC	Cloud Computer
CFTC	Commodity Futures Trading Commission
DAO	decentralized autonomous organization
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DOB	Date of Birth
DORA	Digital Operational Resilience Act
DP	Data Privacy
EC	European Commission
ECB	European Central Bank
EMD2	Electronic Money Directive
EU	European Union
FinCEN	Financial Crimes Enforcement Network
GB	Gigabyte
GDPR	General Data Protection Regulation
GLD	Governance & Legal Documentation
IAAS	Infrastructure as a Service
ICP	The Internet Computer
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
kWh	kilo Watt hour

Abbreviation	Definition
KYC	Know Your Customer
LB	Liability
MiCA	Market in Crypto-Assets
MiFID	Markets in Financial Instruments Directive
NFT	Non-Fungible Token
NNS	Network Nervous System
OECD	Organization for Economic Cooperation and Development
OS	Operating System
PAAS	Platform as a Service
PoH	Proof-of-History
PoS	Proof-of-Stake
PoW	Proof-of-Work
R&D	Research and Development
RoC	Regulations of Conduct
SAAS	Storage As a Service
SC	Smart Contract
SDR	Special Drawing Rights
SEC	U.S. Securities and Exchange Commission
TPS	Transactions per Second
TWh	Terra Watt hour
UN	United Nations
VAT	Virtual Asset Taxes
VM	Virtual Machine
WWW	World Wide Web
XAAS	X As a Service

List of Figures

List of Tables

1

Introduction

1.1. Research Background

The metaverse is a new space that allows for more intimate connections to be formed in an online world. Essentially, it enhances the online experience that one might get from a Zoom call or while playing a game. As it is still a new space, developers and users are unsure what the path of the metaverse will be and how well it will be integrated into society as well as its user base. However, as the metaverse mimics the characteristics of the real world, there must be certain policies and regulations that will ensure that this space does not get out of hand and is a safe place for all age groups. Unfortunately, there are currently no regulations or policies for this space in the EU-zone with no concrete plans to create them in the near future either. One of the aspects that makes it more complicated is that they are being built on blockchains, which is still considered to be a modern technology and, like the metaverse, has no strict regulations either in the EU. The most up-to-date regulation from the European Union (EU) is the Markets in Crypto Assets (MiCA) bill, which mostly addresses cryptocurrency scams, rug-pulls and pump and dumps, rather than address the technical features of blockchain.

The metaverse is an extraordinarily complex project and essentially a replica of the real world that everyone lives in today. There are many elements that are transferred from the real world to the metaverse, such as buying and selling real estate, pieces of art, concerts and games that can be played. This makes the space complex and includes many stakeholders from a variety of different fields, including: blockchain engineers, policy analysts, users, developers, regulators and law enforcers. Moreover, since it is borderless, there must be new policies and regulations set that account for the decentralized and borderless characteristic of blockchain. It could be argued that all the laws that exist for the material world must be recreated and translated to fit into the metaverse.

This makes the metaverse more ambiguous in terms of its future and potential policies and regulations that the EU might or should impose on the metaverse. This thesis will therefore investigate regulations within the EU regarding this landscape, as well as look into the technology behind it. At the end, a recommendation will be made to policy makers on what they should focus on to address potential issues with the space and the technology behind it.

1.2. State of the Art

1.2.1. Metaverse

The Metaverse, as defined by Bobrowsky & Needleman (2021), is an extensive online world where people interact via digital avatars. The term *metaverse* was originally coined in the book 'Snow Crash' by Neal Stephenson in 1992, where he referred to it as a 3-dimensional virtual world, which is inhabited by avatars of real people (Stephenson, 1992). When looking at Facebook's definition of The Metaverse, who are at the forefront of developing it, they say that ”The 'Metaverse' is a set of virtual spaces where one can explore and create with others who are not in the same physical space (Bosworth & Clegg, 2021).” According to several sources, the metaverse is expected to change several aspects of society, most notably of which are business-oriented activities and gaming (Hackl, 2020; Bayse, 2021; Lambden, 2021).

The COVID-19 pandemic has undoubtedly accelerated the shift to a more online environment for individuals, businesses and education (Fawns et al., 2020; Mahmood, 2021). The metaverse could be the solution for a more interactive and engaging online world with enhanced experiences for the users (Swilley, 2016; Du et al., 2021; Bourlakis et al., 2009).

1.2.2. Traditional Hosting Technology

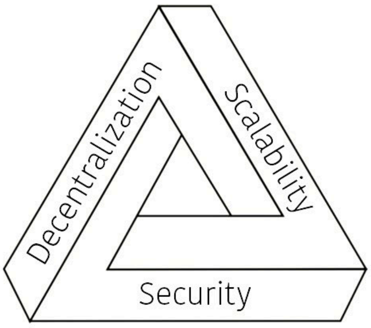
The metaverse can be built on blockchain, but could also be built on traditional hosting technology, such as cloud computers (CCs). CCs are essentially a distributed computing system, where users can use services such as: storage, analytics and software (Jena, 2020). One of the biggest players in this industry is Amazon Web Services (AWS), which controls about 32% of the total cloud computing market (Kumar, 2022).

The main purpose of cloud computing is to provide easy and scalable access to computing systems to individuals and organizations that need IT services (Chai & Bigelow, 2021). With this model, users can dictate how much hardware they need for a given period and run their programs on these computing systems, also known as 'the cloud'. This hardware is case specific and has a lot of dimensions to it. For example, one might just want to store some data on the cloud, in which case they only need to buy some storage, which can range from Gigabytes to Terabytes. On the other hand, one might need to run a python model, requiring many CPU cores, an adequate amount of RAM and some storage space to save the data as well. These are all customizable features that users of CC can tailor for themselves. Although it might be difficult to pinpoint exactly how much one needs at first, in most cases one can change this later in the process. There are in total 3 service models that CC make use of: software as a service, platform as a service and infrastructure as a service. customers can choose which one they wish to use and tailor the hardware for their specific requirements.

1.2.3. Blockchain

The first true blockchain that was used widely was bitcoin, which was created by an anonymous author, who goes by the name of Satoshi Nakamoto (Kay, 2021). Bitcoin was the first blockchain to solve the double-spending problem and has since been the most valuable cryptocurrency in the world (Nakamoto, 2008; Haar, 2021). Blockchain is a distributed ledger, with participants around the world contributing to it. The blocks are validated through cryptographic hash functions, such as SHA-256, which is used as the sole hash function for bitcoin (Nofer et al., 2017; Nakamoto, 2008). Moreover, all transactions that are made on a public blockchain are public for everyone to see (Nofer et al., 2017). The most important note there is that not every blockchain is completely permissionless - posting all the transaction for the public to see. One notable example of such a blockchain is Monero, which has untraceable transactions that can only be accessed if the necessary keys are provided (Saberhagen, 2013). There are several types of algorithms that blockchains utilize. The first one of those, which is what Bitcoin is based on, is Proof-of-Work (PoW) (Nakamoto, 2008). The next algorithm, which has both advantages and disadvantages regarding PoW, is Proof-of-Stake (PoS) (Cointelegraph, 2017). Since then, there have been even more variations, such as Solana's Proof-of-History (PoH) and The Internet Computer's chain-key cryptography (Solana, 2021; Dfinity, 2021). Each of these have their own benefits and drawbacks when it comes to *The Impossible Triangle*, which focuses on the three main aspects of a blockchain: security, scalability and decentralization, which is visualized in figure 1.1 (Jia, 2014; BTSE, 2021). This triangle originated in 2014 with security, decentralization and environment-friendly on its edges. However, Vitalik Buterin has adopted this and replaced environment-friendly with scalability, which has now been adopted as the standard (BTSE, 2021). Essentially, this triangle shows the trade-offs that blockchains must make when designing a consensus mechanism, where one of the edges is always compromised for the other two. In the case of bitcoin for example, the network is highly decentralized and secure, but not scalable. Ethereum 2.0 is trying to fix that scalability issue by giving up some level of decentralization and while maintaining security. This is how the triangle can be applied to real world blockchain consensus mechanisms.

Figure 1.1: The impossible triangle reiterated by Vitalik Buterin as presented in BTSE (2021).



Besides consensus mechanisms, there are also generations of blockchains. Generally speaking, there are three generations of blockchains: digital currency, digital economy, and digital society, with each generation building on the ealier one (Efanov & Roschin, 2018). With most blockchains, anyone can create a wallet to send and receive coins and tokens. The second generation blockchains introduced the functionality of smart contracts, with Ethereum being one of the first and biggest networks to do so (Efanov & Roschin, 2018; Buterin, 2013b). The third generation builds even further on this and enables a vast array of applications, such as: identity, education, governance and many aspects of communication and culture.

For the purpose of this thesis, the focus will be laid on permissionless blockchains, as they allow any developer to build and launch applications on the blockchain and anyone can interact with the network as they please (Miller, 2019; Lichtigstein, 2020). One does not need special identification or to verify themselves in order to do so. These types of blockchains are the most known blockchains, including Bitcoin and Ethereum. While most blockchains are permissionless, there are only a handful of blockchains that have large teams and allow computations to be done on the blockchain network. This is one of the core aspects of this thesis, as it is expected that anyone can build the metaverse and build feature and/or additions to the metaverse. One example of a blockchain that can do this is The Internet Computer (ICP). Besides being a blockchain with many functionalities and developments, it makes for a fitting example to compare to cloud computing, as it has many similarities when it comes to the technology and computing. Developers can run their smart contracts on-chain to do real-time computations on the ICP blockchain. Since the direct comparison will be with cloud computing, it is crucial to have a blockchain that has the ability to perform computation on-chain, allowing for a potential metaverse to be built completely on one blockchain.

1.2.4. NFTs, DAOs and DeFi

There are several other technologies that blockchain technology enables, namely: Non-Fungible Tokens (NFTs), Decentralized Autonomous Organizations (DAOs) and Decentralized Finance (DeFi). All these three developments can live in harmony on a blockchain and complement one another.

NFTs represent true ownership of a digital asset (J. Fairfield, 2021). In the current market, this technology is mainly used to buy and sell art pieces on platforms like OpenSea, which has seen tremendous growth over the past few years, perhaps even growing too fast (Clifford & Mathews, 2022).

A DAO is a decentralized organization which is represented by rules encoded as a computer program and is: transparent, controlled by the members of the organization and cannot be influenced by a central government (Prusty, 2017; Chohan, 2017). One of such a DAO is integrated into the ICP blockchain, where users can vote on governance proposal and decide what upgrades to bring to the network and which ones to leave out (Conwell, 2021).

DeFi, which enables decentralized exchanges (DEXs) have evolved the space and essentially eliminate the need for centralized exchange to exist for trading cryptocurrencies. On a DEX, people can trade their tokens for other tokens and easily exchange them. The main current limitation of a DEX is that there is limited support for cross-chain currency swaps and high gas fees, but this will soon be a limit of the past.

Each of these concepts will be explored in more detail in chapter 3, together with its linkage to blockchain and the metaverse, and the impacts it can have on potential regulations.

1.2.5. Difficulties and Challenges

The metaverse comes with huge challenges from multiple perspectives such as: cybersecurity, payment systems, laws, regulations and many more (Dzyuba & Rohi, 2021). This is where recent advancement in blockchain technology can play a huge role. The Dfinity Foundation, founded by Dominic Williams, has created a blockchain called *The Internet Computer*, which is an advanced blockchain that functions and web-speed and can scale without bound (D. Williams, 2020, 2017). Although the statements from Dominic Williams about scaling without bound is optimistic, the technology behind it does prove sufficient. If this technology were to hold true, the blockchain could scale its network with its user base and facilitate the metaverse, where current technological solutions might be limited in doing so like AWS (Hines, 2021). Hosting the metaverse on a blockchain instead of cloud computers like AWS comes with both benefits and drawbacks. Some of the benefits are around cybersecurity and additional features, such as NFTs, yet it depends on a case-by-case basis (S. Singh & Singh, 2016; Demirkan et al., 2020; P. J. Taylor et al., 2020). These concepts, along with several others, are important aspects to consider when making a full-fledged metaverse on the blockchain. However, the concept has not been explored in much detail, and other perspectives are usually not considered when developing such a digital environment. Therefore, this research will focus on how The Internet Computer can best implement aspects from the metaverse, while tackling the current challenges faced by the metaverse and taking the multiple perspectives into account.

Additionally, besides hosting the whole metaverse on a single blockchain, there is also the possibility that multiple blockchain can each host a single part of the metaverse, which are then connected by cross-chain bridges (Bahga & Madisetti, 2016). At first glance, the benefit of this would be that there is no single point-of-failure, which might be the case if everything is hosted on one blockchain. However, the downside would be that there are now multiple, smaller, points-of-failure. While the former case is yet to be investigated, the latter has happened multiple times, the most recent case of which is the Solana wormhole hack, where hackers walked away with $320 million due to exploitation of its source code (Sigalos, 2022).

1.3. Research Objective

Creating the metaverse is a big challenge with many aspects that must be taken into account. The following problem statement has therefore been formulated:

> The metaverse is expected to change the landscape of digital interaction and has many elements to it, it must therefore be closely regulated with policies and regulations in a manner that it will adhere to the EU, while not limiting its potential.

This problem statement takes the location of the metaverse into account, which is significant since its geographical location determines which regulations it must adhere to.

1.3.1. Research Questions

There is one core research question, which is aided by 4 sub-questions. The sub-questions will help build up to the core research question and answer it in the end. The main research question for the paper has been formulated as follows:

> What are the main technological factors that must be taken into consideration for policy makers in the EU to create new regulations and policies for a decentralized metaverse?

In order to answer the main research question, several sub-questions will be formulated which will aid in steering the thesis and building up the required information step by step. With this being said, the first step is to uncover current policies and regulations around the world surrounding the space - blockchain and decentralized metaverse. As policies can be different from one country to another, there might be cases where policies are already set in place that are effective at what they do, or less so. Either way, it will shine light on what is currently going on around the world and in similar markets, and ultimately help in answering the main research question. The following question has been formulated for answering this:

1. What are the current policies and regulations in the EU that are associated with blockchain and the metaverse?

The second step is to investigate the current centralized version of a metaverse and challenges it has that stem from it being centralized. This will help identify possible weaknesses and strengths of using a type of technology for building a metaverse and explore the technological landscape. Traditional technology is defined as cloud computing for the purpose of this thesis. The following sub-question has been formulated from this:

2. What are the main technical challenges currently faced by the current technology (i.e., cloud computing)?

The third sub-question is strongly related to the second sub-question and will go over the advantages and disadvantages of building a metaverse on a decentralized platform versus a centralized one. This question will expand on the second one and start integrating the concept of blockchain to the metaverse and its potential. This leads to the third sub-question:

3. What are the benefits and drawbacks of hosting the metaverse on a blockchain compared to the current technology?

These previous two questions will help illustrate why blockchain would be a better choice than traditional centralized systems in building a metaverse, as well as explaining some of the concepts that are needed to formulate policies. These two questions will be answered by exploring the technological landscape and gathering opinions from industry experts to formulate an accurate conclusion.

The last step will be to bring the previous three steps together and look at future possibilities of the metaverse in the EU. While doing this, it must conform to the regulations within the EU and in turn, the EU must ensure not to limit the possibilities of the industry. From this, the fourth and final sub-question has been created:

4. Considering future development of a blockchain based metaverse, what should policy makers do in order to regulate the space while not limiting its development?

All the above-stated sub-questions aim to aid in answering the main research question. Answers to each of the sub-questions will be given at the end of each chapter and a summarized version will be provided at the end of the thesis.

1.4. Research Flow

The flow of the research is essentially in which order the questions are answered, what the purpose of each chapter is and where the answers to the sub-questions can be found. Figure 1.2 illustrates this along with the types of data that will be collected for each of the sub-questions.

Figure 1.2: Research flow diagram of the thesis

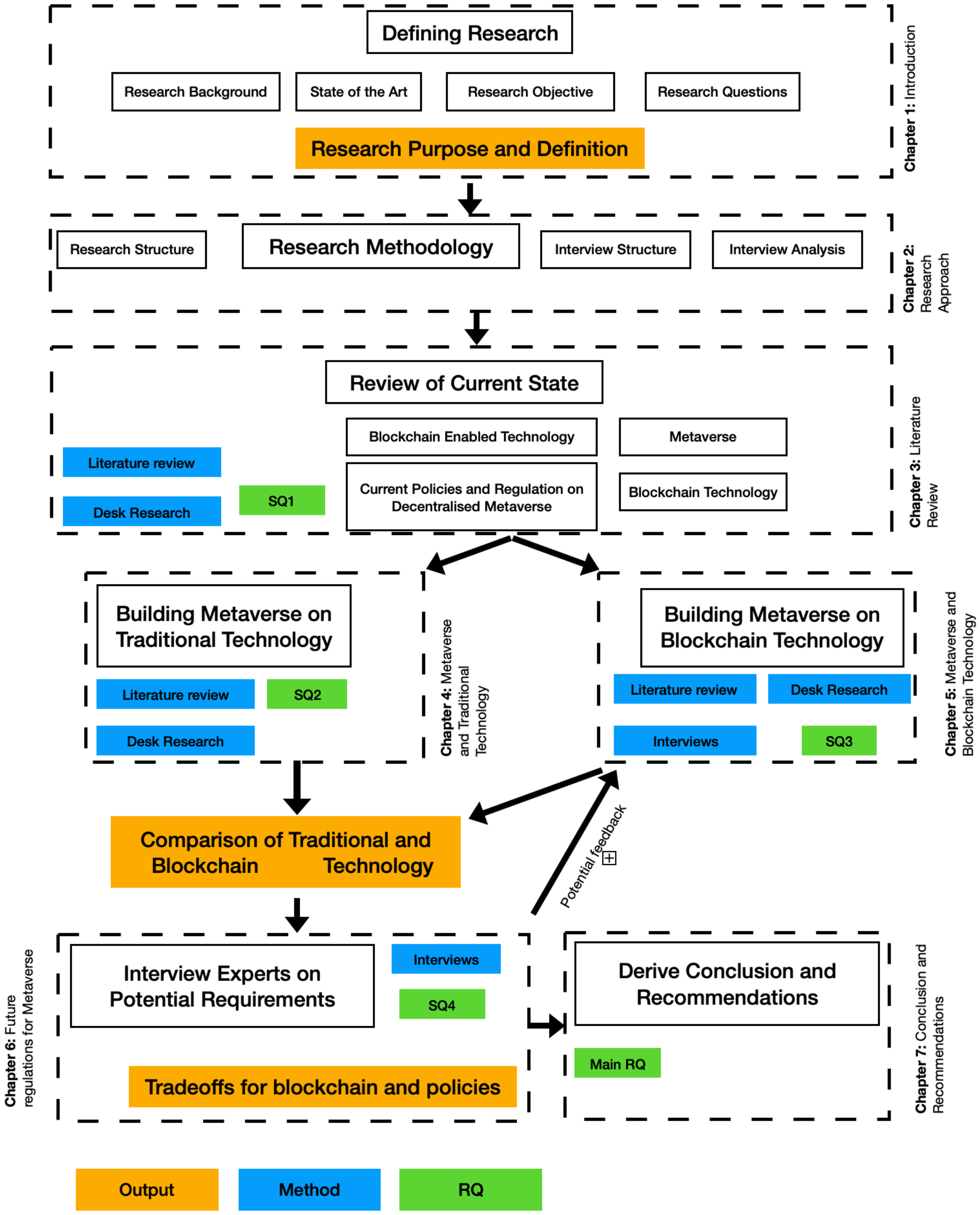

Defining Research
Research Background
State of the Art
Research Objective
Research Questions
Research Purpose and Definition
Chapter 1: Introduction
Research Structure
Research Methodology
Interview Structure
Interview Analysis
Chapter 2: Research Approach
Review of Current State
Blockchain Enabled Technology
Metaverse
Literature review
Desk Research
SQ1
Current Policies and Regulation on Decentralised Metaverse
Blockchain Technology
Chapter 3: Literature Review
Building Metaverse on Traditional Technology
Literature review
SQ2
Desk Research
Chapter 4: Metaverse and Traditional Technology
Building Metaverse on Blockchain Technology
Literature review
Desk Research
Interviews
SQ3
Chapter 5: Metaverse and Blockchain Technology
Comparison of Traditional and Blockchain Technology
Potential feedback
Chapter 6: Future regulations for Metaverse
Interview Experts on Potential Requirements
Interviews
SQ4
Tradeoffs for blockchain and policies
Derive Conclusion and Recommendations
Main RQ
Chapter 7: Conclusion and Recommendations
Output
Method
RQ

Figure 1.2 has 3 labels: output, method and research question. The outputs are given whenever a significant output is also used for the following chapter. Methods are further divided into 3 groups: literature review, desk research and interviews. The literature review looks specifically at the scientific articles, papers or books published on the topic. Desk research refers to any type of secondary data that will be obtained. This can also be through non-scientific articles, such as other users that have used a blockchain or a blockchain organization releasing information about the network. Interviews will be used towards the end and are relatively self-explanatory. The last category, research questions, illustrates which research question will be answered in which chapter.

The first chapter is an introductory chapter that discusses the core ideas and makes the reader known with the relevant topics. The background, objective and questions of the research are first introduced here as well as the state of the art of the technology that will be discussed. There is one core research question which is aided by four sub-questions which are meant to build up to the core research question. The outcome of this chapter is the research purpose and definition.

The second chapter elaborates more on the research approach of the thesis, as well as the interview structure. The first thing elaborated on in this chapter is the design and methodology of the research. Hereafter, the interview structure, as well as the profiles of all the interviewees are given. This will help create a better understanding of what to expect from this part before going into the analysis.

The third chapter is a literature review of the current available technologies. In this chapter, literature on blockchain, traditional technology and the metaverse will be analyzed, which will lay a foundation for the following chapters and sub-questions. Another aspect that will be elaborated on in this chapter is the current policies and regulations regarding a decentralized metaverse. This addresses the first sub-question and will thus be answered in the literature review. The answer can be found towards the end of the chapter with a summary in the conclusion of the literature review.

From here on, the research technically splits into two parts, the first part of those is the fourth chapter, where building a metaverse on traditional technology will be discussed. Traditional technology in this thesis will be defined as cloud computing technology. This chapter will uncover some of the technical aspects of building the metaverse on this type of technology and will be used to compare it to blockchain technology in the following chapter. This will be done with the help of certain criteria that are crucial to building a metaverse and all the elements that go into it.

The second part of this two-part chapter, which is chapter five, is building a metaverse on blockchain technology. It will discuss the same points that are discussed in chapter four, but on blockchain technology, and make a comparative table between the two technologies at the end. Additionally, the opinions of industry experts from both sides will be asked, which will justify the comparative table and add extra validity to it. The outcome of this table will be used as a foundation for the last chapter.

The sixth chapter will tie everything together and look at future policies and regulations that should be focused on. The goal is to create a table with trade-offs that policies and regulations will have to make to regulate the space. The previous two chapters will have built the necessary technological foundation to understand it and create regulations around it. The way this will be done is by using the previous chapters and the industry experts from a variety of stakeholders in the landscape.

The last chapter will primarily answer the main research question that is at the center of the whole thesis. The answer will include a recommendation to policy makers in the EU to regulate a decentralized blockchain in the future. On top of this, the information could also be used for blockchain companies to assess potential regulations that might arise in the future and act accordingly. Moreover, it will conclude the whole report, discuss it and elaborate on potential future research that can be done on the topic.

2 Research Approach

This research will aim to come to an understanding of the policy and regulations of building the metaverse on both a centralized and decentralized system. More specifically, it will look into the possibilities of creating it on the blockchain. Since it encompasses both the policy and technological aspect of the landscape, it is vital that the research approach is appropriate for both of these perspectives. The former aspect is more concerned with qualitative data, looking at similar policies in other jurisdictions as well as consulting with experts on what the future might bring. On the other hand, technological aspects are more quantitative and regard the speed of certain systems, as well as costs. However, there will likely be some qualitative data as well, as usability and perspective of the users also contribute to the adoption of technologies.

The research approach must therefore fit both the criteria of qualitative and quantitative data, as well as include primary and secondary sources of data. For this reason, the **mixed-methods approach** is best suited, as it combines the two data types into one research.

2.1. Research Design & Methodology

As each sub-question investigates various aspects, they will all have a different approach as to what type of data will be collected and the way it is collected. This being said, there are some questions that will need similar data gathering to one another and therefore can use similar methods. Moreover, a panel of industry experts on both the technological and policy aspects will be formed, which will help to form a deeper understanding of both the perspectives and give an expert's view on the topic.

Sub-question one makes use of qualitative data and looks into the current policies and regulations on blockchain and metaverse within the EU. More specifically, it will aim to understand the current landscape of the policies in and around the EU, which will form a basis for the subsequent research questions. This chapter must be executed thoroughly in order to build a strong foundation for all of the following chapters.

Sub-question two looks at the challenges that traditional technology faces when it comes to building the metaverse. This will require an in-depth overview of the technology as well as the metaverse and create a deeper understanding of each of them. Most of the gathered data in this chapter will be quantitative, as it will refer to the capabilities of the technology and vastness of the metaverse. The result of this chapter will be to figure out the most critical points on traditional technology and create a list of the biggest challenges that are in its way.

The third sub-question will look at the list generated by the first sub-question and quantify the benefits and drawbacks of blockchain technology when it comes to these challenging points of traditional technology. This will again require quantitative data to compare the two technologies for each of the points to see if blockchain performs better in that aspect.

The last sub-question will aim to combine the previous question and formulated policies that will guide the space into a regulated future. Regardless of the findings, there will be trade-offs when it comes to this, as both regulations and policies are naturally limiting certain aspects of development and/or usage. Interviewees will be presented with a set of potential aspects of the metaverse that can be regulated. Their opinions on the matter will then be gathered, which will be used to identify the most crucial aspects of the metaverse. This chapter will mostly include qualitative research as well as interviews, and it is mainly concerned with creating policies and regulations for a decentralized metaverse built in the EU.

With all of the sub-questions, extensive desk research will be conducted, as well as interviews. The main limitation here is the interviews, which must be standardized to a certain degree. This will help get some quantitative numbers out of the interviews, making it easier to draw conclusions from them. Figure 1.2 illustrates the manner in which the sub-questions are structured, what data they need, and in which order they will be present.

2.2. Interviews

Regarding the interviews, there are several aspects that must be considered and pre-determined, these are: the interviewee profiles and the structure of the interviews.

2.2.1. Interview Profiles

As for the profiles of the interviewees, there will be three main categories of industry experts that must be interviewed: blockchain experts, cloud computing experts, and policy makers or regulators. The reason for the first two groups is to get a better understanding of the difference between the two technologies to answer sub-question 3. The end of this chapter will represent a table with the core differences between the two technologies to which the interviews will add more validity. The last profile is for finding the right balance between trade-offs for policies and the technology. The list of interview profiles can be seen in table 2.1. From this table, one can see that there are interviewees from many different backgrounds, namely: blockchain, cloud computing and policy analysts/regulators. There will therefore also be three different set of questions, as the interviewees that are more technologically oriented will have questions about the technical differences between blockchain and cloud computing. On the other hand, the interviewees that are in the policy/regulations domain will be asked more specific questions regarding the current, future and potential policies that could surround a new decentralized metaverse.

2.2.2. Interview Structure

There are two possibilities when conducting interviews: structured and semi-structured. For the purpose of this thesis, the structure of the interviews will be created in a semi-structured manner. This will allow for input from the experts in case any details were missed or not addressed previously. Additionally, it will give the opportunity to present ideas from both sides and steer the interviewees in the right direction in case the topic is starting to shift. This is of particular interest when asking questions about the end of chapter 5, which will see the key difference presented between cloud computing and blockchain. The interviewees will not be initially presented with this information when asked about it, as it is possible to create a bias in the mind of the experts and could limit the answer possibilities from them. Therefore, a more general question regarding the topic will be asked, which can then be steered in the direction of more specific topics later on. The specific questions can be seen in Appendix A.1

Towards the end, the interviewees will be presented with a table that illustrates 9 potential regulations in the metaverse, which are discussed in chapter 3.2.2. After asking which regulations the interviewees think apply or not, they are asked to rank the top 3 most important regulations in their opinion for the metaverse. The same 9 categories will be asked to all 3 sub-groups that are interviewed.

Table 2.1: List of interviewees with their background and expertise that will be interviewed later on in the thesis.

#	Background	Expertise	Years Experience	Function
1	Academia/Industry	Cryptography	5	Cryptography expert
2	Industry	Blockchain Protocol Engineer	5	Blockchain network developer
3	Industry	CC Application & Blockchain Enthusiast	27	Senior Director Product Development
4	Industry/Academia	Blockchain Regulator	8	Financial strategist, Xreg Consulting
5	Industry	Senior Policy Advisor	4	Secretary General of Blockchain for Europe
6	Industry/Academia	Blockchain Policy Strategy	15	Head Chair, Israeli Information Technology Chamber

2.2.3. Interview Analysis

The analysis of the interview will have 2 main parts to it: quantitative and qualitative. The quantitative part will focus more on the previously mentioned 9 categories and how they have ranked in the end and within each group. On the other hand, the qualitative part will look more into what was said during the interviews from the perspective of the interviewee and try to uncover more information from it.

As for the quantitative part, the starting point is the top 3 of all the participants for the 9 rankings. For each interviewee, the number 1 pick gets 3 points, the rank in second place gets 2 points and the rank in third place gets 1 point. In the end, all the values for all the categories will be added up, which will yield 1 (or more) category(-ies) that will be in the first, second and third position. While an emphasis will be placed on the overall top 3, the qualitative analysis will cover the others as well.

As for the qualitative part, rather than looking at the rankings themselves, some of the answers given throughout the rest of the interview will be analyzed. This can for example help determine where the perspectives, expertise and priorities lie of each one of the participants.

3 Literature review

While chapter 1.2 focused on the current state of the technology, this chapter will look more into scientific articles on the matter. Moreover, it will aim to combine both the technological and non-technological landscape and will build on this foundation for the coming chapters. The structure of this chapter is divided into 2 main parts: technology and policy. The former part will first discuss the metaverse itself, followed by traditional technology and then blockchain technology. The latter part will discuss all the relevant policies that currently exist within the EU on the landscape. The research questions in 1.3.1 have been formulated in iterations with this chapter.

3.1. The Technology

3.1.1. Metaverse

The term ”metaverse” was first coined in 1992 by Neil Stephenson in his fiction novel *Snow Crash*, in which he described a virtual reality space that was accessed through virtual reality goggles (Stephenson, 2003). Ever since this (fictional) cyberspace was first mentioned, many technological developments throughout the decades have slowly turned this idea into reality. As the metaverse kept evolving, a wide range of different definitions have also emerged throughout the years. A study conducted by Park & Kim (2022), analyzed 260 academic papers and focused on the definitions and corresponding viewpoints that define the metaverse. Consequently, the following definition from (Mystakidis, 2022) is adopted for this research, as it is deemed to be an extensive definition that encapsulates the core concepts of the metaverse, and will be used as a reference point throughout the research paper:

> *"The Metaverse is the post-reality universe, a perpetual and persistent multi-user environment merging physical reality with digital virtuality. It is based on the convergence of technologies that enable multisensory interactions with virtual environments, digital objects and people".*

It is important to note that the metaverse is considered by many to be a crucial part of the next phase of the evolution of the web/internet (Austin, 2021). This new generation is referred to as Web 3.0 or the Spatial Web, and is expected to fundamentally change the way humans interact with the digital world (Cook et al., 2020). Blockchain is referred to as one of the key driving forces behind this next generation of the internet, as it completely transforms the data structures in the backend of the web by writing smart contracts of the applications and deploying them on the decentralized platforms (Kasireddy, 2021; Geroni, 2021). The Web 3.0 blockchain market is projected to grow exponentially by 2030 (MRFR, 2022), and the estimations for the value of the metaverse lie between 1 to 8 trillion US dollars by the end of the decade (Canorea, 2021; Holmes, 2021; Swartz, 2021). Due to this huge potential, the metaverse has attracted paramount attention. Facebook, the parent company of Facebook, Instagram and WhatsApp, among other subsidiaries (Reiff, 2021), had recently changed its name to Meta in October 2021 (Meta, 2021), and expects to invest over 10 billion US dollars on a yearly basis in its metaverse project (Brown, 2021). Microsoft is also slowly stepping foot in this industry by rolling out Mesh, which aims to bring immersive meetings to its cloud-based collaboration platform Teams (Harford, 2021; Roach, 2022).

Centralized Vs. Decentralized

Although these and similar corporate announcements and developments have had a positive contribution on the growth and adoption levels of the metaverse (Emergen, 2021), they will not be investigated to a great extent, as they are centralized versions of the metaverse. This research aims to explore the policies and regulations surrounding a decentralized metaverse, not a centralized version. The key differences are control, creation and governance (Ledger, 2022). A single entity governs the entire network in a centralized metaverse. This includes the servers, but also the respective policies that are designed to regulate the virtual world. Communities within this metaverse are confined to a controlled space, in which there is no self-ownership of one's digital assets (Moe, 2021; Canavesi, 2022). Furthermore, user data collection and storage are also stored in a centralized manner, which makes it difficult for users to verify who has access to their data and under which conditions (Han et al., 2021). This could have serious privacy implications for metaverse users in terms of data mismanagement. Christopher Wylie, the renowned whistleblower that informed the public on the Cambridge Analytica scandal of 2018, in which the data of millions of Facebook (Meta) users were used without their consent (Hern, 2018; Chan, 2019), has serious concerns for the data harvesting and usage in centralized metaverses (Darby, 2022). Users are focused and putting their energy into decentralized solutions to mitigate potential problems on data management and theft. Accordingly, decentralized metaverses and Web 3.0 initiatives have been growing in popularity and attracted around 30 billion US dollars from venture capital in 2021 (Rai, 2022). A great example of a decentralized metaverse is Decentraland, and they are making use of DAOs, in which users are given the ability to dictate the future of the metaverse. This influences governance, as users can now vote on implementing certain changes and updates to control the way the metaverse is being built and operated (Caleb & Brown, 2022; Decentraland, 2022). Metaverses that are decentralized are of significant importance, as the platforms are open-sourced and the control lies within the communities, giving them more control over their own digital assets and the future landscape of the metaverse, while keeping the respective data secure on the blockchain (Jeon et al., 2022).

When looking at the current publication on the metaverse, it is evident that the current research done by scholars is outdated (Dionisio et al., 2013; Kemp & Livingstone, 2006), and new ones are mostly based around surveys (Ning et al., 2021; Lee et al., 2021). The outdated papers have no mention of blockchain, NFTs, DAOs and Meta, as that technology is relatively new. The newer papers do mention some of those aspects, but do not go into much detail.

Status and Issues with The Metaverse

Ning et al. (2021), introduces five different perspectives that one can take on the status of The Metaverse: network infrastructure, management technology, basic common technology, virtual reality object connection, and virtual reality convergence. Additionally, the authors of this paper conclude that currently, there are still six issues when it comes to The Metaverse. The mentioned issues are interaction, computation, ethical, privacy, cyber-syndrome, and standards and compatibility. While the paper also discusses the implementations of blockchain technology, it does not go in-depth on the characteristics of what sort of blockchain would fit best in terms of processing speed, scalability and other metrics. Lee et al. (2021), goes more in-depth and outlines six pillars which must be built for the ecosystem of the metaverse and another eight pillars for the technology enablers of The Metaverse. While the ecosystem has more to do with the social aspect and content creation in the metaverse, the technology enablers is the more interesting aspect to focus on. The eight pillars mentioned are: network, cloud, AI, computer vision, blockchain, robotics and Internet of Things (IoT), user interactivity, and extended reality. While this paper does discuss the application of blockchain in The Metaverse, it does so by only taking in the PoW mechanism. The PoW mechanism is inherently slow and inefficient when it comes to power, as nodes are constantly competing against each other in order to solve the next block (Gervais et al., 2016). Lee et al. (2021), did not discuss the newer PoS mechanism, which, in most cases, is more secure, and is always more efficient and faster when implemented correctly (Gao & Nobuhara, 2017). While PoW and PoS are used by the biggest cryptocurrencies, Bitcoin and Ethereum (Nakamoto, 2008; Buterin, 2013b), there are many other consensus mechanisms, with each of them offering several benefits and drawbacks (Aggarwal & Kumar, 2021; Bodkhe et al., 2020). Some of these public blockchain are Solana, Polkadot and Cardano, each with their own unique implementation and use of consensus mechanisms (Yakovenko, 2017; Wood, 2016). Another development is The Internet Computer, which developed their own mechanism called 'Chain Key Cryptography' (Dfinity, 2021).

More Digital Presence

Besides the technology, there must also be users and companies that shift towards this world in order to attract more people. This trend is clearly evident, as recently big corporations like Meta (formerly known as Facebook), Nike and Adidas are entering the metaverse with different strategies (Bonifacic, 2021; Z. Sun, 2021). This shift seen from big corporations will be an incentive for other smaller companies to make a similar move and follow the trend. This trend is most likely a continuation of the shift to a more online environment which was forced by the COVID-19 pandemic (Fawns et al., 2020).

3.1.2. Traditional Hosting Technology

According to several sources, the three above mentioned cloud service providers are the three biggest in the world and control more than 60% of the world's cloud servers (Dignan, 2021; Cohen, 2021). There could be several theories as to why Amazon, Microsoft and Google dominate the market in this industry. However, this is outside of the scope of this paper. Rather, it will aim to explain how these servers work, and what they are good at and some of their drawbacks. This sub-chapter will look at how cloud servers work 'from both a theoretical and practical perspective. In other words, it will explain some of the theoretical perspective about the topic, as well as look into the current implementation of the biggest three companies.

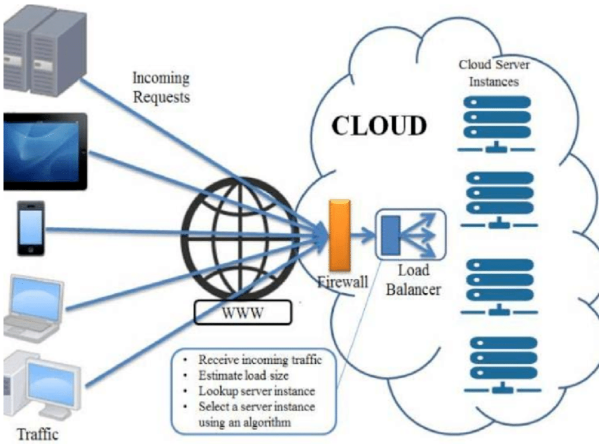
Theoretical Perspective

Yu et al. (2010) describes cloud computing as being able to offer a variety of different services in the format of "X As a Service" (XAAS), where X can be replaced with hardware, software, data storage, just to name a few. These services can be bought independently of each other and complement one another. These cloud servers can be accessed through the internet and are cost effective for both small and large businesses. Therefore, rather than each company owning their own information technology (IT) infrastructure, they can save the up-front cost of acquiring such expensive hardware and simply use the pay-as-you-go cloud computing environment (Ranger, 2022). Cloud computing can be used for a variety of tasks and can support both small and large computations. For example, while individuals can use it to save some of their data and run relatively small and simple code, many large corporations like Netflix, Samsung and NASA also outsource some of the computing power they need to AWS (Amazon, 2022; Gillar, 2020).

Figure 3.1 shows a simplified version of the infrastructure of cloud computing. While this is a simplified version of the whole system, it does give a clear overview of the workings. On the left of the figure, there are all the customers that send requests to the servers, which is known as the traffic. This traffic goes through a firewall, which is necessary for the security of the system. After the requests have been cleared, a load balancer in the system distributes the traffic across the different machines to ensure that one system is not overloaded while the others are idle and realize higher satisfaction of the users and resource utilization ratio (A. B. Singh et al., 2017b). This makes load balancers one of the most crucial elements of cloud computing and is essential for the entire system to work effortlessly. Additionally, they argue that load balancers still needed to be optimized and could use different parameters and algorithms for it. The cloud servers on the right can represent any form as service previously mentioned.

Cloud computing can be divided into three components: essential characteristics, service models and deployments models (Mell et al., 2011).

Figure 3.1: Block diagram of cloud computing infrastructure (A. B. Singh et al., 2017a)



Essential Characteristics

There are five essential characteristics when it comes to cloud computing according to Mell et al. (2011). These characteristics can be found with any cloud computing provider and are: On-demand self-service, broad network access, resource pooling, rapid elasticity and measure service.

On-demand self-service refers to the ability of consumers to unilaterally provision the computing done on the cloud. This includes controlling elements such as server time and network storage. This should be done automatically without requiring human interaction in the process.

The consumer should also be able to access their cloud computer with different devices, known as broad network access. The provider should ensure that they promote these practices and satisfy the client in this sense.

The system must be able pool its resources to serve multiple consumers. This can be done using a multi-tenant model, which includes a set of physical and virtual resources that are assigned dynamically and can be reassigned at any given time according to the demands of the customers. While the customer can have a broad sense of the location of the service provided, one should never be able to pinpoint the exact location of the provided resources. These resources include storage, network bandwidth, processing and memory.

Another aspect is that the system must be elastically provisioned and released, referred to as rapid elasticity. In some cases, this should be done automatically in order to scale rapidly outward and inward, depending on the demand at the current time. From the customers' perspective, scalability should appear to be infinite and should be appropriate for the required job at any quantity and time.

Cloud systems should be able to automatically control and optimize resource use by leveraging a metering capability, known as measured service. This should be done at a certain level of abstraction which is appropriate for the type of service: storage, processing, bandwidth and active user accounts. The resource usage should be monitored, controlled and reported, which would provide additional transparency for both parties of the utilized service.

Service Models

According to Mell et al. (2011), there are three different types of service models: software as a service (Saas), platform as a service (PaaS) and infrastructure as a service (IaaS). Each of these is tailored towards the different customers and has both benefits and drawbacks compared to another.

SaaS is the most basic type of model a customer can acquire and gives customers the ability to use the cloud infrastructure of the provider without having control over the network, servers, operating system (OS) and storage. Regardless of this, the client should be able to access the programs from either a web-browser or specific program interface.

PaaS takes this one step further and requires the customer to use programming languages, libraries, services and tools that are supported by the provider. The capability that is provided to the consumer is to deploy their project onto the cloud infrastructure acquired or consumer-created applications. However, the consumer still does not manage the underlying infrastructure manually, which would include aspects, for instance: network, servers, OS or storage. What the client does have control over is the deployed applications and possibly the configuration settings of the hosting environment for the application, giving the client a bit more flexibility in what is happening compared to SaaS.

The final model that is discussed is IaaS, where the client has full control over the OS, storage and deployed applications. However, the customer still does not have control over the underlying cloud infrastructure and cannot manage this. Ultimately, the capability provided to the consumer is to provision processing, storage, networks and other computing resources that are fundamental for any application.

Deployment Models

The last component of the three is the deployment model, which is comprised of four elements: private cloud, community cloud, public cloud and hybrid cloud.

In a private cloud, the infrastructure is exclusive to the consumer, whether that is an organization or individual. This type of deployment could be owned, managed and operated by the organization, a third party or a combination of the two.

A community cloud gives exclusive access to the users of a certain community or organization. It could therefore be owned by one or multiple organizations with which it is shared of.

The cloud infrastructure of a public cloud is open to the general public and can thus be accessed by anyone. This being said, it could still be owned, managed or operated by a business, academic or government organization.

The three infrastructures mentioned are the fundamental ones and can be combined into a hybrid cloud. This would include any combination of two or more cloud infrastructures that remain unique entities and are yet bound together by standardized or proprietary technology. This technology would enable both data and application portability.

Strengths and Weaknesses

When it comes to the strengths and weaknesses of cloud computing, the usual comparison has traditionally been between outsourcing the computation to the cloud, or investing in the hardware and software by the company itself (Baciu, 2015; Plotņikovs & Kodors, 2017).

Strengths

According to Plotņikovs & Kodors (2017), there is one main advantage that trumps all others, which is the cost effectiveness of using cloud computing. The author compares this to the cost of setting the same infrastructure up in-house, which would include costs from equipment to maintenance. This advantage is also mentioned first in other articles and seems to be one of the strongest strengths for cloud computing (Peterson, 2022; Government, 2017). Other strengths of using cloud computing relative to creating similar systems in-house include scalability, collaboration, employee productivity and disaster recovery (Baciu, 2015).

Weaknesses

However, like any other system, cloud computing also has its disadvantages. Baciu (2015) mentions that the most important weakness of cloud computing is data security, as it is a factor that cannot be controlled by the users. Taking AWS as an example, there have been several breaches in the past few years that have exposed sensitive information of millions of people worldwide (Kedrosky, 2022; Heiligenstein, 2022). In some cases, these breaches can have profound consequences for the people, the company that owned the data and the company that was hosting the data. This security issue will be further explored in a dedicated sub-chapter to it.

3.1.3. Blockchain

Blockchain technology has been briefly introduced in chapter 1.2. Here, more detailed analysis will be looked into of published papers surrounding the topic, deriving the technologies that enable the existence of the metaverse. Towards the end, the aim is to integrate this into the legal framework and regulations that are published by governing bodies as well as discussed in other scientific articles.

There are several elements of blockchain that must be discussed in order to create an understanding of the technology that would aid in answering the research questions. Essentially what blockchains try to do is to find the perfect balance when it comes to the impossible triangle (Jia, 2014). While this perfect balance is subjective to most people, in an ideal scenario, blockchains would be highly scalable networks while maintaining a good level of decentralization. Developers of many different blockchains are experimenting with finding this 'perfect balance', which is subjective in nature. This triangle represents the scalability, speed and decentralization of blockchains. This triangle is presented as a trilemma in blockchain, where developers must, in theory, give up one angle for the other two. One of the main aspects of blockchain that contributes to this triangle is its consensus mechanism, which is how the blockchain operates and comes to agreement with all its nodes. Blockchains can further be divided into three generations, where each generation builds upon the previous one and expands its functionalities. This is essential for building a metaverse on a blockchain, as it requires an advanced technology and more functionalities than first generation blockchains would bring, such as Bitcoin.

Blockchain Generations

Efanov & Roschin (2018) divides blockchains into three generations: digital currency, digital economy and digital society. What separates the generations is a combination of: mining, hashing, the public ledger, transaction enabled software and the digital currency itself (Burgess & Colangelo, 2015).

First Generation - Digital Currency

Firstly, there is the first generation of blockchains (blockchain 1.0), which only support peer-to-peer transactions between wallets of the network. Bitcoin serves both as a store of value, as well as providing value to the Bitcoin protocol itself (Burgess & Colangelo, 2015). Key advantages of using such a technology are more anonymity than credit cards and (in Bitcoin's case) a hedge against inflation (Moore, 2013).

Second Generation - Digital Economy

While the first generation was only able to facilitate peer-to-peer transactions, second generation blockchains allow for several financial applications to be built on its platform (Peters & Panayi, 2016). One prime example of such a blockchain is Ethereum, where developers can create *smart contracts* on the blockchain (Buterin, 2013b). The idea of smart contracts was first published by Szabo (1997), but it was Buterin (2013b) who implemented the idea with its blockchain. What smart contracts allow for are applications in the form of contract that run on the blockchain. These applications can be anything from new tokens, non-fungible assets and DAOs. However, while individuals can create and exchange NFTs on the Ethereum network, they can also be taken off-chain and host them on other data centers, such as AWS (Canellis, 2019).

Third Generation - Digital Society

The third generation blockchains expand to non-financial forms, including: art, identity, governance and communication (Burgess & Colangelo, 2015). One of the most promising applications in this field is in smart cities, which would combine horizontally cumulative elements: smart mobility, smart governance, smart living, smart use of natural resources and a smart economy (J. Sun et al., 2016). Another aspect is digital identity, as blockchain technology can help the two billion unbanked individuals in creating a digital identity and gain access to bank accounts and loans (Underwood, 2016).

It is the third generation that will be able to enable the metaverse and grow to its utmost potential. Therefore, when looking into blockchain technologies and ones that can possibly host the metaverse, it is crucial that this must be a third generation blockchain. If this is not done, then the space is already limited in certain areas before true development can begin.

Consensus Mechanisms

While the blockchain generations cover the technological advancement of blockchain from a more holistic view, the consensus mechanisms go more in-depth on the technology itself. Blockchains have consensus mechanism to come to agreement on the state of the network among all distributed nodes (Aggarwal & Kumar, 2021). Essentially, the consensus mechanism ensures that the blockchain network is being operated properly without any bad actors.

The consensus mechanisms used by the two most popular crypto currencies (Bitcoin and Ethereum) are PoW and PoS. These two mechanisms are used by many other crypto currencies and blockchain.

Proof-of-Work

PoW, used by the Bitcoin network, utilizes the computational power of machines to establish consensus (Nakamoto, 2008). Blocks get added to the chain one at a time by a random node in the network, which publishes the findings to the others and gets the rewards for mining that particular block. While this mechanism is secure and reliable, it is not energy efficient, fast and not scalable compared to other mechanisms (Rain, 2022). When looking at the impossible triangle, this mechanism gives up scalability in order to be secure and decentralized.

Proof-of-Stake

PoS is a mechanism that is currently used by Cardano (ADA) and is being implemented by Ethereum as well. This mechanism is much less computationally heavy compared to PoW, but can have a higher barrier to entry. This is because in PoS, a node must stake a certain amount of crypto coins in order to start being a validator on the network (Rain, 2022). Staking this crypto coin means that the validator does not have access to it, but they do earn interest on it. If a validator ends up being malicious, the staked crypto is taken away and the individual will lose all of it, which should disincentives them to act in such a way. While this mechanism is much more scalable, it gives up a certain level of decentralization compared to PoW.

Other Mechanisms

Along the road, developers have come up with variations of the PoS mechanism as well as brand new concepts that would help address the impossible triangle and find the best balance between the three elements. Three of the most popular and perhaps effective blockchains in this sense are Polkadot's Parachains, Solana's Proof-of-History and The Internet Computer's Chainkey Cryptography (Parga, 2021). Each one of these three has its own benefits and drawbacks when it comes to each one of the three elements of blockchain and addresses the issues is different ways.

Web 3

The time it took for the World Wide Web (WWW) to transition from Web 1 to Web 3 has taken a few decades, as the earliest trace of Web 1 can be tied back to the creation of the Mozilla (Netscape) web browser back in 1994 (Starry, 2019). In Web 1, there were a handful of content creators, with the majority of the users being consumers of the content (Sharma, 2022). This made the flow of information a one-way street, as users could not alter, create or publish content on the web. This version of the web can be compared to newspapers, where users are presented with a set of information, only on the web one was able to search for more information than in newspapers.

From there on, the WWW developed into Web 2, where the consumers could turn into content creators on the web and publish it for others to see Sharma (2022). This web is also dubbed as 'the participative social web' and is the version of the WWW that many people currently use (Aghaei et al., 2012). Moreover, Aghaei et al. (2012) gives an overview of the features as well as the potential usages between Web 1, Web 2 and Web 3. One prime example of Web 2 usage is Facebook, where users can post content that is created by themselves onto a centralized platform owned by Meta. Meta can decide whether or not the content adheres to the policies of the platform and has the authority to delete the content if it does not fit the criteria. In addition to this, it can decide to block users from its platform, which was the case when Donald Trump got banned from Twitter in January 2021.

As for Web 3, it was John Markoff that first used the term 'Web 3.0' to describe the new era of the WWW back in 2016 (Spivack, 2011). According to one of the first definitions of Web3, its core concept is to define structure data and link these. This will lead to more effective discovery, automation, integration and reuse of the data across a wide variety of applications (Ossi, 2003). Another definition of Web3 is the Semantic Web, as per the inventor of the WWW itself (Berners-Lee, 1998). Essentially, the Web3 revolution will get rid of the centralized players in the industry and have a more decentralized structure in terms of data and its usage (Choudhury, 2014). Gavin Wood, the founder of the Web3 Foundation, has mentioned in an interview that Web3 is a movement towards a more liberal model and will safeguard the liberal world (Ortega, 2022).

Looking at these definitions of Web3, one can easily identify the link with blockchain technology. As mentioned, Web3 makes use of decentralized data, and it is more effective when using this data for a wide variety of applications. Aghaei et al. (2012) explains that Web 3 is essentially a 'web of data', where there are links between primary objects (documents and files). However, since this paper is relatively old for the space, it has no mention of blockchain and how the two tie together. While the paper also briefly touches on Web 4, the authors acknowledge that it is still an abstract idea and far into the future.

Decentralized Autonomous Organizations

Blockchain-based ecosystems, such as metaverses, are aiming to realize a future in which (online) groups can successfully coordinate (pseudonymously) by relying entirely on software. This ambition has been slowly coming into flourishing by the introduction of another technological advancement within blockchain technology; DAOs. DAOs are decentralized systems that run on blockchains and enables people to coordinate and govern the system based on a set of self-executing rules (Hassan & De Filippi, 2021). While the first publications on DAOs date back to 1997, were Dilger (1997) introduced the idea of defining multi-agent systems in an IoT environment, the definitions have changed. It has taken on a more modern version and has been re-introduced in 2008 by Satoshi Nakamoto - the anonymous founder of Bitcoin (Nakamoto, 2008; Hassan & De Filippi, 2021). It was only until 2013 that the term started to be used more frequently on online forums and by the Ethereum co-founder, Vitalik Buterin (Larimer, 2013; Buterin, 2013a).

While the definitions of DAO slightly differ from one paper to another, they are in essence all the same and include the blockchain infrastructure and self-governance of software (Nabben, 2021; El Faqir et al., 2020). Instead of the governance being tied to jurisdictions that are bound by location, DAOs aim to transcend national borders with thousands of members that abide by and govern their matters through software, cryptography and ”the rule of code” (Rodrigues, 2018; Filippi & Wright, 2019). DAOs rely on autonomous smart contracts that oversee and facilitate member-to-member interactions and transactions without the need of a centralized entity or intermediary. It also keeps track of the organizations' memberships, which can be purchased, earned or rewarded in the form of a token. These tokens provide the members specific rights over the system to access, manage or influence the resources and/or services of an organization through on-chain voting, providing members with a chance to engage within an organization's decision-making processes (Zhao et al., 2022; Filippi & Wright, 2019).

To some, the first example of a DAO is the Bitcoin network, as it was scaling through community agreements and did not have an organized governance mechanism. However, as aforementioned, the definition of DAOs is constantly changing, and Bitcoin does not classify as a DAO by today's standards anymore. The project does not have a governance mechanism that allows members to vote on treasure and/or resource usage. Taking that into consideration, one could say that Dash would be one of the first DAO's; in August 2015 they have introduced nodes (*Masternodes*) with voting abilities to determine what could happen to 10% of the (monetary) block rewards of the project (Johnson, 2016).

As DeFi satisfied the desire of the blockchain community for an open, permissionless and decentralized financial system, DAOs became a crucial component of projects that wanted to demonstrate their level of decentralization through community governance. Consequently, when DeFi grew in popularity in 2020, so did the popularity of DAOs and governance tokens (Graah, 2022). The most prominent projects that label themselves as DAOs are: Uniswap, ApeCoin and Aave (Brooke, 2022; CoinMarketCap, 2022). However, it is important to note that a variety of different cryptocurrency projects, such as ICP and Solana, are also starting to integrate governance tokens into their ecosystem and expand their use-cases, making some (DAO) ecosystems relatively nascent in comparison to others. While Solana's on-chain governance system is still a concept and has not yet been implemented, ICP has already done so with the Network Nervous System (NNS) (Bor, 2021; Dfinity, 2021). At the moment, it is therefore impossible for users to vote on proposals to improve the network and change its trajectory. On the other hand, the NNS for the ICP network has been live since the genesis event back in May of 2021. Holders of the native ICP token can stake their coins on the NNS app with a lockup period of 6 months to 8 years. The voting power and rewards of the staked coins increase with longer lockup periods. The proposals are grouped into different categories to make it clear to the user what the proposal is about. Moreover, one can delegate the voting to follow the votes of other people (at this point it is only possible to follow organizations) and vote exactly the same as them (Dfinity, 2021). This can be done for all topics, except for governance topics, as the network feels that this is too important to delegate and ensures that most people consciously vote on these types of proposals. Therefore, ICP clearly has the upper hand over Solana, as Solana does not have such a system in place and has no detailed schedule on when this could become available.

At its most rudimentary level, a DAO can provide a way for a large group of people to (financially) organize themselves towards a collective aim. However, difficulties might arise in the real world. AssangeDAO was founded in late 2021, after the High Court ruled that Julian Assange, founder of Wikileaks who is wanted in the US over publications of classified documents, can be extradited from the UK to the US (Morton, 2021; AssangeDAO, 2022). It had raised $55 million to bid on an NFT project that would funnel those funds towards efforts that support Assange's case. The project drew support from high-profile figures, such as Ethereum co-founder Vitalik Buterin and whistleblower Edward Snowden. However, there were ideological differences within the community on how the funds should be spent. This ”leaderless organization” had difficulties with resolving differences in these low-trust environments, as they lacked the mechanisms to properly measure the will of the DAO, and that ultimately tore it apart. Amir Taaki, one of the people behind the development of Bitcoin, even wrote in a post following this controversy: *”DAOs are unproven to the vast majority of the world”* (Kuhn, 2022; Castrovilli, 2022).

Non-Fungible Tokens

Emergent technologies, such as blockchain, tend to bring new forms of applications to the general public that were previously deemed to be unnecessary or unfeasible. Furthermore, as these new technologies bring along new applications and concepts, they also create new desires and needs that have to be met. In this case, the growing adoption levels of blockchain in combination with the concept of (partially) adopting a 'digital/online identity', such as in the Metaverse, have created the need of proving the authenticity of ownership of certain digital assets. Accordingly, NFTs have appeared to resolve this matter, as it aims to represent ownership of digital objects like art, collectibles, jpegs and video clips, or in-game items. Generally, NFTs are encoded within smart contracts that are deployed on the blockchain, making the certification unique and therefore not interchangeable, while providing the owner with a unique digital certificate of ownership (Evans, 2019; Nadini et al., 2021).

The public attention towards NFTs peaked in 2021, when Mike Winkelmann - known as Beeple - sold an NFT as art for $69 million. This event had put someone, who had never sold a single print over

$100 six months prior to the big sale, in the current top three of most expensive living artists in the world (Kastrenakes, 2021; Barnebys, 2022). Nevertheless, the concept that became the driving force of NFTs was written in a paper dating back to 2012, in which Meni Rosenfield introduced the concept of ”Colored Coins” for the Bitcoin blockchain, which was an idea to represent and manage real-world assets on the blockchain by proving asset ownership (Rosenfeld, 2012). However, due to technical limitations of Bitcoin the concept was not able to become reality at that time. Nonetheless, on May the 3rd, 2014, Kevin McCoy had ’minted’ the first NFT *Quantum* on the Namecoin blockchain, in which ’minting’ refers to publishing the token on the blockchain. From that point on, many events that included significant amounts of experimentation and developments have led to Counterparty (Bitcoin 2.0) as one of the first NFT platforms, which has paved the way for mass-adoption in terms of NFT minting and trading (Wong, 2021; Gaskin, 2021; E. Taylor, 2021).

Currently, over 90% of all digital assets are on the Ethereum network and have the ERC-721 standard, which refers to a subset of Ethereum tokens that are suitable for NFT-minting. However, all this popularity has come at a cost. Due to network saturation, high transaction fees and specific blockchain configurations, many other (NFT) platforms have emerged and are currently successfully operating in their own ecosystem (Matob, 2022; Ethereum, 2022). ICP and Solana have introduced their own standard(s), such as DIP-721 and SPL Metaplex, and are supposed to be cheaper and faster alternatives to Ethereum’s ERC-721 standard (ICP, 2022; Solana, 2022). However, regardless of an NFT’s standard specifications, they are set to be great use-cases for it in the metaverse. The concept of virtual marketplaces is one of the most prominent outcomes of NFT-usage in the metaverse, in which users will be able to buy and sell digital items with certified ownership attached to it. Furthermore, as the metaverse is aiming to incorporate many aspects of the real world in a virtual setting, the idea of an art gallery or integrating art (as NFTs) in ’virtual real-estate’ is growing and slowly becoming reality.

3.1.4. Comparison Between the Technologies

While both technologies are fit to host the metaverse and share similarities, there are some crucial differences between the two. Here, the motivation for comparison between the two technologies is discussed, as well as the motivation behind choosing ICP as the specific blockchain to compare traditional hosting technologies to.

Motivation for Comparison

Although a completely centralized version of the metaverse is excluded from the research, it is a possibility that the metaverse could make use of both hosting technologies. What is meant by a centralized version is that the metaverse itself is run on the servers of a single enterprise and the digital goods are not transferable to other metaverses. By making use of both technologies, the best aspects of either one of them can be used and combined to create the best possible hosting environment between the two. Moreover, blockchain might not suit every application and further research is needed to figure out the best manner in which blockchain technology can be adopted in governmental bodies (Ølnes et al., 2017).

Motivation for Specific Blockchain

Comparing blockchain in general to traditional hosting technologies is nearly impossible, as there are many different blockchain, which all have their own (dis)advantages. Therefore, in some cases it must be compared to a specific blockchain, which as mentioned earlier, will be ICP. There are a few reasons behind this, which will now be discussed.

First of all, ICP allows for computation to be done on-chain. Even though the metaverse will likely be hosted on a combination between the two technologies, it is crucial for the comparison chapter to use a blockchain which can perform computations on-chain. Smart contracts, or ’canisters’ as they are called on ICP, can make use of the computational power that the nodes of the network possess. In addition to computations, users can store data on the network at relatively low prices compared to other blockchains, with prices competing with large CC enterprises, such as AWS (Buenconsejo, 2022; Siffert, 2022).

3.2. Policies and Regulations

Now that the technologies have been discussed, the current policies and regulations that are currently implemented in the EU will be looked at. These regulations could be either for blockchain or the metaverse itself. However, since the metaverse is a new concept, it is expected that there are currently only regulations for blockchain in the EU, while future regulations could impact both.

3.2.1. Policies versus Regulations

While many people use the two terms synonymously, policies and regulations are different by nature, and it is important to distinguish them before diving deep into each one of them. While both of them are put in place to direct the people in a certain way, they usually have different goals and the consequences of breaking a policy or regulations can differ drastically. As Dawson (2012) describes, policies that are made to achieve goals of organizations and governments to carry out certain plans. On the other hand, a regulation more so has the effect of an implemented law and is considered to be more restrictive than policies. Regulations are usually enforced and imposed by authorities to ensure that people follow the code of conduct in alignment with the implemented regulations. Surbhi (2021) seconds this by stating that policies are meant to act as a guide to decision making, whereas rules (regulations) help with discipline and regulating the work and environment within an organization or country. The author outlines key differences between regulations and policies, which can be seen table 3.1. This table lays out the key differences between the two on various fronts and gives a clear overview of the discrete differences between the two.

Table 3.1: Comparison table between policies and regulations (Surbhi, 2021).

Comparison	Regulations	Policies
Definition	Set of rules that imply a clearly stated standard that regulates the behaviour of individuals	Principle of action created by organizations or governments, acting as a guide for decision making in different circumstances
Represents	An order that must be followed	Framework where decisions will be made with
Determines	What should and should not be done by individuals	what must be done in different circumstances
Sources	Procedures and policies	Objectives
Rigidity	Highly rigid	Relatively less rigid
Type of statement	Specific statements	General statements
Objective	Maintain discipline, ensure compliance and govern behaviour	Guide decision making processes and ensure alignment in decisions

Now that the differences between the two have been laid out and understood, one must grasp a firm understanding of the different types or policies and regulations. This will aid in advising what type of either a policy, regulation or both to implement for a metaverse built on the blockchain.

Types of Policies

According to Lowi (1972b), there are four types of policies that can categorize all of the existing policies, namely: distributive, regulatory, constituent and redistributive. Each of these types has its own benefits and drawbacks and are designed for specific purposes.

Figure 3.2: The four different types of policies as described by Lowi (1972a)

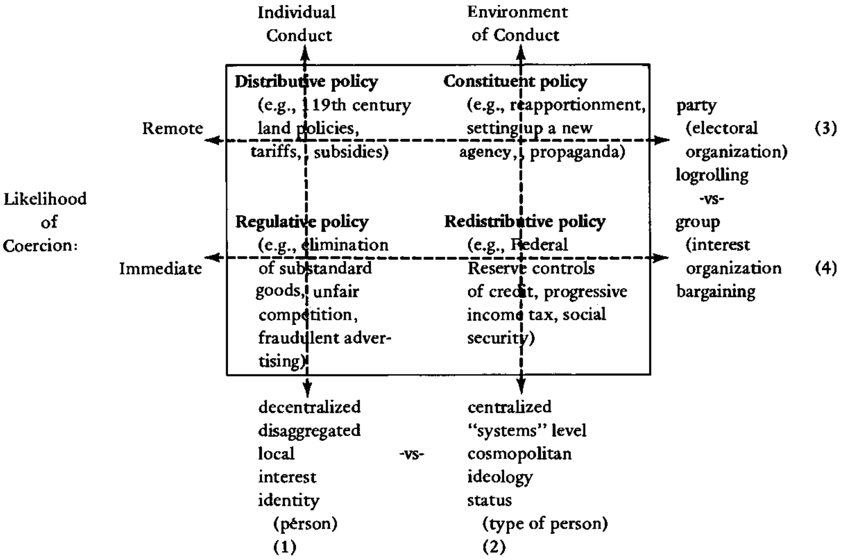

Individual Conduct
Environment of Conduct
Likelihood of Coercion:
Remote
Immediate
Distributive policy (e.g., 19th century land policies, tariffs, subsidies)
Constituent policy (e.g., reapportionment, setting up a new agency, propaganda)
Regulative policy (e.g., elimination of substandard goods, unfair competition, fraudulent advertising)
Redistributive policy (e.g., Federal Reserve controls of credit, progressive income tax, social security)
party (electoral organization) logrolling (3)
-vs-
group (interest organization bargaining (4)
decentralized disaggregated local interest identity (person) (1)
-vs-
centralized "systems" level cosmopolitan ideology status (type of person) (2)

Figure 3.2 depicts the image which Lowi (1972b) created for understanding the four types of policies. Each of these four different types of policies are discussed in the following sub-chapters. All of the information is obtained from Lowi (1972b), which examples given from the modern-world to link the theory to something more tangible.

Distributive policies

The first type of policy is the distributive policy, which can be seen at the top left of figure 3.2. These types of policies are focused on distributing goods and services to members of an organization or group. However, the costs of those goods and services are also split amongst the same organization/group that would use them. One great example of such policies is expenditures for public education and welfare, as citizens benefit from these investments from the government, but also (indirectly) pay for those through taxes.

Regulatory Policies

The second type is regulatory policy, which looks more at the environment conduct rather than the individual conduct. These types of policies are more limiting in nature and are supposed to compel specific types of behaviour. This can best be done when there is a clear differentiation of good and bad behaviour as defined by the policy. Bad behaviour can then be penalized through the use of sanctions or fines on the person, group or other form of organization. One such successful example are speed limits, which are enforced by the law and there is a clear distinction between good and bad behaviour, since speed limits are not ambiguous.

Constituent Policies

The third policy is the regulative policy, which is more aimed at immediate coercion. Moreover, these types of policies deal with laws and create executive power entities. In some circumstances they can also deal with fiscal policies, which are more linked to monetary issues.

Redistributive Policies

The last type is the redistributive policy, which in some ways is similar to the first type but is more focused on a specific group. While the likelihood of coercion is also immediate, as with the regulative policies, it does not necessarily mean that the differentiation is between good and bad behaviour. Rather, it is between individuals that are in need of the redistribution of goods or services and individuals that are not. One great example of such a policy is health insurance, where the collected money gets redistributed amongst the people that need it most.

Now that the four types of policies have been discussed, there is a clearer picture of what type of policy could potentially be implemented for the metaverse. Obviously different areas would require different types, as they are not a one-size-fits-all type. However, it will aid in both formulating and understanding the theory behind the policies itself.

3.2.2. Metaverse and Regulations

There are two forms of regulation in the metaverse: regulation by architecture and regulation by law, in which the former refers to a computer software that prohibits the users from performing certain actions by choice of the developers and the latter refers to regulatory frameworks that are imposed by a third-party (country or organisation). This sub-chapter will discuss the existing (international) regulatory frameworks that are relevant for understanding the concept of decentralized metaverses regulations.

Currently, the governance of the internet varies considerably from country to country, and it is expected that the metaverse will adhere to a similar nature (Hui, 2021). It is important to note that there are significant challenges that are associated with regulating decentralized platforms. Decentralized metaverses are autonomous organisations (chapter: 3.1.3), meaning, they are operated and governed by a code or protocol without the interference or influence of a central body. This poses an intriguing question, whether one will be able to successfully regulate the operations of a decentralized platform that is strictly governed by a programming code. A paper by Salami (2021), puts forward the idea that this highly depends on how decentralized these platforms are and whether the organisation has sufficient power over the operations to be held accountable for the activities that are occurring on the decentralized platforms. Furthermore, as there is a growing need for clarity on decentralized platform regulations, there seems to be a greater emphasis on enforcing the regulations based on how people are using the platform. This has shifted the focus of literature on the practices of humans on decentralized platforms, rather than the technological aspects that facilitate the respective actions (J. A. Fairfield, 2021; Trotz, 2019).

In terms of past legislations that could be deemed as relevant for today, there are three key regulatory regimes in the U.S.: Financial Crimes Enforcement Network (FinCen), US Securities and Exchange Commission (SEC), and Commodity Futures Trading Commission (CFTC). For Europe, the most prominent regulations stem from the European Commission within the European Union (Aberg et al., 2022; Commission, 2022b). The following is a set of legislations that are important to consider for regulating the decentralized metaverse (Commission, 2018; ESMA, 2018; EUR-Lex, 2009):

- General Data Protection Regulation (GDPR) - data protection law.
- Markets in Financial Instrument Directive II (MiFID II) - protection for investors
- Electronic Money Directive 2 (EMD2) - licenses of an electronic money institution

One might presume that these laws and regulations are of great importance, but due to the technological advancements within the blockchain space, they have become less relevant and more difficult to apply to the respective operations and concepts of (decentralized) metaverses. With respect to GDPR, it is still unclear who bears the responsibility of data processing in a decentralized platform and becomes liable in the event of lost or stolen data. The platforms are also aiming to be interoperable, which could lead to the sharing of sensitive information of businesses (such as pricing) and that is supposed to violate the anti-trust challenge and competition law. What happens when digital assets are embodied as NFTs, or real buildings are being replicated in the metaverse. How does this relate to copyright law? In 2018, the Financial Conduct Activity (FCA) commented the following: *”we do not consider* *cryptocurrencies to be currencies or commodities for regulatory purposes under MiFID II"*, and since then not much has changed for crypto(-related) assets within MiFID (FCA, 2018). EMD2 does not take into account the concept of cryptocurrencies into their current legislative framework and does not cover blockchain technology. They have even released a report for the European Commission, stating that crypto-assets are not part of the financial services law in the EU (EBA, 2019).

The existing legal laws have proven to be insufficient to address the complex matter of regulating decentralized metaverse. Accordingly, In February 2022, the European Parliament (EP) has directed questions towards the European Commission asking whether they could: *"launch a study to better understand the metaverse and the risks to the general public"* and start the investigation process of regulations *"right away"*, as *"it could slip through the net of current legal and consumer protection safeguards"* (Parliament, 2022). This developing technology has proven to put immense pressure on the existing laws and is demanding regulators around the world to construct more detailed and sophisticated regulations.

However, regulatory progress of blockchain and cryptocurrencies has been occurring. The SEC has recently announced the establishment of the Crypto Assets and Cyber Unit to ensure the protection of the investors in the crypto market (Franck, 2022). Organizational steps are being taken and proposals are being constructed for potential legislation forming. One of the most prominent regulations of the European Commission is the MiCA Directive. It has been introduced in 2020 and aims to provide a sound legal framework that can be used to define the regulatory treatment of the crypto-assets that are not (yet) covered by the existing legislations (Commission, 2020a). However, the term metaverse has not been mentioned once in this Directive, as it mostly focuses on requirements for crypto-asset issuers and service providers in terms of market abuse, which does not have significant levels of influence on the type of regulations in the metaverse (Alexandrov, 2020). It is also important to note how the Council has adopted another proposal known as the DORA. Similarly, this proposal also does not provide a framework for regulating the metaverse, but has a focus on mitigating IT risks and providing a framework to harmonize the digital resilience processes and standards across financial institutions (Commission, 2020b). The key takeaway from this is that both proposals might indirectly influence some aspect of crypto-usage within the metaverse, through setting certain requirements of utility-tokens, but do not address any type of regulations within the metaverse or the technology itself.

There has been one instance of a distributed ledger technology that has been used as a pilot for drafting new EU regulations (Zetzsche & Woxholth, 2022). While the structure of this study is in the right direction towards understanding implementations of policies for blockchain, the policies themselves have little to do with blockchain technology and the metaverse. Rather, this pilot study has a similar focus to MiCA as it aims to address EU financial law regulations rather than possible blockchain technology and metaverse regulations.

As one can see, there are no current regulations that directly address possible issues that might occur in the metaverse itself, such as the 9 mentioned categories mentioned in the next sub-chapter. On top of that, there are no regulations that focus on the technology on top of which the metaverse is built: blockchain. All that the current regulations focus on is crypto assets and the safety of investors themselves. Therefore, addressing the first research question, there are no current regulations within the EU that address the metaverse or technological aspects of blockchain

Potential Metaverse Regulations and Policies

While there are currently no regulations or policies that specifically address the metaverse, there are some areas that could and/or should be regulated (Lau, 2022; Madiega et al., 2022; Ara et al., 2022). These areas are governance & legal documentation, liability, intellectual property, data privacy, DAOs, smart contracts, know your customer (KYC), virtual asset taxes and regulations of conduct. These 9 categories for potential regulation are mentioned mostly in relevant publications and articles and will therefore be looked at first. Table 3.2 was presented as is to the interviewees and asked whether they think the aspects apply and their top 3 rankings for the 9 aspects.

First, there is the *Governance & Legal Documentation*, which refers to the governance and documen-

Table 3.2: List of potential critical aspects that could be monitored with the help of policies or regulations in a decentralized metaverse.

Possible Regulation	Description
Governance & Legal Documentation (1)	The governance of the blockchain should be outlined clearly with detailed descriptions of the technology.
Liability (2)	The liable party in case of malfunctions, wrong transactions or other faults caused by the network.
Intellectual Property (3)	IP rights within the metaverse; ensuring that companies have the necessary IP rights to publish and use certain content.
Data Privacy (4)	The security and privacy of the data of the users of the metaverse built on the blockchain.
DAOs (5)	Should the creation and operation of DAOs stay decentralized or will it need some regulation? Which party will be responsible when something goes wrong?
Smart contracts (6)	Will smart contracts need some sort of additional compliance layer in order to satisfy as a 'legally enforcing contract' to settle goods or other virtual matters in the future?
KYC (7)	Will some sort of KYC be needed for either the users or the node operators that power the blockchain? For example, when addressing the liability issues mentioned earlier.
Virtual Asset Taxes (8)	Since a lot of wealth will be transferred to this new virtual world, should governments start taxing the wealth created/generated in this digital environment?
Regulation of Conduct (9)	How will the behaviour of individuals in this digital world be regulated and what will be the consequences of misconduct? Are bans of the platform enough or should there be additional follow-up?

tation of blockchains and the code. The sources mention that these codes should be outlined clearly with enough documentation for others to understand the code itself and know the specifics.

The second aspect is the *liability* issues in case of a malfunction, wrong transaction or any other fault that can happen in the network. Most notable of these are potential smart contract failures that can occur on blockchain networks when interacting with them. The sources stipulate that there could be need for a potential regulation that clearly outlines the liable party in case of such an event. In the hypothetical example of the smart contract failure, the liable party could be either the developers of the smart contract, the users that interacted with it or the owners of the network where the smart contract is deployed.

The third concerns the *intellectual property* rights of creations on the blockchain and in the metaverse. More specifically, it concerns the correct rights that must be obtained from the parties in order to publish and use the content in question. This can be particularly tricky, as there are many ongoing projects, and it is (as of now) difficult to follow and track everything that is going on.

The fourth aspect is *data privacy* of the users that would use the metaverse. The discussed blockchains are public and permissionless blockchains, where anyone can access the data of the users and could be shared and used in other applications. One great example of this use that is currently being implemented in applications are targeted advertisements on, for example Facebook and Instagram.

The fifth element is the *decentralized autonomous organizations* that will to some extent regulate the blockchains. The issue is whether the creation of these should stay completely decentralized or whether they need certain regulations and must therefore adhere to some centralized guidelines. Moreover, as is also the issue when it comes to liability, some sources state future regulations could include a liability factor for the developers of the DAO in case of malfunction.

The sixth feature that was discussed is *smart contracts* that run on blockchains. More particularly, whether an additional regulatory layer is needed for them be legally enforced by law in order to settle virtual assets in the metaverse. Since smart contracts offer new advancements and can be implemented in a much more efficient manner than traditional contract and in a wider variety of cases, they are likely to be the most prominent type of legally enforced contract that will be used in the metaverse. Therefore, it might be necessary to add an additional regulatory layer that makes all smart contracts legally enforceable in the jurisdiction that the user is in.

The seventh aspect regards the *know you customer* procedures of that the metaverse might implement. As with many other aspects in life, certain KYC procedures might be implemented in the metaverse to verify a user's identity. This could be for any number of reasons, including linking physical and digital users and goods. However, the discussed blockchains are, by nature, anonymous and can be used by anyone without providing proof of identity. It is therefore difficult to implement. Moreover, there are multiple ways to go about this and implement the KYC, besides using traditional ways that have been used in the past.

The eighth element is the *virtual asset tax* that can be implemented as digital assets within the metaverse. This can be capital gains tax, which is already being implemented on cryptocurrencies in the United States but could also encapsulate other types of tax. One form that has not been discussed yet are potential property taxes on houses in the metaverse, waste tax or other forms that are currently in the physical world. Since a lot of wealth is expected to enter the metaverse, it is likely that governments will receive less from taxes if nothing is done about it. There could therefore be new regulations that tax certain aspects of the metaverse.

The ninth and final aspect that could be regulated in the metaverse is the *regulation of conduct*. This refers to the behaviour of individuals within the metaverse and ensuring that users that misbehave have consequences of their actions. Since this is a virtual world and no physical harm can be done to others (yet), this would primarily be focused on virtual harm or theft in the metaverse. Moreover, what the consequences could be are also of importance, as actions that are more harmful should be punished with greater consequences. However, deciding the severity of the consequences is outside of the scope of this research.

3.2.3. Blockchain and Regulations

Now that regulations for the metaverse have been discussed, it is time to look at one of the possible underlying technologies: blockchain. However, even though there might not be any direct regulations and policies for the metaverse as discussed above, there could potentially be blockchain regulations within the EU that indirectly affect the metaverse in some respect.

EC & ECB Plans

The European Commission has already published a legal and regulatory framework for blockchain, which includes a digital Euro, crypto laws for the EU region and future plans for blockchain regulation

(Commission, 2022a). The digital Euro has been an idea of the European Commission (EC) and the European Central Bank (ECB) since January of 2021 (Commission, 2021). More recently, the ECB has published an official statement where they declare their plan: getting ready to possibly issue a digital Euro coin. (Bank, 2022).

OECD and Regulations

In 2019, the Organisation for Economic Co-operation and Development (OECD) published a case study report focused on sustainability infrastructure of blockchain and outline some implications for policy makers (OECD, 2019). The core benefits from their perspective of implementing blockchain technology into financial services are threefold: unlocking new sources of financing, bringing visibility to alignment and enhancing awareness and access. When it comes to policy makers, OECD (2019) states that policy makers should take the initial steps to address legal and regulatory issues. Moreover, since many of the mentioned issues are on an international level, the article emphasized on the international coordination between countries and elaborates four specific actions. The first of these actions addresses education around blockchain technology and aims to create a ”standardised toolbox” that will facilitate further R&D. The second point concerns the knowledge transfer to developing economies, as well as collaboration for research and partnerships between the private and public sector. The third item is the clarification of regulatory treatment of the space, with a specific spotlight on securities law, tax law, legal recognition of data from blockchain databases, data privacy and consumer protection. This should be done through a close collaboration between governmental regulators and stakeholders in the blockchain ecosystem. All of these areas are also of interest when looking into the metaverse and will thus be further expanded upon. The last point that the study touches upon is all about increasing the understanding of the metaverse and sharing information on online forums and blogs.

Three out of the four said points regard the increasing and sharing of information across stakeholders to ensure that everyone is up to date with the current knowledge. While these are good ideas to improve understanding and assure that all stakeholders are on the same page in that regard, it does little to address the actual policies and regulation in the jurisdiction involved. The third point is of most interest to this research, as it involves actual policies and regulations being created in the landscape, particularly around the areas that were mentioned. OECD (2019) continues to discuss the application of blockchain in four different areas as case studies but does not expand on what type of policies and regulations would fit best, how strict they should be or whether they should be more local or global.

Besides blockchain, this future regulation could have an impact on the metaverse as well. The areas that could have an impact are tax law, data privacy and consumer protection. Since the metaverse is expected to grow to a $3 trillion industry in the next decade within the next decade (Ramage, 2022), meaning that there will be a large influx of wealth into this space. If this money were not taxed, governments could expect to lose some of their income from taxpayers. Data privacy is perhaps just as important as taxation, as many users are expected to use the space and will thus store lots of data in the metaverse. If this data is stored on the blockchain, it must be stored in such a manner that others are not able to see sensitive data, such as one’s address or social security number. These two regulations could therefore have a direct impact on the metaverse, which the OECD should take into account when drafting such regulatory frameworks. As for consumer protection, it depends what direction the OECD will go. For example, there is already a regulatory framework that addresses consumer protection in the blockchain space but is much more tailored towards crypto assets. This is not expected to have a big impact on the metaverse itself, as it is more about the technology behind it. However, if they decide to focus more on protecting consumers in case of misconduct in the metaverse or crypto-phishing (for crypto and potentially NFTs), then it will have an impact on the metaverse. Therefore, it is still unclear whether this last point will have a direct impact on the metaverse but will most likely have some sort of indirect effect on the users of the metaverse and protect them in some ways.

3.3. Knowledge Gap

While the blockchain technology has advanced to levels sufficient enough to host a metaverse, the policies are yet to catch up to the developments. The current policies only focus on the investment and financial side of blockchain technology and aim to protect investors from extensive harm. There are currently no policies in place in the EU that address the underlying technology of blockchain itself or the metaverse, leaving room for new research to be conducted and explored.

3.4. Conclusion

All in all, the metaverse is a complex space and its definition still varies depending on the source. There are multiple ways to build a metaverse, using both traditional cloud computers (centralized) and newer blockchain technologies (decentralized). There are many new developments in the technological aspects of the metaverse, while the scientific articles on the matter are lacking behind. The most recent papers on the metaverse briefly mentioned that it could be built on a blockchain but did not go into detail on how it could be implemented or what type of blockchain to use, merely the potential benefits that blockchain could bring to the table.

As mentioned in the paragraph above, the metaverse can be built on two technologies: cloud computing and blockchain. the cloud computing infrastructure has been around longer than blockchain and is thus also more developed. There are three service models in this respect: SaaS, PaaS and IaaS, which are each tailored towards different consumers, giving the users the option of which model they want to work with. Different elements of the metaverse can thus utilize different service models. Blockchain on the other hand is a newer technology and although it offers new concepts, such as DAOs and NFTs, it is much less mature than cloud computing and thus has its drawbacks as well.

As for the regulations on blockchain and the metaverse in the EU, currently there are only a few that apply to this space. The first regulation is that of the MiCA framework, which focuses specifically on the crypto assets, rather than the blockchain technology itself. This regulation is aimed at reducing the number of illegal activities within the crypto-asset space. It also gives regulation on what companies must do in order to release new crypto tokens that would be legal from the perspective of this framework. Beyond this, the EC and ECB are planning to release their own digital Euro coin, but as of Q2 2022, these are merely possibilities and not a reality yet. The OECD published an article in 2019 that emphasizes on increasing the knowledge about blockchain amongst the stakeholders for regulating blockchain technology. Therefore, one can see that there are no current regulations on blockchain technology itself within the EU. The metaverse, an even newer development than blockchain, also does not have any current regulations. However, in February of 2022, the EP has asked the EC to conduct a study into understanding the risks that the metaverse carries to the general public. Even though there are no updates yet on this matter, this study could kick start the first few regulations within the EU for the metaverse. Yet as of now, there are no regulations at all that focus specifically on the metaverse in the EU.

This chapter was aimed at answering the first sub-question:

What are the current policies and regulations in the EU that are associated with blockchain and the metaverse?

It can be said that there are currently no regulations or policies in effect that affect either blockchain technology or the metaverse in the EU. However, there is the MiCA framework, which focuses on regulating crypto-assets and there are plans to regulate both in the future, although it is still unknown what will be regulated, and which aspects will be the first to be regulated.

4 Metaverse and Traditional Technology

The first topic that will be explored is the metaverse with respect to traditional technology. Traditional technology as defined by this scope, are systems that do not utilize blockchain, such as Amazon Web Services, Google Cloud and Microsoft Azure. These three companies are examples of cloud computing companies that provide its resources for others to use. The theory behind this chapter is to dig into the technological landscape of this world and uncover its limitation when it comes to building a metaverse on these servers. By locating the critical points of these servers, it will be possible to accurately address them in the next chapter, which will focus on the potential advantages and disadvantages that blockchain has over traditional technology.

4.1. Cloud Servers and Metaverse

The metaverse is comprised of many different elements, making the hosting and development a relatively big project. Since a technical background is already given on the technology, this chapter will look into the aspects that are comparative to blockchain and will aim to find the difference between the two. The aspects that will be looked into are: energy usage, security, scalability, governance, democratization, cost and additional features (such as digital ownership). All of these will be defined in their respective sub-chapters.

4.1.1. Elements of The Metaverse

There are many elements of the metaverse when it comes to the full scale project. However, there is no concrete scientific evidence that states what is exactly needed for hosting and running a metaverse on centralized cloud computing services (Ning et al., 2021; Xu et al., 2022). That being said, the papers are making connections between games and the metaverse, which will be taken as a standard for this part, with the addition of features such as training AI models, and optimizing models and simulations (Xu et al., 2022). This essentially means that the metaverse will need extra computing power compared to traditional games in order to sustain the project. In addition to this, the metaverse is also expected to have legally binding contracts, with which users can purchase real estate and other goods. These contracts themselves do not have additional protection when done on cloud computers and rely on the security of the data centers themselves.

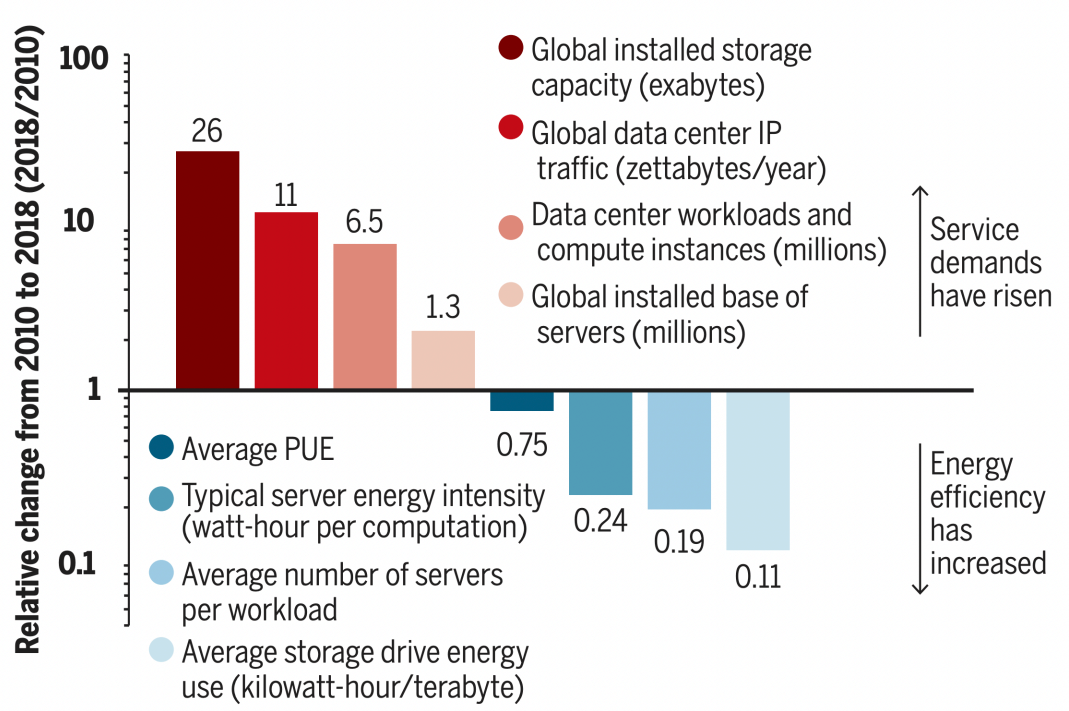
All of this essentially means that there are five main components that will be compared between cloud computing and blockchain: Energy usage, security, scalability, governance, democratization, costs and additional features. A comparative overview between cloud computing and blockchain of all the discussed aspects is given in chapter 5.4 in table 5.2.

Energy Usage

While energy usage might be overlooked and labeled as irrelevant by some, recent scrutiny's against Bitcoin for its inefficiency have made it an import topic to uncover (Cuen, 2021). However, measuring the exact energy usage of cloud computers differs widely per application and specific scenario.

While many policy makers might believe that cloud computers are giant warehouse-sized computers that consume many Terra watts of energy, recent studies show otherwise (Lohr, 2020; Masanet et al., 2020b). Research conducted by Masanet et al. (2020b) looked at the increase in usage of certain cloud computing services as well as the average efficiency increases. For example, the authors found that many of the cloud computing services increased significantly in the time period between 2010 and 2018 (Masanet et al., 2020b). Workloads of global data centers and compute instances increase by more than sixfold and internet protocol (IP) traffic by more than tenfold. The biggest increase however, was in storage capacity, which grew more than twenty-five times in the same time period. However, while these usage has increased, electricity per computation has decreased by a factor of four, and the usage per terabyte of installed storage by a factor of nine. Comparing both the increase in the servers, computers themselves, as well as the efficiency of computers, the net increase is much lower than what analysts presumed. The last metric that Masanet et al. (2020b) looked into, was the increase in the average number of virtual machines instances hosted per server, which have increased by a factor of five.

Figure 4.1: Trends in global data center energy-use drivers (Masanet et al., 2020a)



Some of the mentioned metrics are visualized in figure 4.1, which compares the respective increase and decreases in the usage and energy efficiency of cloud computers. On the left of this figure, the increases are illustrated as a factor between 2010 and 2018. As shown, there were 26 times more globally installed storage capacity in 2018 compared to 2010. However, in the same time period, the kilowatt-hour per terabyte has decreased by a factor of 9, thus the additional storage yielded a net increase of *only* a factor of 2.89. Overall, the researchers found that the total energy consumption of data centers, increased from 92 Terra Watt hour (TWh) to 130 TWh, a net increase of just above 40%, while usages of the technology have increased by a much larger factor.

Unfortunately, it is difficult to measure the exact usage of electricity per GB stored per month or per computation. Nevertheless, it is safe to say cloud computing has become much more efficient, and is continuing this trajectory today, as the increases in efficiency are a combination of both hardware and software improvements (Kirvan, 2022).

The lack of exact numbers per computation makes it difficult to get an exact number for a metaverse example. The only exact number given is the kWh per terabyte of data, which is a metric that can have comparisons to the blockchain. While not accurate, it could also be used as a reference number to compare other metrics such as computation and hosting.

Security

The security of cloud computers has been discussed in chapter 3.1.2, here some of the weaknesses will be looked at as well as what it could mean for the metaverse.

It is crucial to have the best security possible when it comes to cloud computers, which is not always the case as there have been several data breaches in the past (Siyal, 2022). According to Yesyev (2022), many of the breaches seem to be regarding misconfiguration of security settings. Misconfiguration refers to a breach in the system by an outsider that portrays themselves as an authorized figure (Sandler, 2022). This can leave the system vulnerable and the attacker will have access to all the data that would be available to the person that the attacker is characterizing as. These types of breaches can be minimized with the use two-factor authentication and the use of stronger passwords. However, it is a security risk that is difficult to overcome from the cloud computing's perspective. The best way to tackle this is to educate the clients of cloud computers and familiarize them with the necessary extra security steps.

Another report by Jumpfactor (2022) also outlined that misconfiguration is the worst security issue, and cyberattacks come in second; which makes up 20% of the investigated incidents. Cyber attacks directly attack the servers themselves, rather than going through the client. Jumpfactor (2022) recommends performing threat assessments on the system in order to identify weaknesses and gaps in the organization's cyber defense technology.

The two issues mentioned above are the most prominent ones when it comes to security of cloud computers. As for the metaverse, this would mean that the company that builds the metaverse and thus is a client of the cloud computing services, must do its best to minimize these risks. However, security threats will still exist and it will still be a risk for the users of the metaverse.

Scalability

When looking at scalability of cloud computers, there are two important metrics to consider: scalability and elasticity (Lehrig et al., 2015). While the two terms might sound similar, there some key differences between the two.

Elasticity of a cloud computing system refers to its ability to handle sudden and temporary spikes in traffic or computation (VMware, 2022). This could happen if everyone decided to go on a certain website, which suddenly increases its traffic and the computational power needed to sustain that website. This would not last very long and it is therefore crucial that the cloud computers act quick enough to facilitate for a sudden increase in demand (Mohanan, 2022). Elastic computing allows the client to adapt a pay-per-use feature, which could be cost effective for certain applications.

Scalability of a cloud computing refers to its ability to increase the workload with its existing hardware sources (VMware, 2022). Programs can scale either vertically (with a certain system) or horizontally (scale out to multiple systems, which is usually not linear) (Ben-David, 2021). This can be done when long-term growth is expected at which point the IT department can decide how much extra computation or storage is required for a certain business to not limit its growth for cloud computing.

For cloud computing companies the ideal solution is to offer the option of having both an elastic and a scalable solution for building a metaverse. As the metaverse continues to grow its user base, it can scale horizontally to more servers and, although not linear, will be able to facilitate the continuous and expected growth of the space. On top of that, the field might see sudden increases in demand, such as certain NFT releases that have had such high demands that blockchain has crashed as a consequence (PYMNTS, 2022). These events make the elasticity of cloud computing very attractive for developers of this space.

Governance

Governance of a cloud computing refers to a set of rules that dictate the cloud computer (Gill, 2022). The governance system of a cloud helps the cloud in managing the system and ensuring it is effective and efficient with its resources.

Ahmed (2021) outlines what the governance of cloud computers are built for. Essentially, the enterprises design the governance protocols and manage them. The author goes into further detail on five governance principles that should and must be adopted by cloud computers. While it is not necessary to discuss each in detail, one of them addresses the compliance issues that might be faced and another one is focused directly towards the client of the servers. The other three are more focused on the business and optimizing the process. Important to note is that the developers and corporations have full control on the governance protocols. While these groups could in theory listen to their customer base and implement some of the feedback that is given, the customers have no direct control over its development.

What this means for the metaverse is that it would be entirely controlled by the corporation that owns the data server that the metaverse is built on. Additionally, projects that do not comply with any of the principles or policies of these data centers would likely only be available to limited users, or deleted entirely. This could have severe consequences for the space, as it might not be possible to run the code on another cloud computing enterprise and be involved in the same metaverse.

Democratization

Democratization can be defined as two ways. The first definition comes from the technology's ability to offer itself to smaller groups of people and thus equaling the playing field compared to big corporation (Pakhira, 2019). The second definition focuses on the democratization of power within the ecosystem. While both of these definitions will be discussed in this sub-chapter, the latter definition is similar to the governance of the ecosystem and will see similarities.

As per the first definition, Pakhira (2019) mentions that cloud computing is a very democratizing technology, as it allows smaller companies the access to the same level of technology as the largest corporations that currently exist. This means that a small startup has the opportunity to use the same hardware as Google or Amazon. Cloud computing has greatly reduced the barrier to entry with its multiple deployment models, allowing for small businesses to utilize the technology. This is about as *fair* as it can get, as bigger companies do not have a significant advantage over others. However, there might be an advantage in the actual hardware that the larger companies can use compared to the smaller startups. This can be seen on Azure (2022), where prices increase dramatically when more advanced hardware is chosen. Thus, while all players in theory have access to the same technology, only some may be able to afford the best options that will yield the best results and could create a bigger gap between large and small companies in the field.

The second definition refers to whether people can have a say in what happens on and around the cloud computing network. This is similar to the governance of the technology, which was discussed in the previous sub-chapter. Unfortunately, for cloud computing there currently is no such thing as democratization of 'power' (Ahmed, 2021). While this could change in the future, the fact of the matter is, the enterprise has full control on what happens on the network and has the final say.

The metaverse is expected to be a big digital world with large corporations dominating aspects of the field. However, similar to the real world, there will be startups competing in one aspect or another with the large firms by bringing something new to the table. Cloud computing will not give the bigger players an advantage in this battle and will ensure a level playing field as far as hardware is concerned.

Costs

When it comes to costs, there are different elements that contribute, such as the service model. Depending on what is needed by the company creating the metaverse, the price could change drastically.

SAAS refers to cloud computers that simply store any data where users pay a monthly fee to their providers (Yu et al., 2010). While this paper puts the cost of 1 gigabyte between $0.12 and $0.15 per month, these numbers are already more than a decade old and prices have dropped significantly since then. More recent numbers show prices anywhere between $0.001 and $0.15 per gigabyte a month, depending on bundles bought and how frequently the customer accesses the data (Microsoft, 2022).

Looking at IAAS, Azure offers many different options on their website depending on the specific type of computations needed (Azure, 2022). The options range from low end virtual machines (VM) with 1GB of RAM and storage up to models of the latest processors of AMD and Intel with Terra bytes of RAM and storage in the VM. Azure's entry level server machines start from around $50 up to $2340 with added CPU cores, RAM and storage for one year (Azure, 2022). Although it would be preferable to have a pay-per-use structure, it is not possible when using the IAAS service model. Regardless, when making the same comparison on blockchain, a better understanding can be made of the exact price differences, as the hardware of the blockchain can make an impact on what hardware to compare it to on Azure.

Tying this back to the metaverse is slightly more difficult than previous metrics, as it is highly dependent on external factors, such as the size of the digital world, efficiency of the code, and storage. The creators of the metaverse can opt to go for pay-as-you-go structure and only upgrade the VMs when reaching the limits of the current computations.

Additional Functionalities

While most of the essential features have been discussed, there are some additions needed in order to have a fully functioning digital world. One of the main aspects is the digital ownership of goods.

As far as digital ownership goes, it is relatively simple, whoever has access to the account where the data is stored, owns it (Chima, 2016). While this should be enough in most cases, it was previously mentioned that cloud computers lack security, especially when it comes to misconfigurations and cyber attacks. Both of these can lead to the loss of data and digital goods of the rightful owner. This could have severe consequences for the original owner of the data, whether that is an individual or a corporation.

Since everything will be digital in the metaverse, including ownership of digital real estate and other goods, this is an area that must be improved in the future. As it stands now, the attacks can lead to the rightful owners losing their digital assets, which can be worth tens of millions of dollars.

4.2. Specific Weaknesses and Strengths

Having covered all of the relevant aspects of cloud computing in the paragraphs above, a clear overview of the challenges can be made with regard to building a potential metaverse.

First of all, since the metaverse is still a very new concept with unknown potential, it is difficult to pinpoint its exact challenges and shortcomings. However, as mentioned previously in chapter 3.1.2, many of the weaknesses of cloud computing comes from its security issues. These issues are not necessarily all of the servers themselves, but also include accessing the cloud computing services from the client's perspective. In the hypothetical sense, this can be a great threat in the metaverse. Personal data can be users, as well as possible legal contracts that have been created and signed in the metaverse:

the information of which can then be used by others. This can have adverse impacts for users of the metaverse and could lead to lower trust in the new digital world, reducing its adoption. Other limitations are the adoption of smart contracts without the use of a blockchain, as they could also be altered by cyber-attacks, which are the second biggest threat to cloud computing.

Besides these challenges, there are not many drawbacks on building a metaverse on cloud computing. One might say that from some perspectives, it could be relatively advantageous, as one can scale the needed cloud computers together with the growth of the metaverse. However, when looking at the broader picture and also what the metaverse would stand for; a digital copy of the world, it becomes impossible not to include crucial elements such as digital ownership and data privacy of the users. This aspect is where current cloud computing technology is lacking, with a more in-depth comparison available in the next chapter.

Reflecting back to the second research question that was formulated earlier on in the thesis, there are several challenges when it comes to building a metaverse on cloud computing software. First of all, the misconfiguration attacks are a great threat that can influence the usage of the metaverse, as users might be as likely to share any personal data if these attacks are very common. The successful cyber-attacks on the cloud computers also pose a big risk to the data of the users and can lead to less people trusting the platform. Other than this, the aspects are either neutral or beneficial for building a metaverse on cloud computers.

4.3. Conclusion

Several aspects of cloud computing has been dissected and looked into in regard to building a metaverse on the platform. While the different service models along with the deployment models that could be utilized by the metaverse were discussed in earlier chapters, this chapter focused more on metaverse specific applications. The general strengths of using cloud computing are: low costs, easy maintenance and scalability. However, there are some crucial challenges of this technology when it comes to building a metaverse on it.

There are several challenges for CC that make it difficult to build a metaverse on it and could force developers to explore other technology for this purpose. The first one of those is the data security aspect. Two of the most frequent type of data breaches in CC are: misconfiguration and cyber attacks. While the latter is commonly more known, the former could enable attackers to pose as a metaverse user, log in to their account and transfer all the goods to someone else. Another crucial part that is missing in CC is that there is currently no standard for digital ownership. As the metaverse is expected to be a vast virtual world with many users and digital goods, there must be some sort of verifiable procedure to ensure the digital goods are authentic and track its transactions. The governance of a metaverse built on cloud computing would also be very centralized, giving the enterprise the control over which projects can run on their servers and which cannot.

This chapter was aimed at answering the second sub-question:

What are the main technical challenges currently faced by the current technology (i.e. cloud computing)?

The main technical challenges are the security and verifiable ownership of digital goods. As of now, these two aspects are lacking in for building a metaverse on cloud computers and must be solved before a metaverse can be built on this platform. Other challenges are less technical, such as the centralization of governance and democratization of power. While these two are also technical in its core, it is the opinion of the users on this matter that would drive them away from a metaverse built on this technology.

5 Metaverse and Blockchain

The previous chapter discussed the aspects of traditional technology, this chapter will focus on how the metaverse could be hosted on the blockchain. While this can be done in different ways, the main aspect is to make a comparison between the two and evaluate the strengths and weaknesses of both. First, an overview of blockchain is given with the different infrastructures that are possible. Once a firm understanding of this is given, the advantages and disadvantages of each structure will be compared to that of traditional technology. Doing so will yield a clear overview of what blockchain does better and where it could still potentially improve. Moreover, it will open a path for the next chapter, where regulations and policies will be applied.

5.1. Blockchain Overview

There are generally two types in which a blockchain can host a project like the metaverse: hybrid and fully on-chain. Both will be discussed and explained below in order to give you an overview.

5.1.1. Hybrid Structure

Hybrid structures refer to arrangement in which the data is stored on a blockchain, which in this case can be both on-chain and off-chain. When taking data off-chain, one is depending on the security of the new storage device, compared to that of the blockchain. By taking data off-chain, one is transferring the data from the blockchain it was originally on either a local computer or cloud computer. This can be done on the Ethereum network, with NFTs being taken off-chain in some cases. This means that the NFT is now stored on either a local or cloud computer and not on the network anymore. This process is reversible, and it is thus possible for NFTs to be taken on-chain again.

While cryptocurrencies and blockchains are known to be decentralized and not controlled by centralized organization, such as governments and data servers, some experts claim otherwise. In 2020, a Bitcoin enthusiast had pointed out that nearly 70% of all the nodes on Ethereum run on AWS servers (Malwa, 2020). One important aspect to note is the difference between a miner and a node, as there is a difference between the two. According to Tarcan (2022), a node is a system that runs a piece of client software. Essentially, a node can store all the blockchain data and this information can be requested by users of the network.

5.1.2. On-Chain Structure

Contrary to blockchain where data can be taken off-chain, there are also blockchains where everything is hosted on-chain, most notably of which is ICP. ICP is a blockchain that stores all its data on-chain and can be queried and updated at any time (D. Williams, 2020). This structure allows for all the data to be called upon when requested, however, it does increase the size of the chain. This is evident when comparing the Ethereum chain size to that of ICP, which are approximately 656GB and 945GB, respectively (I. C. Association, 2022; Buterin, 2022). While this does not sound like a big difference, it is important to note that Ethereum started in July of 2015 and ICP started in May in 2021. Thus, the ICP ecosystem can store a lot more and be more efficient with the data.

One of the key differences between on and off-chain structures is where the data is stored and how it can be accessed. Moreover, as more personal data gets stored on the blockchain, the on-chain structure must adhere to the GDPR regulations (GDPR, 2022). This is easier said than done, as blockchains are inherently decentralized, unknown and changing location as anyone can become a node on the network. This will then reduce the decentralization of the network. However, this loss in decentralization could increase the scalability and security as per the impossible triangle.

For the purpose of this thesis, as the ideal scenario is that the whole metaverse is built and hosted on a blockchain, the on-chain structure will be followed and taken as reference point. It limits the blockchains that can be used in comparison to cloud computing, but will give a clear overview of the differences between the two and what is needed from a regulatory standpoint.

5.2. Blockchain Strengths and Weaknesses

The strengths and weaknesses of blockchain, involves different consensus mechanisms prioritizing different aspects, as discussed in chapter 3.1.3. However, a general perspective will be taken into account, as well as the perspective from third generation blockchains, which establish the baseline to build a potential metaverse on. Examples of these types of blockchains are: Solana, Polkadot and The Internet Computer (Conor, 2021; Parga, 2021).

5.2.1. General Blockchain Strengths

Blockchains in general have different strengths depending on which blockchain is looked at. That being said, there are still some strengths that are universal across all blockchains.

IBM (2022), reports five crucial benefits of using blockchain technology, namely: enhanced security, transparency, traceability, efficiency and speed, and automation. These are crucial metrics when it comes to building a metaverse on a blockchain, especially in terms of security, as it is one of the major challenges of cloud computing. However, the security of a blockchain highly depends on its consensus mechanism and can thus differ widely from one blockchain to another (Sayeed & Marco-Gisbert, 2019). The same can be said for the efficiency and speed. Analysis conducted by Parga (2021) shows the transactions per second (TPS), finality and blocks per second of popular ones. Within this list of nine of the most popular blockchains, the blocks per second metric ranges from 0.05 to 22.5 (although more recent numbers put this number at 35, creating a bigger difference (I. C. Association, 2022)). Blocks per second is not the only metric that matters, as the TPS of a blockchain ultimately decides how many transactions the blockchain can handle. However, even this metric changes widely from Ethereum's 15 TPS to Solana's 50,000 TPS. The other mentioned metrics: transparency, traceability and automation hold true for all blockchains as long as its a public blockchains. These five advantages are at the core of blockchain technology and with new developments constantly rolling out, it is only a matter of time before there are more (Zadikoff, 2021).

5.2.2. General Blockchain Weaknesses

As with cloud computing, blockchain too has its disadvantages that could play a major role in the adoption of the technology and building a metaverse on it. One aspect that one must keep in mind when discussing these shortcomings is that blockchains can evolve over time with upgrades to its network, such as Ethereum moving to the PoS consensus mechanism from PoW (Deer, 2022).

Although the analysis conducted by Brett (2018) is slightly outdated, some the elements are still valid today. The two most prominent arguments that the author makes are that blockchains inherently use a lot of energy and have scalability issues. The same arguments are made by Sam (2022), and thus these seem to be blockchain's greatest weaknesses.

5.3. Blockchain and Metaverse

As mentioned in chapter 4.1, the metaverse is a complex landscape that requires many element to be created. In chapter 4, certain metrics were taken into account for building a metaverse on cloud computing. In order for fair comparisons to be made, the same metrics will be used to assess the quality of blockchain and its potential to create a metaverse on it. Since it is difficult to assess blockchain in general on each of the metrics, as these differ widely from one blockchain to another, some metrics might put a focus towards a specific blockchain or group. Earlier, it was mentioned that the focus will be on third generation blockchains, such as: Solana, Algorand and ICP. When possible, this group will be compared on a metric. However, if there is still a wide range within that group, one specific blockchain from the list will be taken into account. This blockchain will likely be ICP, as they have had the most development done within the past 3 months and have one of the biggest growing teams within blockchain (Claeys, 2022; Shen, 2022).

5.3.1. Elements of The Metaverse

Energy Usage

The energy usage of a blockchain is highly linked to its consensus mechanism, as PoW and PoS have significant differences in the energy that they use per transaction or block on the blockchain (Bada et al., 2021). However, as mentioned before, the focus will be on third generation blockchains, which use more efficient mechanisms and thus use less electricity per transaction. Moreover, the speed of these blockchains are faster as well, as outlined in the strengths of the blockchain, further increasing the efficiency. That being said, the total energy usage of a blockchain differs widely from one to another. For example, Friedman (2022), outlined the energy consumption of both Bitcoin and ICP per transaction and found that bitcoin uses approximately 2131kWh per transaction, versus the ICP that uses 0.00036kWh per transaction. First of all, this shows how far blockchain technology has come since the introduction of bitcoin. Second, it puts the differences into perspective as the new third generation blockchains are getting better each year. The exact difference is a factor of over 5.8 million, which is a very significant increase in energy efficiency over a development cycle of just over a decade.

While it is difficult to make a clear estimate as to how much energy the metaverse would consume, it is safe to say that the development is going into the right direction. At the time that Friedman (2022) made the analysis, the servers running the ICP blockchains were estimated to consume 1kW each. There are currently 518 node machines on ICP, creating a total of 35 subnets on the blockchain, meaning that 518kWh of energy is being used each hour. This comes to a total of 372 GWh per month, compared to bitcoin's 10TWh. Additionally, on top of sending transaction, users of the ICP blockchain can query and update calls, as well as store data on the network at one of the cheapest rates compared to any other public blockchain (Watts, 2022). All of these extra functionalities have not been taken into account, as they can differ widely from one aspect to another.

These developments make blockchain a suitable candidate to create a metaverse on. This continuation of energy efficiency is what will make blockchain an even fiercer competitor in this regard to cloud computing and building a metaverse on it.

Security

Security is one of the major flaws of cloud computing technology, as discussed while answering subquestion 2. However, when it comes to the security of blockchain, it is one of the main advantages and selling points.

While blockchains are immutable, it is possible to take control of the network for future transactions. Depending on the consensus mechanism one needs at least a 51% stake in the blockchain or control its network in order to do so (Nakamoto, 2008). In Ethereum's PoS mechanism, the theoretical value at which a malicious actor could use the network to its advantage is around 51%. Attackers must therefore own at least 51% of the total staked Ethereum on the network. Today, around 12,000,000 Ethereum tokens are staked on the network. Therefore, one must increase this number to 24,500,000 in order to take control of the network. In terms of US Dollars, this equates to $41.6 Billion; not taking potential price increases into consideration due to buying large amounts of Ethereum. There are very few corporations and individuals that have such wealth, making this very unlikely. Moreover, the network could potentially identify malicious actors like that want to control the network and can be forked away by the stakers from the network (Gu, 2022).

One of the main issues of security in blockchain however, is code exploitation. This has been seen in many cases, such as flash loans and most notoriously: the Terra Luna collapse (M. Williams, 2022). While the latter was not necessarily direct exploitation of the code, it is assumed that the individuals that caused it knew what the result would be (Ngari, 2022). This can be a serious issues, especially since all the codes are public (in the discussed blockchains) and can thus be seen and studied by anyone with internet access. The attackers would study the code, find flaws and then exploit those with only their own interests in mind. This often causes significant monetary damages for other users and the developers themselves. One simple way to fix this is by peer-reviewing the code by colleagues and potential third parties, which could bring more security to the smart contracts. However, there are always risks involved, as anything can be overlooked.

Another issue with security is the management of keys and passphrases. While these are most often secure enough, the users that hold them can either lose them or give them away unwillingly by not storing them in an encrypted environment. This issue is similar to the misconfiguration problem of traditional technologies.

While these issues are expected to persist in the future when a metaverse will be built on it, the mentioned improvements are already being implemented and are expected to increase and improve the blockchain. Moreover, with users gaining more experience with the technology and education on blockchain becoming more available as time passes, it is expected that users will have a better understanding of where to store their private keys. The main risk that will still persist in the metaverse will likely be code exploitation, which could be used to obtain more digital assets. However, even this risk will be significantly reduced by the time this technology becomes widely available, as the mentioned services already exist for some computing languages and will undoubtedly be altered to suit smart contract languages, such as Solidity, Go and Rust.

Scalability

Scalability is one of the major drawbacks of blockchains, as they traditionally do not scale linearly with the addition of extra nodes and/or miners. However, new blockchains seem to have solved this slightly by coming close to linear scaling of the blockchain. ICP is again one of the best examples, as their chainkey cryptography can ensure that the addition of node machines on the network can automatically generate new subnets if there are enough. Essentially how this works is that node machines get added randomly to a subnet, increasing the number of machines on a single chain. Once there are enough machines to create a new subnet, they will deviate from their old subnet and together form a new one. As each one produces approximately 1 block per second and is identical in performance to any other subnet, this allows for linear scaling of the blockchain.

When discussing the scalability of the programs within blockchain, ICP again is a great example. Since the subnets on the blockchain run in parallel, canisters (which are bundled up smart contracts) can be deployed on different ones, thus ensuring that there is always enough room for other processes. Moreover, as each subnet is run by multiple nodes, there is room for growth within each canister, since there will always be room within the nodes for sudden spikes in traffic.

For the metaverse, this means that scalability should not be an issue when created on ICP or a similar blockchain. The blockchain has enough flexibility to scale with the program and leave room for peak traffic times. This will give the metaverse room to grow into the blockchain and not be limited by the platform it is being built on.

Governance

The governance of blockchains involves two aspects; dictation by both developers and users. On-chain governance can have many different forms and can be implemented into the blockchain in a variety of different ways.

On-chain governance refers to upgrading blockchains according to changes in code that is voted on by stakeholders (Reiseman, 2022). These upgrades can range from minor tweaks to drastic changes, such as the Ethereum network switching from PoW to PoS. Since this is being done by stakeholders in the network, the voting power is usually a function of the capital that is staked. While this concept favours those that stake more capital in the network, everyone gets a vote on the proposed upgrades. This is a form of a DAO, as the structure (smart contract code) is laid down beforehand. The NNS of the ICP blockchain puts this theoretical concept into practice. Users of the NNS can stake the native cryptocurrency for a period of 6 months to 8 years, with longer lock up period receiving more rewards. Users can then vote on proposals and automate this process to a certain extent.

Some problems may arise with copyright or trademark issues in this case, as there is not a single entity that controls everything and can simply shut it down. Since the DAO will have full control over anything that goes on in the network, it also becomes responsible for decision making. While this can pose a problem in the future, there has already been an incident where a game created by Nintendo™ was uploaded to the ICP network, giving everyone access to the game. Nintendo followed up to this incident by sending a notice to remove it from the blockchain. However, since there is no single entity in control, it is impossible for the Dfinity Foundation to simply delete the canister. They therefore submitted a proposal to the NNS to delete the canister, which was passed shortly after the submission. This is a significantly longer and more difficult process compared to other technologies, but it can have both benefits and consequences when similar problems arise in the future.

The example given above is a great illustration of how a blockchain governance system would work in the metaverse, as similar issues can arise in that environment. Moreover, any system upgrades in this metaverse would have to be approved by the stakeholders, which are mostly assumed to have the best interest in the network. Thus, these individuals and organizations are expected to vote in favour of new developments in the space. It is still uncertain how the exact structure will look like when the time comes, but what is certain is that it will always be possible to submit proposals to fix issues and improve the network and metaverse.

Democratization

Earlier on, two definitions of democratization were given, which will again be used in this chapter. As a quick reminder, the first definition looked at democratization of the technology while the second focuses on the power within the ecosystem.

The first interpretation can be looked at from both a holistic and a more detailed view. When looking at the big picture, it is important to remember that blockchains are made up of nodes and miners (in some cases, a node can be a miner). The nodes are the hardware that power the smart contracts, while miners take care of the transactions that happen on the blockchain. In some blockchains, the nodes are not standardized, meaning that they can have different grades of hardware, while maintaining a minimum specification. The benefit of this is that no matter the application or individual, everyone that runs smart contracts on these blockchains will be treated the same. The downside is that in some cases this costs a lot of money which poses a big barrier to entry. Eric (2021) has conducted an analysis on the fees needed to deploy a smart contract on Ethereum, which are estimated between $500 and $10,000. For small developers, this is not a feasible amount to spent on deployment of smart contracts, especially if something goes wrong and the developer has to redeploy the project. However, recent advancements have made is significantly cheaper to deploy smart contracts on a blockchain. While some aspects will be discussed later, table 5.1 gives the exact number of cycles needed to deploy a canister, which is approximately $0.15. This fee does not depend on the type of smart contract deployed and this levels the playing field between small and big players in the industry.

The second definition is again highly linked to the governance within the network, which can range from very decentralized to somewhat less. The ICP blockchain has a very open governance system, where anyone can submit a proposal for possible upgrades on the network. These are usually discussed beforehand on the developer's forum to reach an agreement and find improvements before submitting the proposal to the network. Since the only cost for doing this is a potential 'rejection fee' of 1ICP (±$9), virtually anyone with technical knowledge can submit them (Dfinity, 2021). The voting can be done by anyone that stakes the native cryptocurrency and locks it up for a minimum period of 6 months, doing so creates a neuron. The voting power of these neurons is proportional to the amount that is staked with possible bonuses. While this system favours the wealthy that have more capital to stake, there is not one single entity that has a majority of the voting power.

Both of these interpretations show that any developer can build on the metaverse, and any individual can have an impact on future developments of the ecosystem that it is being built on. The democratization of both technology and power is clearly evident. The extremely low fees combined with providing the same technologies for all parties building on the blockchain prove that democratization of technology is undeniable. Anyone that has an internet connection, and that can gain knowledge of the programming language, can start building on the ecosystem and make proposals to improve the blockchain. This can be anything from creating a new digital space where people can live to making small accessories.

Costs

Cost is another metric that differs widely from one blockchain to another. One important element here is that it must be possible to store data on the blockchain, which is something that has not been made very affordable.

The Ethereum network works with gas fees, making it naturally very expensive for users to store data on the blockchain. Kostamis et al. (2021), have conducted an experiment showcasing the gas costs needed to store bytes on the network. The authors found that storing 12KB of data on the network can cost up to 7 million Gwei, equalling 0.007 Ethereum tokens. At the time of writing, this would put the cost of 12KB of data on the blockchain at $13.7. Scaling this up to MBs, GBs and even further to TBs will become unfeasible for developers and individuals. Some estimates put the price of storing 1GB of data on the Ethereum blockchain at $40 Million (Lehmann, 2022).

Taking the comparison one step further to a third generation blockchain that can host everything on-chain, the cost gets reduced heavily. Guide (2021), outlines the cost of storing 1GB of data on the ICP blockchain for a year at 4 Special Drawing Rights (SDR). The SDR unit is created by the International Monetary Fund and, while not a currency, can be used to denote other currencies, such as the US Dollar, Euro and Yen (IMF, 2021). At the time of writing, the approximate cost of 4 SDR is 5 Dollars, which means that 1GB costs $5 per year. This is almost a 10 million factor reduction from Ethereum's cost and could be feasible for developers, if the size does not exceed several hundreds of Terra bytes.

Besides the costs for storage, there are also costs associated to computation, which the ICP denotes in

Table 5.1: Table depicting the operation as well as cost of selected computation on The Internet Computer Blockchain (D. Association & ICA, 2022). Conversion rate as of June 2022 ±750 Billion cycles per US Dollar.

Operation	Description	Cycles
Canister Creation	For creating canisters on a subnet	100,000,000,000
Compute Percent Allocated Per Second	For each percent of the reserved compute allocation per second	100,000
GB Storage Per Second	For storing 1 GB of data per second on the blockchain	127,000

cycles, see table 5.1. As one can see from this table, the cost of using one percent of the compute power costs 21% less than storing 1 GB worth of data. This means that using one percent of the compute power will cost around $4 per year. With server grade hardware, as well as continuous upgrades for both hardware and software, these costs are expected to decline (Pena, 2021). Additionally, the author notes that there will be a second generation of servers that the ICP blockchain will utilize, which is expected to drastically decrease the current costs.

As one can see, the costs for storage differs widely per blockchain and it is therefore difficult to pinpoint an exact number. However, taking ICP as a reference point, it becomes clearer and gives a better comparison metric to cloud computing. When it comes to the metaverse, it would definitely be feasible to build it on a blockchain. The comparison of the metaverse earlier was made with games, and the same comparison can be made here. With the current biggest game being 165GB in size, it would cost developers only $825 to (theoretically) store the game on the ICP blockchain and deliver it millions of users.

Additional Features

While the additional features of cloud computing are limited with respect to the metaverse, there are some blockchain concepts that aid in the development of the space. One of these examples are NFTs, which are discussed in chapter 3.1.3. This technology gives a new meaning to digital ownership, which is both verifiable and secure. This can be useful when, for example, dictating which user owns something. NFT smart contracts have already been standardized on the Ethereum and ICP network, with the ERC-721 and DIP-721 standards, respectively. These standardization help the creators of NFTs, as they make it easier to launch NFT projects.

Besides verifiable ownership, users must pay for their goods using a digital currency. Since most, if not all, public permissionless blockchains have their own cryptocurrency, it is easy to pay for goods using that. However, these currencies can be incredibly volatile and users might not want to get paid in this form of currency. Thus, a digital currency that is pegged to a FIAT currency could also be an option, for instance the USDT, BUSD or USDC stablecoins. These coins are pegged to the US Dollar and should, in theory, always hold this value with an insignificantly small margin.

5.4. Blockchain vs. Traditional Technology

Now that both traditional technology and blockchain technology have been analyzed with respect to the metaverse, a comparison will be made on all the aspects discussed in chapter 5.3.1 and 4.1.1. The benefits and drawbacks of each technology on each segment will quickly be summarized, whereafter a superior technology will be chosen to investigate further.

For some aspects that have been discussed for both blockchain and traditional technology it is complicated to dictate exact numbers. This can for example be seen in the energy usage of the two technologies. For cloud computing, the total energy usage of the servers is known. However, since these servers perform a multitude of tasks, it is difficult to examine how much energy each task consumes.

The same can be said for the servers on the ICP blockchain. Besides energy usage, the costs of blockchain is another metric that is intricate to compare. While the exact numbers for both the storage costs and computational costs are known for specific blockchains, not every network has these capabilities. This complicates the comparison between the technologies.

The table below has been created to aid in this comparison to give a clear-cut overview of both technologies. The aspects of traditional technology are given on the left and on the right blockchain technology.

Table 5.2: Comparison of cloud computing and blockchain technology on the aspects that have been analyzed.

Traditional Technology	Blockchain Technology
Energy Usage	
• Known to be very efficient and will keep increasing in efficiency. • Server grade hardware makes it very efficient. • Energy usage depends on scale of project.	• Efficiency highly depends on consensus mechanism. • New blockchains are increasingly energy efficient. • Server grade hardware makes nodes on blockchains very efficient.
Security	
• Misconfiguration allows attacker to pose as original user. • Cyber attacks steal data from servers. • Proactively working towards improvement. • Both will still be a risk for metaverse.	• Prone to 51% attacks for PoW and 66.7% attacks for PoS. • Code exploitation in flawed smart contracts. • Management of personal keys and passphrases.
Scalability	
• Both elasticity and scalability are available. • Good for both growing projects and sudden spikes in traffic.	• ICP allows for linear scalability of network with added nodes. • Canisters on ICP can run on parallel subnets, ensuring availability of resources.
Governance	
• Enterprise controls governance. • Developers can have indirect influence on outcome. • Users have no influence on outcome.	• Governance of blockchains are decentralized. • Developers can submit proposals, users can vote on them. • Voting power of users is a function of invested capital.

Table 5.2: Comparison of cloud computing and blockchain technology on the aspects that have been analyzed.

Traditional Technology	Blockchain Technology
Democratization	
• Democratization of technology is present to a certain extent, as more capital can purchase more advanced hardware. • Democratization of power is not present.	• Developers cannot choose which node to run their smart contract on, allowing for high level of democratization of technology. • New blockchains make it cheaper to run smart contracts, removing the capital barrier to entry. • ICP allows anyone to submit proposals for network improvement. • Anyone that has staked native cryptocurrencies on PoS based blockchains, can vote on proposals.
Costs	
• Price depends on chosen hardware. • Costs are constantly decreasing due to improved hardware and software. • Storage costs are between $0.01 and $1.2 per GB per year.	• Older blockchains such as Ethereum are inherntly expensive to develop and deploy on. • ICP reduced this cost by a factor of nearly 10 million. • Storage costs on ICP is approximately $5 per GB per year. • Computation costs are $4 for every percentage of computational power of a node.
Additional Features	
• No clear additional features that would benefit the metaverse.	• NFTs allow for verifiable digital ownership of goods. • Digital currencies can be created with the help of currency standards, such as ERC-20 and DIP-20.

The comparison above gives a clear overview of the main similarities and differences for each one of the 7 categories that has been investigated in the previous chapters. Both of these will be outlined and examined in detail for building a metaverse on either technology, with the aid of table 5.2.

5.4.1. Similarities

The main similarities can be seen in the following aspects: energy usage, scalability and costs. Even though one technology might be more scalable than the other, rather than looking into the 'better' technology, the ways in which the technologies are similar will be discussed.

As for *energy usage*, traditional hosting technology has come a long way in terms of energy efficiency and progress is still being made, as illustrated in figure 4.1. Likewise, blockchain technology has also come a long way in this respect from inefficient consensus mechanisms, such as PoW, to much more efficient mechanisms, like PoS and chain key cryptography. While some might argue that currently traditional hosting technology is more efficient, they have both come a long way and will continue to make improvements in this respect, as the world is shifting to a more sustainable future.

Scalability is another aspect that is similar between the two technologies. Traditional hosting technology, as of now. has more scalability and elasticity; blockchain is making similar advancements. PoW is inherently not very scalable, as miners are competing against one another to mine the next block. PoS has made good progress towards being more scalable and has made some good improvements compared to its predecessor. Other solutions, like Solana's PoH or ICP's chain key cryptography are designed to be even more scalable and efficient than the previous two. These continuous developments have helped blockchain come a long way in the field of scalability, but further advancements must be made to come to the same level as traditional hosting technology.

Lastly, similarities can be drawn to the *costs*. Although table 5.2 clearly depicts that traditional hosting technology is cheaper than blockchain technology in all aspects, the manner in which the payments work is very similar. Since not all blockchains can be compared to traditional hosting technology, the main comparison will be to the ICP blockchain. In this blockchain, users pay per second for every GB stored and the computational costs. However, since the costs per second is so low, users can top up their account and use their balance throughout the year to pay for their usage. Similarly, traditional hosting technology offers pay-as-you-go bundles, where users pay for the amount of resources they use for the given time period. Besides this option, users of traditional hosting technology can also opt for other options, such as a monthly subscriptions for a particular package, which is not available on blockchain. Nevertheless, one can see the similarities between the two technologies, although, traditional hosting technologies has a few more options.

5.4.2. Differences

The differences between the two technologies can be seen in the following: security, governance, democratization and additional features. The differences will be discussed from the perspective of hosting a metaverse on either one of the technologies.

From a *security* perspective, there are currently many differences between the two. One of the main differences is how each technology is prone to cyberattacks. In blockchain, the 'easiest' way is to control either 51% of a PoW blockchain, or 66.7% of a PoS blockchain (numbers can vary from one blockchain to another). On the other hand, traditional hosting technologies are more prone to misconfiguration and cyberattacks targeted directly towards the data centers to steal information. While misconfiguration can be compared to the management of personal keys and passphrases to access accounts, cyber-attacks are very different in nature. Furthermore, blockchain smart contracts are prone to code exploitation, which can have a big impact on the other users of the smart contracts, leaving them with very little or sometimes, nothing at all.

The *governance* of each one of the technologies is another aspect in which the two differ. In the case of traditional hosting technology, the enterprise controls the governance of the network. Developers and the corporation have a direct influence on the development of the network, whereas users do not. While users can give feedback, the enterprise is not obligated to incorporate it. On the contrary, blockchains need the approval of users to implement certain network upgrades. Some blockchains only need approval from the public for big upgrades (BTC, ETH), while others need every proposal approved before it can be implemented (ICP). Moreover, on ICP, virtually anyone can submit proposals, given they meet the minimum requirement of 1 ICP token in their account. This makes the development of the technology much more decentralized than traditional hosting technology, which could be both advantageous and disadvantageous, depending on the situation.

Democratization is very similar to governance and its differences. There are 2 main parts to democratization: power and technology. Democratization of power is not present in traditional hosting technology, whereas the faith of some blockchains lie completely in the hands of the stakers in the network. Corporations can own a large percentage of the voting power and have a big impact on the final outcome. However, it must also appeal to some of the stakers if they want to implement certain upgrades. Traditional hosting technology offers different hardware specifications for their users, allowing them to pick and choose which one fits them best. An individual might need much lower requirements for their project than a big corporation, who can both turn to an enterprise such as AWS for cloud computing solutions. Users that want to run computations on the ICP blockchain cannot choose what kind of hardware they wish to utilize. Instead, the smart contracts are run on a random node of the network and occupy a certain percentage of the hardware.

The last category that was discussed was about the *additional features* that the metaverse could make use of. While traditional technology has no clear features that could be useful, blockchain has two distinct ones. One of these features are the NFTs that can be verified on the blockchain for digital ownership. This technology is necessary when verifying the authenticity of certain digital goods in a future metaverse and ensuring that there are no fraudulent items. The second is for creating digital currencies that can be used in the metaverse. These currencies do not have to hold any value to them, they can be structured similarly to 'karma points' on Reddit. However, the possibility to have value attached to them is possible and can be modified by the developer.

5.5. Conclusion

Thus, blockchain technology has been discussed in great detail on all the relevant aspects. First some general concepts of the technology were discussed together with strengths and weaknesses. The most prominent advantages are security and transparency, but it lacks in scalability. Second, a detailed overview on all the discussed aspects of blockchain technology was provided, similarly to what was provided for traditional technology in chapter 4.1.1. In some cases, it was difficult to generalize the results, such as the costs of blockchain. In these sub-chapters, specific blockchains were taken as reference points, most notably the ICP network. Lastly, a comparative table was made to compare traditional technology to blockchain technology. The similarities between the two technologies is the energy usage, scalability and costs. While one technology might be more scalable and cheaper than the other, the mechanisms for them are similar, as well as the potential to improve. The key takeaway here are the differences between the two technologies. Development of traditional hosting technology is much more centralized, and they have no direct impact, while it is the exact opposite in blockchain. This does not mean that one technology is superior to the other, as some users might not act in the best interest of the blockchain or are uninformed on the matter. Another difference is the security aspect between the two, as they have different weak points and are thus prone to different types of attacks. Perhaps the main difference between the two technologies that is most relatable to the metaverse is the additional feature of NFTs for blockchain technology that currently does not exist in traditional hosting technologies. This feature is a key element of the metaverse, as it will all be focused around the creation, transfer, and use of digital goods.

As a refresher, sub-question 3 is:

> *What are the benefits and drawbacks of hosting the metaverse on a blockchain compared to the current technology?*

The main benefits of using blockchain technology is in the security and additional features, such as NFTs. While other aspects are similar to that of cloud computing, the main drawbacks are in the scalability perspective. Cloud computing is currently much more scalable and has the capacity to host much larger projects with fluctuations on traffic, whereas blockchain is currently limited in this respect.

6 Proposed Regulations and Policies for the Metaverse

Now that a fair comparison has been made between blockchain and traditional technology in table 5.2, the possible policies and regulations that can be created for the technology can be discussed. This chapter will first briefly revisit the previously mentioned 9 aspects that are crucial to regulate in the metaverse. Once this is done, the interview data will be analyzed to see what aspects of blockchain should have policies and/or regulations first. For this, the perspective of both technical experts and policy experts will be taken into consideration in order not to get a one-sided view on the topic. Once these areas have been identified, the type of either a policy and regulation will be discussed that would be most suitable for these aspects, as well as the way to implement it into the technology itself.

6.1. Elements of The Metaverse

When it comes to regulating certain areas of the metaverse, it is important to ensure that all of the main aspects have been thought out in advance. For this reason, after the interviewees were asked what they thought was most important to regulate in the metaverse, a list was given that comprised of the most critical areas for regulation, which can be found in chapter 3.2.2. As a refresher, the subsequent aspects were: governance & legal documentation (GLD), liability (LB), IP, data privacy (DP), DAOs, smart contracts (SCs), KYC, virtual asset taxes (VAT) and regulations of conduct (RoC).

6.2. Interview Analysis

The analysis of the interviews will be done in two parts. First is the quantitative part, where the most critical areas will be uncovered with the help of the rankings of the interviewees. This will give a list of most important aspects to regulate with their respective scores to see which one ranks at the top and the following ranks. Once this has been done, the second part of the analysis will commence and will look at qualitative data gathered from the interviews to compile and assess the manners in which the interviewees mentioned they would resolve the issue. Since there has been a lot of input from this end from all interviewees, it can be taken into consideration and be used as a starting point for potential policies or regulations, together with potential drawbacks it could have.

6.2.1. Quantitative Analysis

The first part, which will be the quantitative analysis of the interview data, will determine the most important aspects that must need regulations and/or policies for the metaverse. This will be one of the nine factors mentioned in table 3.2.

The approach for this is to ask the interviewees to rank the top 3 most important factors in their opinion. This will yield a list of top 3 choices for every interviewee. Hereafter, each rank will be given a score and the total score of each of the factors will then be calculated by taking the sum of all interviewees for that particular aspect. Based on these final values, the aspect with the highest score will have top priority, followed by the second, third, etc. In order to do so, first a table will be constructed with the rankings of all the interviewees. Hereafter, a score for each of them will be assigned and a second table with the final scores will show the most to least important aspects to regulate and/or create policies on. The first table can be seen below on the left and the second table on the right.

Table 6.1: Rankings of top 3 most important factors to regulate according to each of the interviewees

Interviewee	#1	#2	#3	Expertise
1	4 (DP)	3 (IP)	7 (KYC)	Tech (BC)
2	3 (IP)	4 (DP)	8 (VAT)	Tech (BC)
3	1 (GLD)	4 (DP)	6 (SCs)	Tech (CC)
4	1 (GLD), 2 (LB), 5 (DOAs), 6 (SCs)	1* (GLD)	7 (KYC)	BC Policy
5	3 (IP)	4 (DP)	2 (LB), 9 (RoC)	BC Policy
6	7 (KYC)	5 (DAOs)	9 (RoC)	BC Policy (DAOs)

Table 6.2: able with final score for each one of the nine factors that could use regulation in order of descending scores (highest first).

Possible Regulation	Final Score
Data Privacy (4)	9
Intellectual Property (3)	8
Governance & Legal Documentation (1)	8
KYC (7)	5
DAOs (5)	5
Smart Contracts (6)	4
Liability (2)	4
Regulations of Conduct (9)	2
Virtual Asset Taxes (8)	1

Now that all the data has been gathered and ranked, values must be assigned to the first, second and third place of each of the interviewees. This will be done by giving points in descending order from first to third place. The first place will receive 3 points, 2 points for second place and 1 point for third. By doing so, a final list will be created with each one of the nine factors and their respective scores on how much the interviewees think that these areas should be regulated.

One interesting observation can be made from table 6.1, as the interviewees have been divided into 2 main categories: tech and policy. One can see that the interviewees that have their expertise on the technology side have similar answers; they rank data privacy and intellectual property relatively high. Although interviewee #5 ranks those high as well, the other 2 interviewees are more focused on other aspects, such as KYC, DAOs and RoC. Besides expressing what they find most important and urgent to regulate, it could also be a reflection of their knowledge in the field. For example, interviewee #3, who creates applications that run on cloud computers finds that it is important to have a metaverse that is reliable, stable, and that will not disappear over night. This could be a reflection of the experience this participant has with building long-term applications that others can rely on, no matter the circumstances. Similarly, interviewee #6 focused a lot on KYC on DAOs, which could again stem from the knowledge this participant has in this field. One thing to note with the rankings of interviewee #4 is that they combined 4 factors and put all of them in first place. This was done since the participant found it difficult to differentiate between the 4 and believes that they are all inter-connected with each other. Moreover, #4 created a new regulation and put that in second place, however, this regulation is closely related to GLD, which it has been replaced by.

From table 6.2, one can see that the top three factors are very close with one another, with data privacy at first with 9 points and a shared second position between IP, and governance & legal documentation with 8 points. This is followed by a gap of a few points and again a shared position between KYC and DAOs at 5 points. This essentially means that on average, the interviewees found data privacy, IP, and governance & legal documentation the most important factors to be considered when it comes to building a metaverse on a blockchain. This was to be expected when conducting the interviews, as many of them mentioned that building this on a public and open blockchain would also mean that the data of the users are public as well. Interviewee #2 mentioned how to solve this and showed that it is possible to encrypt this type of information with the help of L2 blockchains.

Essentially what this all means is that the quantitative data obtained by conducting the interviews could be more of a reflection of the knowledge of the participants, rather than what actually matters most. However, it is still important to take all perspectives into consideration and not leave certain elements out of potential future regulations. This is because almost all of the interviewees mentioned that all of the them apply to the metaverse and that they should all should be regulated in the future. Moreover, some of the regulatory aspects on the list are more difficult to implement than others and will thus take a longer time. For example, VAT, which only has 1 point, will be difficult to implement, as the jurisdiction in which a metaverse user will be taxed must first be determined. This aspect could be part of the KYC of the users themselves, which would put the KYC regulation before the VAT. Nevertheless, the focus will lie on the top 3 regulations, which will be discussed separately.

6.2.2. Qualitative Analysis

Besides the ranking that the interviewees were asked at the end of the interviews, there were meaningful discussions about the regulations in general prior to this. While individuals with different backgrounds were selected, there were some issues that seem to originate from all sides and, according to them, must be addressed first before implementing anything else.

First and foremost, many interviewees mentioned that the metaverse will essentially be borderless and that it will be difficult to create regulations and/or policies when there is no clear border between countries. Therefore, several participants proposed to have global regulations, where each country accepts general rules in order to include its citizens. The core reasoning for this according to the interviewees is because the underlying network that the metaverse will be built on is by nature already decentralized and in potentially many countries around the globe. It is therefore difficult to pinpoint exactly which country's rules the metaverse must adhere to. Interviewee #3 for example, mentioned that since blockchain technology does not fit the 'country model', some sort of global organization is needed to create regulations for the technology. This participant then continued with mentioning that it could be a similar entity to the United Nations (UN), in which case it would apply to all the countries within that body. While this solution would definitely solve some of the issues that come with putting regulations on blockchain, it will be difficult to create a brand new organizational body that represents this. It might thus be most beneficial for now to use some of the already existing organization that compass many of the worlds countries, like the UN that was mentioned. This would be a good starting point to create potential policies and/or regulations in. On the other hand, from the perspective of the users themselves, there is another challenge: figuring out the country where a user will be taxed. As interviewee #5 mentioned, it would be difficult to tax individuals with multiple nationalities that live in other countries. For example, someone with a dual nationality of a country within the EU and a country outside of the EU might be confused about which jurisdiction to follow for the metaverse. One might say that they should follow the tax laws of the country they live in. However, this could be a different country than the two nationalities. This detail has currently not been worked out and is important to look into before addressing other issues, such as taxation.

Secondly, many of the interviewees mentioned that the governance and legal documentation is very important when it comes to building a metaverse on a blockchain. What this entails is that the documentation for the code must be well written and the governance is somewhat 'bullet-proof'. Some interviewees mentioned similarities between future metaverse developers and current IT companies and emphasized on ensuring that the metaverse is offered as a reliable service. Moreover, it is important that users are protected to a certain degree and that developers or others cannot simply pull the plug one night and erase the digital assets of the users of this metaverse. This again ties with something that a specific interviewee mentioned, which is that while the technology itself should not be regulated, the users should have a protection of some sort against malicious actors.

Third, the interviewees that had more of a focus on the technical side of blockchains emphasized the need for a stable environment. This refers to making sure that the metaverse cannot be simply 'deleted' one day and erase a virtual world where potentially many people spend many days/weeks/months building various elements with a lot of value. Essentially, it is to ensure that the goods of the users in a virtual world cannot disappear over night. This would be crucial when building something that would potentially need to be active for many years, with minimum downtime.

Fourth, since the assumption is that it will be built on an open, public blockchain, the data of users would also be public. This would be a big issue as this information can contain a lot of private information that people might not want to share with others, such as their Date of Birth (DOB), address, email and height, just to mentioned a few. While it would not be too complicated to adjust this (according to interviewee #2), it is a crucial part that must be done before major adoption can take place in the project. The best manner in which this can be successfully implemented is to have it in that way from the beginning, which should be enforced by regulators of the space. Moreover, solving this must come before potential KYC checks, as that could contain sensitive information, such as passports and driver license numbers. This type of data must be securely encrypted in the place where it is stored and must be solved prior to KYC regulations.

Lastly, the IP right should be more clearly defined according to many of the interviews that were conducted. The specific aspects that should be addressed or the approach that should be taken when doing so was not discussed in detail. One of the interviewees mentioned that currently there is very large market for NFTs with buy and sell volumes at very high levels, it might be unclear as to who owns the IP rights after purchasing the NFTs. These details, along with the usage of the IP rights should be more clearly defined and perhaps expressed when purchasing the NFT. This would make the buyer also more aware of the rights he/she has when owning the NFT and what they can do with it. Additionally, with a new market arising where NFT owners can use their NFTs as collateral for a loan, it would also be important to address the rights of owners that take the NFTs as collateral.

All in all, while nine preliminary aspects were presented, 5 out of these nine are deemed as important according to the interviewees and was the largest part of the discussions, with only 3 being very important. These top 3 factors will be looked into with more detail in the next sub chapter.

6.3. Regulations versus Policies

While regulations are stricter and more limiting in nature that policies, it is important to distinguish between the two and which one would suit better for each factor. The three elements that will be focused on are the top three that were mentioned previously, which are: data privacy, IP and governance & legal documentation. This sub-chapter will go over each one of them, looking into whether policies or regulations should be made for them and how they would restrict the discussed aspect. This will all be done while keeping in mind some of the most crucial elements that were mentioned by the interviewees, such as limiting the technological developments and that it should be applicable to most jurisdictions, especially the EU.

When it comes to creating either policies or regulations, many of interviews always mentioned the term 'regulations' and not 'policies'. This could be due to a lack of knowledge between the differences of regulations and policies and simply use them interchangeably. That being said, it could still be possible to create policies for the relevant elements before creating more restrictive and asserting regulations. When it comes to three aspects that will be focused on: data privacy, IP and governance & legal documentation, the main and only type of policy that would directly apply is the regulatory policies. This is because for all of these elements, some sort of information or behaviour must be more limited and clearly defined then what is it now. However, while both regulations and policies are enforceable in court, regulations define expected behaviour and identifies the limitations of actions of users in certain scenarios. In contrast, policies are more for setting a process in order to achieve something in the end. In that sense, it is more suitable to create regulations on each one of the three aspects that would limit the users in their behaviour and ensure that they comply with the law.

6.4. Specific Regulations/Policies

Since it has been decided that mainly regulations will be implemented for each one of the three aspects, the exact details of the regulations must be discussed. When doing so, the perspective of all the interviewees will be taken into account, which is obtained from the discussions during the interviews. One common aspect between all the three elements would be that it must not limit the technology itself. This was mainly discussed with interviewee #4, who mentioned that any regulation will not and must not limit the underlying technology, only the usage of it. This was also what was kept in mind when they aided in creating the MiCA-bill, which does not limit the crypto currency technology, but rather the use and issuance of them in order to protect investors.

First there is the data privacy of the potential users of the metaverse. This data can contain anything from surface level data within the metaverse, such as the NFTs they own and how much of each token they have in the wallet that they use, to more personal data, such as name, DOB, address and potentially even social security number. While the latter information is much more sensitive, even the formerly mentioned information could be considered private in some cases. This was mentioned by interviewee #2, who said that people might not want to disclose their personal holdings to others, which could include friends & family, corporations and government. Many of the other interviewees had the same idea and do not want their information to be public. While this is understandable for the more sensitive pieces of information, it might not be realistic for disclosing the amount of tokens one holds or NFTs, as governments would likely want to tax that. However, the more sensitive information should be addressed by regulators and be one of the first regulations to be focused on. While taking that into account, since the data of the metaverse could be fully stored on a blockchain, retrieving that information for the specific users and other authorized personnel would be fairly easy. Moreover, as mentioned before, the regulation should not limit the underlying technology, as it could limit how much data a blockchain can store. This can for example be imposed by regulating the manner in which the data is uploaded to the blockchain. This would not limit the technology and would still protect users by having their data cryptographically encrypted. One of the first aspects to focus on for policy makers would therefore be to make this practice, or similar practices where the data would not be accessible and visible for everyone, a necessity. This can be observed by looking into the most popular metaverses and tracking the way data is uploaded to the blockchain. Regulators can double-check this by using the metaverse. This could increase the amount of information regarding how the blockchain is storing the personal data.

Secondly there is the IP right that one might have when playing or doing business in the metaverse and obtaining digital ownership in the form of NFTs. The IP rights become an important aspect when dealing with everything in the metaverse. The rights as an owner of these NFTs must therefore be clearly written out and stipulate what users can and cannot do. However, since NFTs can represent the digital ownership of different types of goods, e.g. art, collectibles, characters, cars, pets and houses, the regulations should address every single one of them to prevent confusion. This should also be done in form of a regulation rather than a policy and give clear guidelines to the users as to what behaviour is prohibited. Luckily, this behaviour can easily be tracked, as all transactions that happen with NFTs are stored on the blockchain and thus visible for the enforcers of the regulation. The underlying asset should also easily be found by going to the source code of the NFT and seeing what it represents. In order to make this process more efficient, regulators could also enforce the creators of the NFTs to mention in what category the NFT would fit. This would make the jobs of the regulators easier and also, once some rules have been established, users can find the type of NFT they have and look at the specific requirements for them. Moreover, by focusing only on the use of it, these regulation would again not limit the NFT and smart contract technology, and makes room for potential future improvements in the field.

Third and last there is the governance & legal documentation that projects in the metaverse should adhere to. As a quick reminder, this regulation would enforce developers to clearly outline their code and give detailed descriptions of the technology. This would essentially build on the white paper and give more documentation with the source code, which would for example be uploaded to a repository on GitHub and/or be published as a smart contract on the blockchain. Since this is more difficult to impose, as it is nearly impossible to regulate each and every single smart contract that is uploaded to a blockchain, it could be more beneficial to have this aspect overseen by a policy. Out of the four policies discussed earlier, the policy that would fit best is the 'regulatory policy'. The distinction between good and bad behaviour would be the difference between having insufficient documentation and having sufficient documentation. 'Sufficient' documentation in this sense is a grey area and developers might take advantage of it. Therefore, a clear guideline must be given that defines this, for example could be: 'Every (two) line(s) of code must be explained by at least one sentence.' In addition to this, the policy could also add that separate functions of code must have a short paragraph explaining it. This gives a clear guideline as to how much documentation is required, and eliminates some of the grey area that could potentially arise. Again, this policy would not limit any technology developments, but rather give a clear understanding of the new ones. It would also be beneficial to the developers themselves, as they can look back on older projects and easily understand what they were trying to accomplish with certain lines of code.

These three regulations were found to be the most important as of the first half of 2022. However, both the metaverse and blockchain technology are developing at a rapid pace, changing the landscape on a monthly basis. This means that the idea of the metaverse today, could differ from the idea in the future. Because of this, it makes creating regulations for a metaverse even more difficult, as policy makers chase the next innovation in the field. New areas might arise with the development of underlying technology that were previously non-existent. This varying landscape should be taken into account by policy makers, also ensuring that future established policies will need to be updated regularly to stay relevant. Additionally, chapter 5.4 mentions that some parts could be built on other technologies, such as cloud computers, to compensate for some of the weaknesses of the current state of blockchain technology. Depending on which parts will be run on the blockchain and which ones will run on cloud computers, some policies and regulation might not apply and would be unnecessary. However, as developments continue and both technologies start to mature, it could be a possibility that the metaverse will completely run on the blockchain.

6.5. Conclusion

To conclude, this chapter analyzed the interview data from both a quantitative and qualitative perspective. This could be done by either creating policies or regulations on the 9 criteria, with the different type of policies being: distributive, regulatory, constituent and redistributive. The list of the criteria was given to interviewees, who were asked to mention whether they think the potential regulations apply or not, and also rank the top 3 most important factors according to them. While most interviewees mentioned that all of them apply, the top 3 rankings varied from one to another. One interesting find was that most of the interviewees with similar backgrounds ranked similar aspects in their top 3. The final top 3 was: data privacy, IP, and governance & legal documentation. Therefore, regulators should focus on all these three elements of blockchain technology. However, this top 3 could also be a representation of the knowledge of the interviewees, which should be taken into account. It must be understood that all of the 9 aspects are crucial to be regulated, as mentioned by the participants. Nevertheless, none of the regulations and policies should limit the technology in such a way that it hinders or blocks development or new innovations to arise in the field.

That being said, the top 3 factors were looked into with more detail in order to figure out the potential solutions for the regulations.

The first aspect that should be regulated is the data privacy through encrypting the data of the users before uploading the information to the blockchain. Since the discussed blockchains are public, permissionless blockchains, the data on the blockchain is available for everyone to see. This would mean that sensitive data of users would also be public, which goes against some of the data privacy acts in the EU. Encrypting the data can be done with the use of L2 blockchains, which would also add more scalability to the L1 blockchain, thus also improving some of the drawbacks of using blockchain technology for the metaverse. The second aspect was that of IP rights, which should also be regulated and have clear direction with what one can and cannot do with certain NFTs. This will ensure that users do not infringe the IP rights of the existing NFTs. The third and final element was that of governance & legal documentation, which is best tackled by implementing policies on them. The policies will serve as guidelines for a minimum number of explanatory sentences there must be for the lines of code written. Developers will likely end up spending more time writing the same code after the implementation of the hypothetical policy. However, it would improve understanding of the code with other developers, as well as making it easier to understand one's code in the future.

To reiterate the last sub-question:

Considering future development of a blockchain based metaverse, what should policy makers do in order to regulate the space while not limiting its development?

The policy makers should be informed that all of the 9 aspects are critical and must, sooner or later, all be regulated. However, the interview data showed that there are three aspects which were deemed to be the most important factors: data privacy, IP rights, and governance & legal documentation. These should therefore be looked into first and regulations must be created without limiting the underlying technology, which would be: blockchain infrastructure, NFTs, and the source code. The ideas that arose from the limited number of interviews conducted has already yielded multiple solutions to potential regulations. Policy makers should therefore continue doing market research and discuss regulations with key stakeholders, which would give feedback on potential solutions. The solutions presented in this chapter can be taken as a starting point for the policy makers, which can be refined in the future.

7 Conclusion

The last chapter will sum up the core findings, as well as answering the main research question and sub-questions that were formulated in the beginning of the thesis. After drawing conclusions from the thesis and answering each one of the research questions, limitations and future research of the topic will be discussed in relation to the Engineering and Policy Analysis (EPA) master program.

7.1. Conclusion

Before going into answering each one of the research questions, they will be repeated here as a memory refresher and will be easily accessible, in case of confusion. The sub-questions are formulated in a way that they build up to answering the main research question.

7.1.1. Sub-Question 1

The first sub-question is formulated as follows: *What are the current policies and regulations in the EU that are associated with blockchain and the metaverse?* Essentially, this only looks at the current regulations that exist in the EU on blockchain and the metaverse, and was researched through a literature review. This literature review found that there are currently only 2 regulatory frameworks in the EU when it comes to blockchain technology: MICA and DORA. From these two, MICA looks into crypto-assets and its aim is to minimize the risks that investors are exposed to, whereas DORA looks into digital resilience processes and standards. There were some additional regulations, such as the general data protection regulation, markets in financial instrument directive II, and the electronic money directive that one might think apply in this scenario, but they do not. It was also found that a metaverse built on a blockchain specifically does not have any official regulations on the EU level as of July 2022. Thus, answering the research question directly: for blockchain the only two regulations in the EU are MICA and DORA, and the metaverse does not have any official regulatory frameworks in the EU.

7.1.2. Sub-Question 2

After looking into the regulation, the first step was to look at how cloud computing fits in the metaverse. The sub question that was formulated for this purpose was: *What are the main technical challenges currently faced by the current technology (i.e. cloud computing)?* Since most of the applications run on cloud computers, it is crucial to investigate this technology and see how it holds up when hosting a metaverse. The 7 criteria that were looked into were: energy usage, security, scalability, governance, democratization, costs and additional features. After having looked into all of them, it was found that the main challenges of cloud computing systems are the security issues, which involve misconfiguration and cyberattacks, as well as the lack of additional features that benefit cloud computing specifically for a potential metaverse. These two issues are the main technical challenges that cloud computing faces for building a metaverse.

7.1.3. Sub-Question 3

Now that cloud computing has been looked into, the other technology of blockchain, must also be studied on the same 7 criteria in order to make an accurate comparison. More specifically, the sub-question is: *What are the benefits and drawbacks of hosting the metaverse on a blockchain compared to the current technology?* Since it is nearly impossible to compare the blockchain space as a whole with cloud computing, in some cases a specific blockchain was chosen. The chosen blockchain must meet the following criteria: public, permissionless and be able to compute. While there are a few blockchains that fit these criteria, perhaps the best suited one is ICP. After having looked into each one of the criterion in detail w.r.t. this blockchain, a comparison table was made (table 5.2). Essentially, cloud computing is more superior when it comes to scalability and costs, whereas blockchain has the upper hand in security, governance, democratization and additional features. While energy usage in cloud computing systems is very low, blockchains are becoming increasingly efficient as well and can perform multiple tasks. On top of this, the ICP blockchain has standardized hardware equipment that each node must adhere to and is soon releasing their second generation specifications. Overall, there are benefits and drawbacks for using either technology. Developers could look into this further and build the metaverse in such a way that the benefits of both technologies are being utilized. This would give the metaverse NFT capabilities and be easily scalable.

7.1.4. Sub-Question 4

The last sub-question stated: *Considering future development of a blockchain based metaverse, what should policy makers do in order to regulate the space while not limiting its development?* The aim with this question was to tie the technical background back to the policies and regulations. Interviews were conducted with experts of different backgrounds to get a clear picture of the most important factors. The backgrounds of these experts ranged from blockchain protocol engineers, cloud computing product developers, and policy advisors/strategists. The specific factors that the experts were asked to rank were governance & legal documentation, liability, intellectual property, data privacy, DAOs, smart contracts, know your customer, virtual asset tax, and regulation of conduct. The final result of all the interviews yielded the following top 3: data privacy (9 points), IP (8 point), and governance & legal documentation (8 points). All of these aspects only apply if the metaverse were to be built fully on a blockchain. Thus, if some parts of the metaverse are built on other technologies, such as cloud computers, some regulations might not apply. While taking this into account, policy makers should

7.1.5. Main Research Question

The last sub-question already partly answers the final research question: *What are the main technological factors that must be taken into consideration for policy makers in the EU to create new regulations and policies for a decentralized metaverse?* The interviews provided good insight into potential solutions for each of the 9 factors mentioned above. As for the quantitative data obtained from the interviewees, the main technological factors should be the data privacy of the users, the intellectual property rights of NFT holders, and the governance & legal documentation of metaverses and other applications. A general direction for finding solutions for each one of them is proposed in chapter 6.4. Besides these three, it is crucial that the other aspects of potential regulations are not ignored and are also being worked on. Additionally, research must be conducted on the best possible procedure to tackle each one of these factors, and whether some should have priority over others. When analyzing the field and taking different stakeholders into consideration, the EU should keep in mind that there can be a big knowledge gap between policy advisors and blockchain developers.

For *data privacy*, one of the prime solutions that came up was that the data of the users can be combined, cryptographically encrypted by a L2 blockchain, and only then uploaded to the L1 blockchain. Policy makers should work with developers to create a regulatory framework that uses this or similar solutions that would secure the data of the users. The second factor: *IP*, must clearly be defined as to what is and what is not allowed to do when owning certain NFTs. The NFTs can, for example, be categorized into art, characters, cars, and real estate. The creator of the NFT would have to mention the type, along with the NFT, which would make it easier to understand for both regulators and users. For the last factor, *governance & legal documentation*, it would best to fit a policy with guidelines that mention how much documentation is required for the lines of code written. There could be additional measures, such as documentation for each function within the code and for each one of the files in the repositories.

All in all, these three aspects are the main factors that policy makers should take into consideration from different experts. One notable aspect from each one of them is they do not limit the technology. It leaves developers with all the freedom to improve and develop new projects, although it might take some extra time to do so by adding these additional requirements.

7.2. Limitations & Future Research

While this thesis went into significant detail on both blockchain and cloud computing when it comes to building a metaverse, there are still some limitations. These limitation lie in both the analysis of the two technologies, the creation of policies themselves and having a single author for such a big project. After elaborating on the limitations, a suggestion is given for future research.

Perhaps the first limitation would be the comparison between blockchain and cloud computing. Even though the comparison was made as detailed as possible, there is only a limited amount of information available on the internet. Future research could be to create a small digital world that would be able to run on both a cloud computing system and on the ICP network, in order to make comparisons. This would yield better results especially when it comes to the energy usage, scalability, democratization, and costs of each technology. The similarities and differences between the two technologies could have been in more detail as this could uncover more information about the two technologies, and showcase the strengths and weaknesses of both in more depth. Additionally, an employee or employer at both a big cloud computing company (such as AWS) or blockchain organization (such as ICP) could have been consulted while building a digital environment such as this, in order to gain greater insight into the two technologies.

The second limitation could be the depth of the interviews that were conducted. While conducting the interviews, there was a clear pattern that the policy interviewees were very elaborate on their answers and gave a lot of insight to the field. On the other hand, the more technical participants kept it to the point. Therefore, some information, especially from the technical side, might not have been shared to the fullest extent that it could have been. Additional follow-up questions for the technical interviewees would allow for more elaborate answers. Nevertheless, while the technical interviewees were more to the point and gave shorter answers, they did answer the question as intended and give solutions to some of the issues that were mentioned. The follow-up questions would help uncover more information and strengthen the arguments by, for example, asking about potential weaknesses in the given solutions. Future research can focus specifically on the 9 potential regulations and conduct significantly more interviews for them.

The third limitation is the lack of previous scientific research in the field. Most of the previous articles that were written merely mentioned that the space should be regulated, but not mention what type of regulations, which aspects, or to what extent. Therefore, the starting point was a blank sheet of paper to try and find the most critical areas to regulate, how to regulate them and what potential technical solution there could be to these regulations. While all of these have been found and discussed in the paper, there could potentially be better solutions and/or more critical aspects that were overlooked because of the lack of information within this space. While this limitation is difficult to overcome, this thesis can form as a base for future research, to the previously mentioned digital world. This world could also be used to enhance the analysis by running simulations. This simulation would be focused towards implementing certain regulations and policies mentioned in the thesis, with simulated users that all have certain characteristics. Once a best possible scenario is found using different policies and regulations, a trial could be done in a real metaverse, such as Decentraland. As a response, the regulations can be adjusted, as well as the model itself to predict the behaviour of the users better. All of this will aid in creating the first few regulations in the space and fine tune them to find the best solutions, while retaining most of the users, as there might be some backlash in the beginning.

The final limitation is the lack of peer-reviews conducted during the process of the thesis, which can result in biased arguments. Meetings with supervisors were held regularly (1 to 2 times per month) who gave feedback on the thesis and points of improvement. Additionally, academic colleagues were consulted during the process to perhaps gain more insight or discuss aspects that would otherwise have been overlooked. However, it is impossible to completely remove bias from the equation without several detailed analyses from peers and professors.

7.3. Implications

The implications of this research can be divided into two: scientific and policy. Here, both of these will be discussed in order to better understand the implications from both perspectives.

7.3.1. Scientific Implications

From a scientific standpoint, this research is one of the first that looked into what type of regulations and policies a metaverse built on a blockchain needs. This was done by discussing previous research and then consulting with experts in various fields to get their opinion on the matter. The collective opinion of these experts then yielded new information that can be used for scientific paper in the future. To be more specific, the final results obtained from the interviews that state which aspects regulators should focus on is one of the first of its kind, as other scientific articles and regulatory bodies merely mention that it should be regulated or have recently started investigation on the digital space. This new information can be used to be built upon into several direction. Besides conducting similar research in order to validate the results, new research can look into the implementation of these regulations and how they can be enforced.

7.3.2. Policy Implications

As for the policy implications, there are three core regulations and policies discussed for future regulations. These three affect the users, but most importantly, the developers of the space. Developers must therefore start to follow these regulations more closely in order to ensure that they are complying with them. This will likely be difficult to begin with, as there are currently no regulations regarding either blockchain or metaverse development. The users will have it easier, as most of the regulations are focused around the development of the space and only the IP rights regulation targets the users to a certain extent.

The data privacy aspect of the new regulations will not affect the users as much as developers. The developers must take the new regulations into account when creating a metaverse and storing the data of their users of it. There will likely be extra work from the developers' side in order to comply with this, as they must ensure that the data of the users is not public. The same can be said for the governance & legal documentation policy. This policy only affects the developers of the space, as they must ensure that their code is well documented for others to understand. Lastly, the IP rights regulations would impact both users and developers. While developers have to make sure that their NFTs are categorized properly, users will now be restricted in certain areas with what they can do with their NFTs. Moreover, new creators should ensure that what they are creating does not infringe the IP rights of other creators.

7.4. Relevance

As with any research, it must be relevant for it hold value from both a societal and academic perspective. Here, the two will be discussed as well as points of interest for the EU.

7.4.1. Societal Relevance

As for the societal perspective, the main focus of the thesis has been to provide the EU with new perspectives. From this perspective, the thesis provides guidance as to which direction to EU should focus their efforts towards. Prior to this research, there were many articles citing that blockchain and the metaverse must be regulated. However, there is little to no research on which aspects should exactly be regulated and how to go about it. This research can be taken as a starting point for the EU, with perspectives of different fields, giving advice on what to regulate as well as possible solutions for some of the mentioned issues.

Besides regulators, this paper also gives users and developers of the metaverse a clear indication of the current state, along with potential future policies and regulations in the space. This way, they can slowly start to prepare for such regulations and ensure that their activities are within the proposed frameworks.

7.4.2. Academic Relevance

As mentioned above, little to no research was conducted on which aspects of blockchain and metaverse to regulate. Academic relevance is not only for TU Delft and the EPA program, but also for other research institutes, as well as the governmental bodies that do research on the topic.

First of all, it is one of a limited number of studies that have explored possible regulations for a metaverse that is built on a blockchain. Moreover, the MiCA-bill officially ended the provisional agreement on June 30th 2022, while the initial proposal came almost 2 years prior to that. Taking this timeline as a potential outline for regulations, it could take several more years to come up with the initial proposal. This is because interviewee #5 mentioned that the EC and EU recently saw advancements in the metaverse and have started to explore possibilities of regulating it. With help of this study, regulators can seek to find a better understanding of the field and use this study as a starting point and guide.

7.5. EPA Relevance

Engineering and Policy Analysis is all about grand challenges that go on in the world. Grand challenges are, by nature, impossible to solve and are very complex with a lot of moving parts. I believe that this is also the case in the study that was conducted in this thesis. First of all, blockchain is a landscape with new developments being implemented on a daily basis. Moreover, every few weeks a brand new blockchain comes out that does something like no other. Although these drastic changes might not occur in a decade from now, they are currently difficult to deal with. This ever changing environment makes it inherently difficult to impose regulation on, as blockchain developers could potentially find loopholes in regulation and create a blockchain around it. Keeping all of this in mind, regulating a digital world, with valuable goods in them becomes even more difficult. The fact that this world in built on the blockchain makes the space even more difficult to regulate and will be a project that will be in progress for a very long time and could potentially never be fully regulated. For this reason, I believe that the problem presented in the beginning of this thesis is defined as a grand challenge, which is what EPA is all about.

References

Aberg, S. E., Khoury, G., & Golda, Z. (2022, April). *March 2022 crypto enforcement actions roundup.* Retrieved from https://www.natlawreview.com/article/march-2022-crypto-enforcement-actions-roundup

Aggarwal, S., & Kumar, N. (2021). Cryptographic consensus mechanisms. In *Advances in computers* (Vol. 121, pp. 211–226). Elsevier.

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From web 1.0 to web 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1–10.

Ahmed, H. S. A. (2021, February). *Building cloud governance from the basics.* ISACA. Retrieved from https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-3/building-cloud-governance-from-the-basics

Alexandrov, I. (2020, October). *Key takeaways from the european commission's proposal ... - kambourov.biz.* Retrieved from https://www.kambourov.biz/en/publications/key-takeaways-from-the-european-commissions-proposal-for-a-regulation-on-markets-in-crypto-assets

Amazon. (2022, April). *Aws customer success stories.* Amazon Web Services. Retrieved from https://aws.amazon.com/solutions/case-studies/?customer-references-cards.sort-by=item.additionalFields.sortDate&customer-references-cards.sort-order=desc&awsf.content-type=*all&awsf.customer-references-location=*all&awsf.customer-references-segment=*all&awsf.customer-references-industry=*all&awsf.customer-references-use-case=*all&awsf.customer-references-tech-category=*all&awsf.customer-references-product=*all

Ara, T. K., Radcliffe, M. F., Fluhr, M., & Imp, K. (2022, June). *Exploring the metaverse: What laws will apply?* DLA Piper. Retrieved from https://www.dlapiper.com/en/us/insights/publications/2022/06/exploring-the-metaverse-ipt-news-june-2022/

AssangeDAO. (2022). *Assangedao.* Retrieved from https://assangedao.org/

Association, D., & ICA. (2022, May). *Computation and storage costs.* Retrieved from https://smartcontracts.org/docs/current/developer-docs/updates/computation-and-storage-costs/

Association, I. C. (2022, May). *Ica network status.* Retrieved from https://dashboard.internetcomputer.org/#!

Austin, S. (2021, September). *The new wave of web 3.0 metaverse innovations.* Entrepreneur. Retrieved from https://www.entrepreneur.com/article/380250

Azure, M. (2022, May). *Pricing - windows virtual machines: Microsoft azure.* Microsoft. Retrieved from https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/#pricing

Baciu, I. E. (2015). Advantages and disadvantages of cloud computing services, from the employee's point of view. *National Strategies Observer No*, *2*.

Bada, A. O., Damianou, A., Angelopoulos, C. M., & Katos, V. (2021). Towards a green blockchain: A review of consensus mechanisms and their energy consumption. In *2021 17th international conference on distributed computing in sensor systems (dcoss)* (pp. 503–511).

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *9*(10), 533–546.

Bank, E. C. (2022, march). *Our work aims to ensure that in the digital age citizens and firms continue to have access to the safest form of money, central bank money.* Retrieved from `https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html`

Barnebys. (2022, Feb). *The 10 most expensive living artists: Barnebys magazine.* Author. Retrieved from `https://www.barnebys.co.uk/blog/the-most-expensive-living-artists`

Bayse, C. (2021, September). *The metaverse is coming — society should be wary.* Retrieved from `https://thehill.com/opinion/technology/580437-the-metaverse-is-coming-society-should-be-wary`

Ben-David, J. (2021, March). *Cloud elasticity vs cloud scalability.* Retrieved from `https://blog.turbonomic.com/blog/on-technology/cloud-elasticity-vs-cloud-scalability`

Berners-Lee, T. (1998). *The world wide web: A very short personal history.* Retrieved from `http://www.w3.org/People/Berners-Lee/ShortHistory.html`

Bobrowsky, M., & Needleman, S. E. (2021, November). *What is the metaverse? the future vision for the internet.* Wallstreet Journal. Retrieved from `https://www.wsj.com/story/what-is-the-metaverse-the-future-vision-for-the-internet-ca97bd98`

Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K., & Hong, W.-C. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*, *8*, 54371–54401.

Bonifacic, I. (2021, November 11). *Nike is building its metaverse inside of 'roblox'.* Engadget. Retrieved from `https://www.engadget.com/nike-roblox-nikeland-metaverse-192234036.html`

Bor, S. (2021, April). *Governance program #1635.* GitHub. Retrieved from `https://github.com/solana-labs/solana-program-library/pull/1635`

Bosworth, A., & Clegg, N. (2021, September). *Building the metaverse responsibly.* Meta. Retrieved from `https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/`

Bourlakis, M., Papagiannidis, S., & Li, F. (2009). Retail spatial evolution: paving the way from traditional to metaverse retailing. *Electronic Commerce Research*, *9*(1), 135–148.

Brett, C. (2018, October). *Blockchain disadvantages: 10 possible reasons not to enthuse.* Retrieved from `https://www.enterprisetimes.co.uk/2018/10/15/blockchain-disadvantages-10-possible-reasons-not-to-enthuse/`

Brooke, C. (2022, Jun). *Best dao crypto projects - what is a dao ?* Retrieved from `https://www.business2community.com/cryptocurrency/best-crypto-dao-projects`

Brown, A. (2021, December). *Facebook expects metaverse project will cost at least $10 billion-in 2021 alone.* Forbes Magazine. Retrieved from `https://www.forbes.com/sites/abrambrown/2021/10/25/facebook-expects-metaverse-project-will-cost-at-least-10-billion-in-2021-alone/?sh=b13f06a25b43`

BTSE. (2021, August 12). *Blockchain dilemma (part 1 of 3): The impossible triangle.* Author. Retrieved from `https://blog.btse.com/blockchain-dilemma-part-1-of-3-the-impossible-triangle/`

Buenconsejo, U. (2022, February). *Study shows it costs $20k to store 500kb on the ethereum blockchain; could nfts be at the risk of link hijacking to alter ownership.* Tech Times. Retrieved from `https://www.techtimes.com/articles/271313/20220202/study-shows-costs-20k-store-500kb-ethereum-blockchain-nfts-risk.htm`

Burgess, K., & Colangelo, J. (2015). *The promise of bitcoin and the blockchain.* Consumers'Research.

Buterin, V. (2013a, September 19). *Bootstrapping a decentralized autonomous corporation: Part i.* Bitcoin Magazine. Retrieved from https://bitcoinmagazine.com/technical/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274

Buterin, V. (2013b). *Ethereum whitepaper.* Ethereum.org. Retrieved from https://ethereum.org/en/whitepaper/

Buterin, V. (2022). *Ethereum charts & statistics.* Retrieved from https://etherscan.io/charts

Caleb, & Brown. (2022, January). *The metaverse part 3: Centralised and decentralised metaverse.* Retrieved from https://www.calebandbrown.com/blog/the-metaverse-part-3-centralised-and-decentralised-metaverse

Canavesi, B. (2022, March). *The foundation of the metaverse.* Retrieved from https://www.td.org/atd-blog/the-foundation-of-the-metaverse-centralization-versus-decentralization

Canellis, D. (2019, September 23). *More than 60% of ethereum nodes run in the cloud, mostly on amazon web services.* Retrieved from https://thenextweb.com/news/ethereum-nodes-cloud-services-amazon-web-services-blockchain-hosted-decentralization

Canorea, E. (2021, November 16). *What companies use metaverses for and why the big tech companies are so interested.* Plain Concepts. Retrieved from https://www.plainconcepts.com/metaverse-companies/

Castrovilli, M. (2022, Feb). *$53 million raised for assange showed the power of daos.* Cointelegraph. Retrieved from https://cointelegraph.com/news/53-million-raised-for-assange-showed-the-power-of-daos

Chai, W., & Bigelow, S. J. (2021, December). *Cloud computing.* Tech Target. Retrieved from https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing

Chan, R. (2019, October). *The cambridge analytica whistleblower explains how the firm used facebook data to sway elections.* Retrieved from https://www.businessinsider.nl/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10?international=true&r=US

Chima, R. (2016, September). *Cloud security – who owns the data?* Blueberry Consultants. Retrieved from https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data

Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. *Available at SSRN 3082055*.

Choudhury, N. (2014). World wide web and its journey from web 1.0 to web 4.0. *International Journal of Computer Science and Information Technologies*, *5*(6), 8096–8100.

Claeys, B. (2022, May). *Ranking cryptocurrencies based on github commits - 3 months.* Retrieved from https://www.cryptomiso.com/months_3.html

Clifford, L., & Mathews, J. (2022, February). *Opensea illustrates the perils of growing too fast.* Fortune. Retrieved from https://fortune.com/2022/02/11/opensea-nft-growth-customer-deman-obstacle/#:~:text=She%20reports%20that%20in%20January,2021%2C%20according%20to%20Dune%20Analytics.

Cohen, J. (2021, December). *4 companies control 67% of the world's cloud infrastructure.* PCMag. Retrieved from https://www.pcmag.com/news/four-companies-control-67-of-the-worlds-cloud-infrastructure

CoinMarketCap. (2022). *Top dao tokens by market capitalization.* Retrieved from https://coinmarketcap.com/view/dao/

Cointelegraph. (2017, October 15). *The history and evolution of proof-of-stake.* Author. Retrieved from https://cointelegraph.com/news/the-history-and-evolution-of-proof-of-stake

Commission, E. (2018). *Data protection in the eu.* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Commission, E. (2020a, September). *Lex - 52020pc0593 - en - eur-lex.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Commission, E. (2020b, September). *Lex - 52020pc0595 - en - eur-lex.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

Commission, E. (2021, January 19). *Joint statement by the european commission and the european central bank on their cooperation on a digital euro.* European Commission and European Central Bank. Retrieved from https://ec.europa.eu/info/files/210119-ec-ecb-joint-statement-digital-euro_en

Commission, E. (2022a, February 23). *Legal and regulatory framework for blockchain.* Author. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain

Commission, E. (2022b, February). *Regulatory framework for blockchain.* Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain

Conor. (2021, September). *What's next for blockchain? 3rd generation platforms.* web3labs. Retrieved from https://medium.com/web3labs/whats-next-for-blockchain-3rd-generation-platforms-a26f34da4d59

Conwell, S. (2021, November). *Smart contracts start transferring icp after upgrade, allowing advanced defi to be developed on the internet computer.* Retrieved from https://finance.yahoo.com/news/smart-contracts-start-transferring-icp-201300152.html#:~:text=Due%20to%20Chain%20Key%20cryptography,%2C%20a%20super%2Dadvanced%20DAO.

Cook, A., Bechtel, M., Anderson, S., Novak, D., Nodi, N., & Parekh, J. (2020). The spatial web and web 3.0: What business leaders should know about the next era of computing. *Deloitte Insights, What business leaders should know about Web*, *3*.

Cuen, L. (2021, March). *The debate about cryptocurrency and energy consumption.* TechCrunch. Retrieved from https://techcrunch.com/2021/03/21/the-debate-about-cryptocurrency-and-energy-consumption/

Darby, I. (2022, February). *Marketing, the metaverse & future of privacy – with the cambridge analytica whistleblower.* The Drum. Retrieved from https://www.thedrum.com/news/2022/02/17/marketing-the-metaverse-future-privacy-with-the-cambridge-analytica-whistleblower

Dawson, O. (2012, August). *Difference between policy and regulation.* Retrieved from https://www.differencebetween.com/difference-between-policy-and-vs-regulation/

Decentraland. (2022). *Decentraland dao.* Retrieved from https://dao.decentraland.org/en/

Deer, M. (2022, May). *Will the ethereum 2.0 update reduce high gas fees?* Cointelegraph. Retrieved from https://cointelegraph.com/explained/will-the-ethereum-20-update-reduce-high-gas-fees

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208.

Dfinity. (2021, May 17). *Chain key cryptography: The scientific breakthrough behind the internet computer.* Medium. Retrieved from https://medium.com/dfinity/chain-key-technology-one-public-key-for-the-internet-computer-6a3644901e28

Dignan, L. (2021, December). *Top cloud providers: Aws, microsoft azure, and google cloud, hybrid, saas players.* ZDNet. Retrieved from https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/

Dilger, W. (1997). Decentralized autonomous organization of the intelligent home according to the principle of the immune system. In *1997 ieee international conference on systems, man, and cybernetics. computational cybernetics and simulation* (Vol. 1, pp. 351–356).

Dionisio, J. D. N., III, W. G. B., & Gilbert, R. (2013, July). 3d virtual worlds and the metaverse: Current status and future possibilities. *ACM Comput. Surv.*, *45*(3). Retrieved from https://doi.org/10.1145/2480741.2480751 doi: 10.1145/2480741.2480751

Du, H., Niyato, D., Kang, J., Kim, D. I., & Miao, C. (2021). Optimal targeted advertising strategy for secure wireless edge metaverse. *arXiv preprint arXiv:2111.00511*.

Dzyuba, A., & Rohi, A. (2021, August). *7 challenges of the metaverse.* Retrieved from https://lucidrealitylabs.com/blog/7-challenges-of-the-metaverse

EBA. (2019, January). *Report with advice for the european commission.* Retrieved from https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. *Procedia computer science*, *123*, 116–121.

El Faqir, Y., Arroyo, J., & Hassan, S. (2020). An overview of decentralized autonomous organizations on the blockchain. In *Proceedings of the 16th international symposium on open collaboration.* New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3412569.3412579 doi: 10.1145/3412569.3412579

Emergen. (2021, November). *Metaverse market, by component (hardware, software), by platform (desktop, mobile), by offerings (virtual platforms, asset marketplaces, and others) by technology (blockchain, vr & ar, mixed reality), by application, by end-use, and by region forecast to 2028.* Retrieved from https://www.emergenresearch.com/industry-report/metaverse-market

Eric. (2021, 17). *How much does it cost to deploy a smart contract on ethereum?* Medium. Retrieved from https://medium.com/the-capital/how-much-does-it-cost-to-deploy-a-smart-contract-on-ethereum-11bcd64da1

ESMA. (2018, January). *Mifid ii.* Retrieved from https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

Ethereum. (2022). *Erc-721 non-fungible token standard.* Retrieved from https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

EUR-Lex. (2009, October). *Lex - 32009l0110 - en - eur-lex.* Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32009L0110

Evans, T. M. (2019). Cryptokitties, cryptography, and copyright. *AIPLA QJ*, *47*, 219.

Fairfield, J. (2021). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal, Forthcoming*.

Fairfield, J. A. (2021). *Runaway technology: Can law keep up?* Cambridge University Press.

Fawns, T., Jones, D., & Aitken, G. (2020). Challenging assumptions about "moving online" in response to covid-19, and some practical advice. *MedEdPublish*, *9*.

FCA. (2018, April). *Cryptocurrency derivatives.* Retrieved from https://www.fca.org.uk/news/statements/cryptocurrency-derivatives

Filippi, P. D., & Wright, A. (2019, Oct). *The rule of code vs. the rule of law.* Harvard University Press. Retrieved from https://hup.medium.com/the-rule-of-code-vs-the-rule-of-law-8dfe75631fee

Franck, T. (2022, May). *Sec nearly doubles crypto unit staff to crack down on abuses in the booming market.* CNBC. Retrieved from https://www.cnbc.com/2022/05/03/sec-adds-to-cryptocurrency-regulation-staff.html

Friedman, J. (2022, April). *Crypto in the age of climate change.* Dfinity Community ∞. Retrieved from https://www.dfinitycommunity.com/crypto-in-the-age-of-climate-change/

Gao, Y., & Nobuhara, H. (2017). A proof of stake sharding protocol for scalable blockchains. *Proceedings of the Asia-Pacific Advanced Network*, *44*, 13–16.

Gaskin, S. (2021, May). *Why kevin mccoy is auctioning off the first nft ever minted.* Ocula. Retrieved from https://ocula.com/magazine/art-news/why-kevin-mccoy-is-auctioning-the-first-nft/

GDPR. (2022). *Gdpr summary.* Retrieved from https://www.gdprsummary.com/gdpr-summary/

Geroni, D. (2021, November). *The role of blockchain in web 3.0.* Retrieved from https://101blockchains.com/blockchain-in-web-3-0/

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 acm sigsac conference on computer and communications security* (pp. 3–16).

Gill, N. S. (2022, May). *Cloud governance challenges and best practices.* XenonStack. Retrieved from https://www.xenonstack.com/blog/cloud-governance

Gillar, M. (2020, January). *Who's using amazon web services? [2020 update].* Contino. Retrieved from https://www.contino.io/insights/whos-using-aws

Government, Q. (2017, July). *Benefits of cloud computing.* Retrieved from https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits

Graah, H. (2022, Feb). *The evolution of daos and why they are expected to take hold in 2022.* Cointelegraph. Retrieved from https://cointelegraph.com/news/the-evolution-of-daos-and-why-they-are-expected-to-take-hold-in-2022

Gu, M. (2022, July). *Ethereum 2.0 is coming – here's what you need to know.* Boxmining. Retrieved from https://boxmining.com/ethereum-2/

Guide, I. (2021, July). *Costs on the internet computer.* Retrieved from https://icp.guide/costs-on-the-internet-computer/

Haar, R. (2021, November 30). *The 10 most popular cryptocurrencies, and what you should know about each before you invest.* Next Advisor. Retrieved from https://time.com/nextadvisor/investing/cryptocurrency/types-of-cryptocurrency/

Hackl, C. (2020, July). *The metaverse is coming and it's a very big deal.* Retrieved from https://www.forbes.com/sites/cathyhackl/2020/07/05/the-metaverse-is-coming--its-a-very-big-deal/?sh=7106fadc440f

Han, Y., Niyato, D., Leung, C., Miao, C., & Kim, D. I. (2021). A dynamic resource allocation framework for synchronizing metaverse with iot service and data. *arXiv preprint arXiv:2111.00431*.

Harford, S. (2021, November). *Microsoft goes to the metaverse, bringing immersive meetings to teams.* Retrieved from https://www.siliconrepublic.com/business/microsoft-metaverse-mesh-for-teams

Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, *10*(2), 1–10.

Heiligenstein, M. (2022). *Amazon web services (aws) data breaches: Full timeline through 2022.* Retrieved from https://firewalltimes.com/amazon-web-services-data-breach-timeline/

Hern, A. (2018, May). *Cambridge analytica: How did it turn clicks into votes?* Guardian News and Media. Retrieved from https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Hines, H. (2021, March). *To dfinity and beyond: Static front-end hosting, internet computer gateway, and the next steps.* fleek.co. Retrieved from https://blog.fleek.co/posts/to-dfinity-and-beyond-dfinity-frontend-hosting

Holmes, F. (2021, December). *The metaverse is a $1 trillion revenue opportunity. here's how to invest...* Forbes. Retrieved from https://www.forbes.com/sites/greatspeculations/2021/12/20/the-metaverse-is-a-1-trillion-revenue-opportunity-heres-how-to-invest/?sh=298364014df9

Hui, M. (2021, November). *China is eyeing the metaverse as the next internet battleground.* Quartz. Retrieved from https://qz.com/2089316/china-sees-the-metaverse-as-the-next-internet-battleground/

IBM. (2022, May). *Benefits of blockchain - ibm blockchain.* IBM Blockchain. Retrieved from https://www.ibm.com/topics/benefits-of-blockchain

ICP. (2022). *Nft minting.* Retrieved from https://internetcomputer.org/docs/current/samples/nft

IMF. (2021, August). *Special drawing rights (sdr).* International Monetary Fund. Retrieved from https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SD

Jena, S. (2020, December). *Difference between cloud computing and distributed computing.* GeeksforGeeks. Retrieved from https://www.geeksforgeeks.org/difference-between-cloud-computing-and-distributed-computing/?ref=gcse

Jeon, H.-j., Youn, H.-c., Ko, S.-m., & Kim, T.-h. (2022). Blockchain and ai meet in the metaverse. *Advances in the Convergence of Blockchain and Artificial Intelligence*, 73.

Jia, C. (2014, March). *Impossible triangle: Security, environmental protection and decentralization.* Retrieved from https://bitcoinmagazine.com/culture/impossible-trinity-security-environment-protection-decentralization-1393990003

Johnson, A. B. (2016, Jun). *How does the dash dao work?* Retrieved from https://www.dash.org/forum/threads/how-does-the-dash-dao-work.9560/

Jumpfactor. (2022, March). *7 cloud computing security issues and challenges.* Retrieved from https://www.buchanan.com/cloud-computing-security-issues/

Kasireddy, P. (2021, September). *The architecture of a web 3.0 application.* Retrieved from https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application

Kastrenakes, J. (2021, Mar). *Beeple sold an nft for $69 million.* The Verge. Retrieved from https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million

Kay, G. (2021, November 28). *Who invented bitcoin? the alleged identities of its creator.* Business Insider. Retrieved from https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12

Kedrosky, E. (2022). *Worst aws data breaches of 2021.* Retrieved from https://securityboulevard.com/2021/12/worst-aws-data-breaches-of-2021/

Kemp, J., & Livingstone, D. (2006). Putting a second life "metaverse" skin on learning management systems. In *Proceedings of the second life education workshop at the second life community convention* (Vol. 20). Retrieved from http://hibgroupbpr.pbworks.com/f/Second+Life.pdf#page=22

Kirvan, P. (2022, April). *How much energy do data centers consume?* TechTarget. Retrieved from https://www.techtarget.com/searchdatacenter/tip/How-much-energy-do-data-centers-consume

Kostamis, P., Sendros, A., & Efraimidis, P. (2021). Exploring ethereum's data stores: A cost and performance comparison. *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. doi: 10.1109/brains52497.2021.9569804

Kuhn, D. (2022, Mar). *Assangedao raised $56m and quickly split up. was it still a success?* CoinDesk. Retrieved from `https://finance.yahoo.com/news/assangedao-raised-56m-quickly-split-210057108.html`

Kumar, R. (2022, May). *Aws market share 2022: How far it rules the cloud industry?* WPOven. Retrieved from `https://www.wpoven.com/blog/aws-market-share/`

Lambden, D. (2021, October). *Metaverse meetings – the future of work or a facebook gimmick?* Retrieved from `https://tech.co/news/facebook-metaverse`

Larimer, D. (2013, November). *Dac revisited.* LTB Network. Retrieved from `https://letstalkbitcoin.com/dac-revisited`

Lau, P. L. (2022, February). *The metaverse: three legal issues we need to address.* The Conversation. Retrieved from `https://theconversation.com/the-metaverse-three-legal-issues-we-need-to-address-175891`

Ledger. (2022, January). *Your guide to the metaverse.* Retrieved from `https://www.ledger.com/academy/your-guide-to-the-metaverse`

Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., … Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*.

Lehmann, S. (2022, May). *Storage cost on ethereum network.* ProDerivatives. Retrieved from `https://proderivatives.com/blog/2019/5/10/minimizing-data-storage-cost-on-the-ethereum-network`

Lehrig, S., Eikerling, H., & Becker, S. (2015). Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics. In *Proceedings of the 11th international acm sigsoft conference on quality of software architectures* (pp. 83–92).

Lichtigstein, A. (2020, May). *Permissioned vs permissionless blockchains.* 101 Blockchains. Retrieved from `https://101blockchains.com/permissioned-vs-permissionless-blockchains/`

Lohr, S. (2020). Cloud computing is not the energy hog that had been feared. *Retrieved January*, *14*, 2021.

Lowi, T. J. (1972a). Four systems of policy, politics, and choice. *Public administration review*, *32*(4), 300.

Lowi, T. J. (1972b). Four systems of policy, politics, and choice. *Public administration review*, *32*(4), 298–310.

Madiega, T., Car, P., Niestadt, M., & Pol, L. V. d. (2022, June). *Metaverse: Opportunities, risks and policy implications.* European Parliament. Retrieved from `https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf`

Mahmood, S. (2021). Instructional strategies for online teaching in covid-19 pandemic. *Human Behavior and Emerging Technologies*, *3*(1), 199–203.

Malwa, S. (2020, October). *70% of ethereum nodes are hosted on centralized services.* Decrypt. Retrieved from `https://decrypt.co/44321/70-of-ethereum-nodes-are-hosted-on-centralized-services`

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020a). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 985.

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020b). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 984–986.

Matob. (2022). *Top nft blockchains for 2022.* Retrieved from https://matob.web.id/news/top-nft-blockchains-for-2022/

Mell, P., Grance, T., et al. (2011). *The nist definition of cloud computing.* Computer Security Division, Information Technology Laboratory, National ....

Meta. (2021, November). *The facebook company is now meta.* Retrieved from https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

Microsoft, A. (2022, April). *Azure blob storage pricing.* Microsoft. Retrieved from https://azure.microsoft.com/en-us/pricing/details/storage/blobs/#pricing

Miller, A. (2019). Permissioned and permissionless blockchains. *Blockchain for Distributed Systems Security*, 193–204.

Moe, K. (2021, November). *The metaverse: Will it be a decentralized haven or a centralized tyranny?* Cointelegraph. Retrieved from https://cointelegraph.com/news/the-metaverse-will-it-be-a-decentralized-haven-or-a-centralized-tyranny

Mohanan, R. (2022, February). *What is elastic computing? definition, examples, and best practices.* Retrieved from https://www.toolbox.com/tech/cloud/articles/what-is-elastic-computing/

Moore, T. (2013). The promise and perils of digital currencies. *International Journal of Critical Infrastructure Protection*, *3*(6), 147–149.

Morton, B. (2021, Dec). *Julian assange can be extradited to the us, court rules.* BBC. Retrieved from https://www.bbc.com/news/uk-59608641

MRFR. (2022, January). *Web 3.0 blockchain market projected to grow exponentially by 2030 - report by market research future (mrfr).* Market Research Future. Retrieved from https://www.globenewswire.com/news-release/2022/01/04/2360814/0/en/Web-3-0-Blockchain-Market-Projected-to-Grow-Exponentially-by-2030-Report-by-Market-Research-Future-MRFR.html

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486–497.

Nabben, K. (2021). Decentralised autonomous organisations (daos) as data trusts: A general-purpose data governance framework for decentralised data ownership, storage, and utilisation. *Available at SSRN*.

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the nft revolution: market trends, trade networks, and visual features. *Scientific reports*, *11*(1), 1–11.

Nakamoto, S. (2008). *Bitcoin whitepaper.* Retrieved from https://bitcoin.org/bitcoin

Ngari, B. (2022, May). *Did do kwon know the luna and ust crash was coming? — legal documents reveal new findings.* ZyCrypto. Retrieved from https://zycrypto.com/did-do-kwon-know-the-luna-and-ust-crash-was-coming-legal-documents-reveal-new-findings/

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... Daneshmand, M. (2021). A survey on metaverse: the state-of-the-art, technologies, applications, and challenges. *arXiv preprint arXiv:2111.09673*.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187.

OECD. (2019). *Blockchain technologies as a digital enabler for sustainable infrastructure.* Organisation for Economic Co-operation and Development Paris, France.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing* (Vol. 34) (No. 3). Elsevier.

Ortega, A. (2022, February 22). *Will web3 save liberal democracy?* Real Instituto Elcano. Retrieved from https://www.realinstitutoelcano.org/en/will-web3-save-liberal-democracy/

Ossi, N. (2003). *Semantic web: Definition.* Retrieved from http://www.w3c.tut.fi/talks/2003/0331umediaon/slide6-0.html

Pakhira, A. (2019, September). *Council post: How cloud computing is democratizing development and accelerating innovation.* Forbes Magazine. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/08/27/how-cloud-computing-is-democratizing-development-and-accelerating-innovation/?sh=22fa162a58df

Parga, B. (2021, November). *Internet computer vs other top blockchains: Competing to build the future.* Retrieved from https://www.dfinitycommunity.com/internet-computer-vs-layer-1-blockchains/

Park, S.-M., & Kim, Y.-G. (2022). A metaverse: taxonomy, components, applications, and open challenges. *IEEE Access*.

Parliament, E. (2022, February). *Question for written answer e-000656/2022 to the commission.* Retrieved from https://www.europarl.europa.eu/doceo/document/E-9-2022-000656_EN.html

Pena, B. P. (2021, September). *How to become an internet computer node operator: Beginner's guide.* Dfinity Community ∞. Retrieved from https://www.dfinitycommunity.com/how-to-become-node-operators/

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239–278). Springer.

Peterson, R. (2022, March). *Advantages and disadvantages of cloud computing.* Retrieved from https://www.guru99.com/advantages-disadvantages-cloud-computing.html

Plotņikovs, A., & Kodors, S. (2017). Advantages and disadvantages of cloud computing. In *Human. environment. technologies. proceedings of the students international scientific and practical conference* (pp. 180–183).

Prusty, N. (2017). *Building blockchain projects*. Packt Publishing Ltd.

PYMNTS. (2022, May). *Overwhelmed by nft transactions, solana crashes.* Retrieved from https://www.pymnts.com/cryptocurrency/2022/another-blockchain-overwhelmed-by-nft-transactions-as-solana-crashes-outright/

Rai, R. (2022, January). *An overview of web3 venture capital activity in 2021.* Forbes Magazine. Retrieved from https://www.forbes.com/sites/rahulrai/2022/01/02/an-overview-of-web3-venture-capital-activity-in-2021/?sh=21aa661f1f16

Rain. (2022, April). *Pow, pos, poa—the most popular blockchain consensus mechanisms.* Author. Retrieved from https://www.rain.bh/learn/pow-pos-poa-the-most-popular-blockchain-consensus-mechanisms

Ramage, J. (2022, May). *The metaverse could add $3 trillion to the global economy within a decade, new study suggests.* Euro News. Retrieved from https://www.euronews.com/next/2022/05/18/the-metaverse-could-add-3-trillion-to-the-global-economy-within-a-decade-new-study-suggest

Ranger, S. (2022, February). *What is cloud computing? everything you need to know about the cloud explained.* ZDNet. Retrieved from https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

Reiff, N. (2021, November). *5 companies owned by facebook (meta).* Investopedia. Retrieved from https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

Reiseman, P. (2022, July). *On-chain governance.* District0x. Retrieved from https://education.district0x.io/general-topics/what-is-governance/on-chain-governance/

Roach, J. (2022, February). *Mesh for microsoft teams aims to make collaboration in the 'metaverse' personal and fun.* Retrieved from https://news.microsoft.com/innovation-stories/mesh-for-microsoft-teams/

Rodrigues, U. R. (2018). Law and the blockchain. *Iowa L. Rev.*, *104*, 679.

Rosenfeld, M. (2012). Overview of colored coins. *White paper, bitcoil. co. il*, *41*, 94.

Saberhagen, N. v. (2013, October 17). *Cryptonote v 2.0.* Retrieved from https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf

Salami, I. (2021). Challenges and approaches to regulating decentralized finance. *American Journal of International Law*, *115*, 425–429.

Sam. (2022, March). *Blockchain technology: What are the disadvantages of blockchain?* Marca. Retrieved from https://www.marca.com/en/technology/2022/03/10/622a292146163f62688b45ce.html

Sandler, V. (2022, February). *Cloud misconfiguration and how to avoid it?* Retrieved from https://blog.lightspin.io/cloud-misconfiguration

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, *9*(9), 1788.

Sharma, M. (2022, January). *Web 1.0, web 2.0 and web 3.0 with their difference.* Geeks for Geeks. Retrieved from https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/

Shen, M. (2022, January). *Electric capital developer report (2021).* Electric Capital. Retrieved from https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d

Siffert, S. (2022, June). *Computation and storage costs.* Internet Computer Association. Retrieved from https://internetcomputer.org/docs/current/developer-docs/deploy/computation-and-storage-costs/

Sigalos, M. (2022, February). *More than $320 million stolen in latest apparent crypto hack.* Retrieved from https://www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html

Singh, A. B., Bhat, S., Raju, R., D'Souza, R., et al. (2017a). Survey on various load balancing techniques in cloud computing. *Adv. Comput*, *7*(2), 29.

Singh, A. B., Bhat, S., Raju, R., D'Souza, R., et al. (2017b). Survey on various load balancing techniques in cloud computing. *Adv. Comput*, *7*(2), 28–34.

Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. In *2016 2nd international conference on contemporary computing and informatics (ic3i)* (p. 463-467). doi: 10.1109/IC3I.2016.7918009

Siyal, G. (2022, January). *Top 5 cloud security data breaches in recent years.* Retrieved from https://www.makeuseof.com/top-recent-cloud-security-breaches/

Solana. (2021, December). *Solana documentation: Synchronization.* solana. Retrieved from https://docs.solana.com/cluster/synchronization

Solana. (2022). *Overview | metaplex docs.* Retrieved from https://docs.metaplex.com/architecture/deep_dive/overview

Spivack, N. (2011). *Web 3.0: The third generation web is coming.* Retrieved from https://lifeboat.com/ex/web.3.0

Starry. (2019, June 19). *What was the first web browser?* Author. Retrieved from https://starry.com/blog/inside-the-internet/what-was-the-first-web-browser

Stephenson, N. (1992). *Snow crash*. Bantam Books.

Stephenson, N. (2003). *Snow crash: A novel*. Spectra.

Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), 1–9.

Sun, Z. (2021, December 2). *Adidas enters the metaverse with nft partnerships.* Cointelegraph. Retrieved from https://cointelegraph.com/news/adidas-enters-the-metaverse-with-nft-partnerships

Surbhi, S. (2021, February). *Difference between rules and policies.* Retrieved from https://keydifferences.com/difference-between-rules-and-policies.html

Swartz, J. (2021, November). *What is the 'metaverse' and how much will it be worth? depends on whom you ask.* MarketWatch. Retrieved from https://www.marketwatch.com/story/what-is-the-metaverse-and-how-much-will-it-be-worth-depends-on-whom-you-ask-11637781312

Swilley, E. (2016). Moving virtual retail into reality: Examining metaverse and augmented reality in the online shopping experience. In *Looking forward, looking back: Drawing on the past to shape the future of marketing* (pp. 675–677). Springer.

Szabo, N. (1997). *The idea of smart contracts.* Retrieved from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Tarcan, H. (2022, April). *Nodes and clients.* Ethereum.org. Retrieved from https://ethereum.org/en/developers/docs/nodes-and-clients/

Taylor, E. (2021, Oct). *How nft minting works - an initial guide to nfts.* Retrieved from https://azbigmedia.com/business/how-nft-minting-works-an-initial-guide-to-nfts/

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156.

Trotz, E. D. (2019). The times they are a changin': Surveying how the howey test applies to various cryptocurrencies. *Elon L. Rev.*, *11*, 201.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17.

VMware. (2022, May). *What is cloud scalability?* Retrieved from https://www.vmware.com/topics/glossary/content/cloud-scalability.html

Watts, A. (2022, April). *Layer-1 performance: Comparing 6 leading blockchains.* CoinCodex. Retrieved from https://coincodex.com/article/14198/layer-1-performance-comparing-6-leading-blockchains/

Williams, D. (2017, January). *The dfinity "blockchain nervous system".* Medium. Retrieved from https://medium.com/dfinity/the-dfinity-blockchain-nervous-system-a5dd1783288e

Williams, D. (2020, September). *A technical overview of the internet computer.* Medium. Retrieved from https://medium.com/dfinity/a-technical-overview-of-the-internet-computer-f57c62abc20f

Williams, M. (2022, June). *What is terra luna? why did it crash 99.9%?* Business 2 Community. Retrieved from https://www.business2community.com/crypto-news/what-is-terra-luna-and-why-did-it-crash-02493117

Wong, B. (2021, Aug). *The history of nfts & how they got started.* Portion Blog. Retrieved from `https://blog.portion.io/the-history-of-nfts-how-they-got-started/`

Wood, G. (2016). *Polkadot: Vision for a heterogeneous multi-chain framework draft 1.* Retrieved from `https://polkadot.network/PolkaDotPaper.pdf`

Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., … Miao, C. (2022). A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *arXiv preprint arXiv:2203.05471*.

Yakovenko, A. (2017). *Solana: A new architecture for a high performance blockchain v0.8.13.* Retrieved from `https://solana.com/solana-whitepaper.pdf`

Yesyev, A. (2022, January). *Prevent the top 3 security threats in the cloud in 2022.* Retrieved from `https://accedian.com/blog/prevent-the-top-3-security-threats-in-the-cloud-in-2022/`

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 proceedings ieee infocom* (pp. 1–9).

Zadikoff, A. (2021, December). *Bitcoin forks: Protocols, upgrades, and changes.* Retrieved from `https://www.gemini.com/cryptopedia/bitcoin-fork-protocol-upgrades-blockchain-changes`

Zetzsche, D. A., & Woxholth, J. (2022). The dlt sandbox under the pilot-regulation. *Capital Markets Law Journal*, *17*(2), 212–236.

Zhao, X., Ai, P., Lai, F., Luo, X., & Benitez, J. (2022). Task management in decentralized autonomous organization. *Journal of Operations Management*.

A Interviews

A.1. Interview Questions

The interview Questions are divided into two part, with the second part again being divided into two parts. This is because the technical experts will be asked different questions from the policy experts, offering more detailed insight from each perspective.

The first part of the questionnaire is as follows:

1. What is your current role and at which company is this?
2. How is your role related to blockchain/cloud computing or policy industry?
3. How long have you worked in the blockchain, cloud computing or policy industry?
4. How long have you been interested in blockchain/cloud/ computing/blockchain policy?
5. Have you heard about the metaverse and if so, what do you know about it?

Note: if interviewee is not familiar with the metaverse, a small explanation will be given here.

From here on, the interviewees will be categorized into two different categories: technical and policy, which will each be asked different questions. The purpose for this is to get special insight from each perspective in the aim of increasing the results from the interviews. As a last touch, cloud computing experts are asked even more specific questions on the respective technology and vice versa. With that being said, the second part for the technical experts is thus:

6. What technical aspects would be important when running the metaverse on blockchain/cloud computing?
7. In your opinion, what are some of the security issues when it comes to the data of the of users in the metaverse when built on the blockchain/cloud computing?
8. Which technology is superior in this respect?
9. Are you expecting blockchain/cloud computing to make further developments in the next few years to be a better technology to host the metaverse?

   For cloud computing experts:

   (a) How do you think the challenges can be addressed? (From the given aspects in Q9.)

   For blockchain experts:

(b) If future regulations were to come to blockchain, what are some of the most important aspects of blockchain that, in your opinion, should be regulated and some that should not be regulated?
(c) How are these regulations tied to the metaverse?
(d) From list shown, which possible regulations would fit within the EU and how would you rank these?
(e) In your opinion, what additional regulations should there be for the metaverse to be a safe environment for everyone?

The question for the other second part that will only asked to policy experts on blockchain are:

10. Are you familiar with the MiCA and DORA regulatory frameworks in the EU? If so, could you briefly explain them?
11. To your knowledge, are there currently any other regulation of policies on blockchain in the EU?
12. Which other aspect(s) should be regulated first for future regulations in the EU?
13. Do you think these regulations will have an effect on the metaverse and if so, how and why?
14. Besides the regulations that you mentioned, should there be additional regulations to target the metaverse specifically?
15. From list shown, which possible regulations would fit within the EU and how would you rank these?
16. Out of all the regulation that you mentioned, could you please rank them from most to least important with respect to the metaverse?

All of the questions above will obtain all the information needed in order to accurately formulate questions. One final question that will be asked regards future interest in the thesis:

16. Would you be interested in finding out the results of the thesis?

These are all the questions that will be asked to each interviewee and the data of which will then be analyzed. The list of Q15 and Q9d is shown in table 3.2.

A.2. Interview Summaries

As part of the ethics guidelines, the transcripts are not allowed to be made public, but must be summarized. The summaries will contain all necessary information needed to conduct the research and draw conclusions from them.

Interview #1

Interviewee #1 has a background in cryptography and has been working in the industry for the past 3.5 years and has been involved in both developing cryptographic proofs, as well as aiding other companies in doing so. Interest in blockchain began prior to this however, towards the end of 2017.

As the field of knowledge is cryptography and privacy, it was not a surprise that the interviewee mentioned that the privacy of users is a big issue with public blockchains. The interviewee proposed a solution that makes use of L2 blockchains, which can, in a way, encrypt the data and then push this version to the L1 blockchain. In this scenario, no one could directly see what this encrypted message holds, only users that have access to the L2 version of the encrypted message will know the information that it contains. For future developments, this interviewee mentioned that scaling is one of the biggest improvements that will happen, for both L1 and L2 blockchains. This, in-turn, will help it make it an even better fit to host the metaverse on the blockchain.

When presented with the 9 potential regulatory factors, this interviewee seemed to be already familiar with all of them. This is likely due to the fact that the participant is actively working in the field and has a very deep and broad understanding of the technology. Without hesitation, the top 3 is: data privacy, intellectual property and KYC. Data privacy was previously touched upon and is also the aspect where this interviewee is specialized. The second rank was given to intellectual property as there are many 'creator economies' that happen inside of blockchain, which should be addressed. While KYC is the third on the list, but still of utmost importance according to the interviewee. Users must be able to prove who they are, while still maintaining some level of privacy.

Interview #2

Interviewee #2 is a blockchain protocol engineer and currently works for a blockchain company that is still developing and thus not have a public blockchain yet. The participant got into this by starting out with the programming language Solidity to create smart contracts on the Ethereum blockchain. After doing this for a year, they wanted a new challenges and decided to become a protocol engineer.

Having experience in both developing smart contracts and the blockchain itself, this participant is highly involved in many aspects of blockchain. More specifically, these aspects are crucial parts for a blockchain that could potentially host a metaverse in the future. Much like other interviewees, this interviewee also acknowledges that current blockchains still need more scalability in order to host such a big project on a blockchain. This could be done through either improving L1 blockchains or add L2 blockchains together, but the best would be to have both layers on a level that it is much more scalable.

When shown the 9 factors of regulation that might apply to blockchain, this participant knew most of the factors already and needed little explanation for each of them. When asked which were applicable, they only mentioned that governance & legal documentation, DAOs and KYC would not be applicable. However, it is possible that they missed the KYC factor, since they mentioned that there must be some sort of KYC earlier in the interview. The top 3 rankings were as follows: IP, data privacy and virtual asset taxes were first, second and third, respectively. The participant emphasized that this ranking would specifically be targeted for a metaverse built on a blockchain.

Interview #3

Interviewee #4 specializes in building application on cloud computing servers and has a high interest in blockchain technology as well. More specifically, this interviewee is a senior director of product development at a multi-national software company. The interest in blockchain is pursued by actively learning the new development that happen in the space as well as engage with the networks themselves.

Having a background of building software programs that must run 24/7, this interviewee acknowledges that currently, blockchains have lots of outages and are relatively unstable. This could be due to internal issues of the network itself, but also external issues, such as a solar flare, which was an example given by the interviewee. While also giving other reasons, the main idea of this interviewee is that the network, which includes the hardware and software that the programs run on must be properly built and ensured that neither can be easily taken down the next day. The same applies to the metaverse, it should be built in such a way and have certain regulations that someone cannot simply pull the plug on a project the next day, erasing the digital assets of users of that particular metaverse. This respective likely comes from the fact that this interviewee manages the development of software applications and understand the struggle of customers when programs do not work effectively or are simply outdated the next day. Another aspect mentioned was that this space will technically be borderless, which should be taken into account when addressing the space.

When the nine factors of blockchain were shown that could have regulation in the future, this interviewee approached these with a similar perspective. The most important factor to regulate is governance & legal documentation. When mentioning this, the interviewee emphasizes on the level of quality that the code must adhere to. The second and third ranked factors are data privacy and smart contracts, respectively. The comparison made by this interviewee is that developers of the metaverse will have similarities with companies. In the sense that there will be a product - the metaverse - with users, code and its all hosted somewhere. Therefore, taking the perspective that a reliable service should be offered to the users, with minimal downtime and risks, the interviewee came up with this specific list of top 3 most important factors.

Interview #4

Interviewee #5 works at Xreg consulting and has a background in working with the European Parliament and EU with developing a framework for crypto assets. The participant has been involved in this and similar activities for the past 8 years. This participant was highly involved with some of the aspects regarding the MiCA bill to ensure that the regulatory frameworks works for the market.

One of the most prominent elements that this interviewee touched upon is that the technology itself should not be regulated and thus have some sort of disadvantage for future developers. Rather, the use of the technology should be regulated, ensuring that users are protected against malicious actors. According to the interviewee, the MiCA bill has a similar nature, that the use of crypto assets are regulated and the same should apply for a future blockchain regulation, where either the use of blockchain and/or smart contracts should be regulated.

Going over the nine aspects that could potentially be regulated in a metaverse built on the blockchain, this participant decided to add an additional facts: transfer of value. What is meant by this is how the transactions are going to be completed in the metaverse. The participant continued by saying that with this new factor, other entities have clearer boundaries and what to tax. When asked to rank the aspects, this participant grouped the following four factors: governance & legal documentation, liability, DAOs and smart contracts. The newly added factor called 'transfer of value' is second and third is the KYC. The reason as to why this interviewee decided to group the four aspects together is because they approach the problem from a holistic point of view and essentially see many parts of the technology as one from a policy and regulatory perspective. As for the transfer of value, one could argue that it somewhat ties with the governance and legal documentation and could be included in that factor. Therefore, by expanding that definition, the second rank also includes governance and legal documentation. The third rank was given to the KYC factor, with an additional emphasis on digital identity, as also mentioned by other interviewees. Similar to others, the participant also had a say in the currently anonymous field that blockchain users are, which should change to a certain degree by adding a KYC layer on top of it.

Interview #5

Interviewee #6 is the secretary general of a blockchain policy advisory company in Europe. This was started in 2018, when the interviewee founded the company. The company actively participates in policy discussion and their most recent talks were with several parties involved with the creation of the MiCA framework in the EU.

This participant acknowledges that establishing country borders when it comes to creating policies and regulations is difficult and that some countries might have a different take then others when it comes to this. Therefore, the online identity should encompass such a variable. One of the issues that must be solved according to the interviewee is that the national regulations that apply to one are still relatively ambiguous when it comes to the metaverse. For example, someone with a Dutch passport that has a residency is two other countries (e.g. Spain and U.A.E.) can adhere to any of the policies of any of the three countries. Therefore, there should also be a clear definition of which countries' rules the users most comply with. Moreover, an additional issue would be when two nationalities do business with each other in the metaverse. This can be in form of collaborating on projects or transferring digital goods from one nationality to another.

When the list of nine of possible regulations were presented, the respondent mentioned that all of the already exist, but must be adjusted to be applied to the metaverse. While some of them are a bit more applicable, as they can be taken from the MiCA framework, most of them must undergo several changes in order to be applied fully to the metaverse. As rankings, this interviewee put the IP rights as most important, followed by data privacy and put liability and regulation of conduct in third position. Since this person is in direct contact with many politicians because of the position they are in, they were also able to give the perspective of those politicians when it comes to ranking the most important factors. The interviewee mentioned that the politicians are most concerned with taxing several aspects of the metaverse and get some regulations in for that part, with KYC and liability coming in second and third place, respectively. This creates a clash between politicians and policy advisors that also include the perspectives of users and developers.

Interview #6

Interviewee #7 currently has multiple roles that are in the blockchain are. The main roles that count towards the expertise needed to conduct the interview is the experience with dealing with blockchain policy strategies in collaboration with organizations such as the World Economic Forum (WEF). This interviewee has been involved with similar technologies since 2007, which gradually built up to advising on DAOs.

When asked what the first aspect that should be regulated in the metaverse that does not yet have regulations is the identities within the metaverse. However, the interviewee argues that this should not be done through traditional KYC procedures, but should encapsulate more of the person's real identity, rather than a few questions that only take a snippet of the person's details.

When asked about regulations of different aspects of blockchain, the interviewee mentioned that there need to be new ways of creating and implementing policies and regulations for blockchain. Since this technology allows for new and innovative ways to implement codes and contracts (smart contracts), the world should take advantage of this technology breakthrough and use it in order to create regulations in this manner. The interviewee argues that there would be multiple benefits to doing this, including: no need for intermediaries such as courts, lawyers and judges, and that it would be much more efficient. In this respect, the law would be written in code and deployed on the blockchain where the metaverse is hosted. This would make any process that involves wrong doing or breaking this code much more efficient.