MASTERARBEIT | MASTER'S THESIS

Titel | Title

The (R)Evolution in Data Ownership

Redefining the notion of data ownership through the means of technology and how this shift affects societies

verfasst von | submitted by

Christoph Edelbrunner BA

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 905
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Soziologie
Betreut von | Supervisor:	Assoz. Prof. Mag. Dr. Maximilian Fochler

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Max Fochler, for his invaluable support and guidance throughout this master's thesis. Thank you for your trust, for allowing me the flexibility to explore this topic, and for providing your expertise – all of which played a vital role for the success of the thesis.

I would like to extend my sincere thanks to State Secretary for Digitalization of Austria, Claudia Plakolm, for taking the time to discuss today's pressing topics in an engaging and insightful interview.

This entire academic journey would not have been possible without the unwavering moral and financial support of my parents, Gabriela and Manfred. I am deeply indebted to both of you and incredible grateful for making all this possible and for believing in me. Many thanks also go to my little sister, Michaela, who has provided me with support and encouraging words throughout.

Finally, my deepest appreciation goes to my partner, Nastassya, for providing constant moral support throughout my entire time of studying. Your acceptance, understanding, motivation, and encouragement during this time are highly appreciated.

AI Usage within this Thesis

I acknowledge the use of generative AI tools such as ChatGPT, Amberscript, and Paperpal in the preparation of this thesis. These tools were utilized for tasks including grammar and spelling corrections, comma placement, summarizing, transcribing interviews, and providing suggestions for alternative wording. I hereby confirm, that I applied these tools with caution and critically reviewed their outputs at all times. I acknowledge their impact and contributions to this thesis and hereby affirm that I consistently reflected on the accuracy and validity of the results generated. I can also state, that using the tools as mentioned has enhanced my understandings of the subject of generative AI. Furthermore, I ensure that this thesis complies with the AI usage guidelines provided by the University of Vienna (KI in Studium and Lehreunivie.ac.at, as of January 2024), and adheres to the standards for academic research.

Abstract

This master's thesis explores the concept of data ownership in the context of digital capitalism and emerging technologies. It examines the mechanisms driving contemporary business models, stresses the necessity of clarifying the notion of data ownership, and investigates the potential role of blockchain technology and its smart contract applications in addressing issues related to digital identity and ownership structures.

Aiming to answer the question "What are the future imaginaries of different actors within the digital economy regarding data ownership and the role of emerging technologies, such as blockchain, in digital societies?" it follows a qualitative exploratory research design by conducting expert interviews. From a sociological perspective and looking through a Science and Technology Studies (STS) lens, this study analyzes the democratization of information access and sharing, the shift from centralized private ownership to decentralized ownership, and its implications for power dynamics in modern society.

The results indicate an increase in the attention of data ownership and proliferation of real-world use cases across industries that utilize blockchain applications for (decentralized) digital identities and data sovereignty. Furthermore, the study challenges prevalent assumptions about blockchain's capabilities. By gathering and interpreting future imaginaries of data ownership and blockchain technology, this study contributes to the ongoing discourses on digital capitalism, data governance, and the reshaping of ownership paradigms in the digital realm.

KEY WORDS: Digital Capitalism, Power, Data Ownership, Digital Identity, Decentralization, Emerging Technologies, Blockchain Technology, Smart Contracts, STS, Sociology

Abstract (ger)

Diese Masterarbeit untersucht das Konzept des Datenbesitzes im Kontext des digitalen Kapitalismus und aufstrebender Technologien. Die Arbeit analysiert jene Mechanismen, die moderne Geschäftsmodelle antreiben, betont die Notwendigkeit, den Begriff des Datenbesitzes zu klären und untersucht die potenzielle Rolle der Blockchain Technologie und Smart Contract Anwendungen bei der Bewältigung von Herausforderungen im Zusammenhang mit digitaler Identität und Eigentumsstrukturen.

Um die Forschungsfrage – Was sind die Zukunftsvorstellungen verschiedener Akteur:innen innerhalb der digitalen Wirtschaft in Bezug auf Datenbesitz und die Rolle aufstrebender Technologien wie Blockchain in digitalen Gesellschaften? – zu beantworten, werden Expert:inneninterviews durchgeführt. Die Forschung folgt dabei einem qualitativen, explorativen Forschungsdesign. Diese Studie analysiert aus einer soziologischen sowie einer Wissenschafts- und Technikforschungs- (STS) Perspektive die Demokratisierung des Informationszugangs und -austauschs, den Wandel von zentralisiertem Besitz hin zu dezentralisiertem Besitz sowie die daraus resultierenden Auswirkungen auf Machtdynamiken in modernen Gesellschaften.

Die Ergebnisse deuten darauf hin, dass Datenbesitz zunehmend an Aufmerksamkeit gewinnt und es vermehrt zu Anwendungsfällen in verschiedenen Branchen kommt, die Blockchain für (dezentralisierte) digitale Identitäten und Datensouveränität nutzen. Die Studie hinterfragt zudem kritisch gängige Annahmen über die Fähigkeiten der Blockchain Technologie. Durch die Sammlung und Interpretation von Zukunftsvorstellungen über Datenbesitz und die Rolle der Blockchain Technologie trägt diese Studie zu den laufenden Diskursen über digitalen Kapitalismus, Datenverwaltung und die Neugestaltung von Eigentumsparadigmen im digitalen Raum bei.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

A

AI *Artificial Intelligence*

AR *Augmented Reality*

C

CAGR *Compound Annual Growth Rate*

D

DI *Digital Identity*

DID *Decentralized Identifier*

DO *Data Ownership*

G

GDPR *General Data Protection Regulation*

GT *Grounded Theory*

I

IoT *Internet of Things*

P

P2P Peer-to-Peer

S

SCM *Supply Chain Management*

SQ1 *Subquestion 1*

SQ2 *Subquestion 2*

SQ3 Subquestion 3

SSI *Self-Sovereign Identity*

STS *Science and Technology Studies*

V

VR *Virtual Reality*

W

Web 1.0 *Static Read-Only Web Pages*

Web 2.0 *Information-Centric and* Interactive

Web 3.0 *User-Centric and Decentralized*

Z

ZK-proof *Zero-Knowledge-Proof*

"Hackers create the possibility of new things entering the world. Not always great things, or even good things, but new things. In art, in science, in philosophy and culture, in any production of knowledge where data can be gathered, where information can be extracted from it, and where in that information new possibilities for the world produced, there are hackers hacking the new out of the old. While we create these new worlds, we do not possess them. That which we create is mortgaged to others, and to the interests of others, to states and corporations who monopolize the means for making worlds we alone discover. We do not own what we produce – it owns us." – Wark 2004: [004]

1 Introduction

Innovation, technological development, and disruption have long been the central forces shaping societal structures and relations. Particularly over the course of the 18th until the 21st century, from the First Industrial Revolution to today's rising Fourth Industrial Revolution, societies have continuously been confronted with numerous challenges and have been compelled to adapt to rapidly shifting environments. Over the past two centuries, in particular, the mechanization of entire industries, proliferation of new technologies, and emergence of new factories and markets have transformed not only the economy but also the fabric of social life.

Since the late 20th century and the dawn of the 21st century and with the rise of the Internet, human interactions, labor, and social relations have steadily been transformed into the digital realm. New, ever-expanding corporations are driving these transformative shifts, covered by capitalism's thrive, centered around the extraction and monetization of a new resource: data. Characterized by profit maximization, wealth accumulation, exploitation (Marx 1844/1932), and creative destruction (Schumpeter 1943), industrial capitalism has evolved into its contemporary form: digital capitalism (Staab 2021).

With the rise of digital capitalism, the introduction of new technologies, and the emergence of Big Tech (Birch & Bronson 2022), data has become one of the most valuable resources of our time – at least for the firms that specialize on the processes of extensive data extraction. These processes enable tech firms to gain power and control over data, allowing their powerful algorithms to analyze vast datasets, distill additional information, and ultimately sell that information for profit. The possession, control, and power over these datasets have facilitated the rise of a new class of capitalists – a class that does not own the means of production but rather has ownership over information (Srnicek 2017; Wark 2004). Driven by the strive to expand their proprietary business operations (Staab 2021) into nearly every sector of society, with new data-extraction applications being introduced every day and novel ways to extract, accumulate, and store user's data, the new class of capitalists continues to consolidate power and wealth by transforming information into valuable and lucrative commodities. However, the business models of today's capitalists raise concerns about the strategies and methods used to collect, store, and sell data.

The proliferation of online activities in contemporary digital landscapes has led to an exponential increase in the creation of digital footprints. This development has prompted societies to ask fundamental questions about data privacy, its ownership, and control. Along with critical questions concerning the power and control over data, the topic of data ownership has gained attention in recent years. However, the concept of data ownership still remains ambiguous and controversial, with no unified definition or consensus (Asswad & Gómez 2021). Today, it can be argued that digital footprints rightfully belong to those that created them. However, because of the absence of a common identity layer (Voshmgir 2020), digital footprints predominantly belong to the owners of today's digital infrastructures, often platform operators (Srnicek 2017). Some argue that early visionaries did not foresee the need for this, as they envisioned the Internet as a decentralized network of computers with democratic values, equal information access and sharing, free from hierarchies, limits, or boarders (see Berners-Lee 2000; Mager 2010: 44).

However, emerging technologies such as blockchain have gained increasing attention over the last few years; not simply because of cryptocurrencies, which are based on and enabled by blockchain technology, but also because of blockchain's promises to address the challenges of digital ownership (e.g. McConaghy et al. 2017; Tapscott & Tapscott 2017; Zyskind et al. 2015). The technology promises to redefine ownership rights (Tapscott & Tapscott 2017) and the ways in which data is managed, shared, and owned (Asswad & Gómez 2021). Despite blockchain's nascent stage of development and adoption (Osborne & Laing 2021), with its true future potential only beginning to be explored (Rozas et al. 2021), its impacts are already envisioned to be wide-ranging and highly disruptive (Treiblmaier 2019; Treiblmaier and Beck 2019a,b; Tapscott and Tapscott 2017; Yli-Huumo et al. 2016). In comparison to industry adoption, however, its rigorous exploration in leading academic journals still lags substantially (Treiblmaier 2019: 1). The increasing prominence of blockchain technology has garnered significant attention across industries, and its purported promises and potential necessitate more rigorous research.

As a result, this thesis aims to contribute to the lack of literature concerning blockchain-based applications for data ownership use cases. Capitalism, along with its driving forces, represents the context of this study. By analyzing both the historical trajectory of capitalism and its impacts on the transitions from industrial to post-industrial and digital societies, this research aims to examine both the challenges that have emerged from these developments and their implications for data ownership (DO) and digital identity (DI). Ultimately, this thesis aims to provide an overview of addressing these challenges and discuss potential approaches for tackling them through technological innovation, particularly with the help of blockchain technology.

Moreover, the thesis aims to provide clarity on whether blockchain technology can effectively help address the various challenges found in the literature, including topics such as private property (Tapscott & Tapscott 2017), decentralized privacy (Zyskind et al. 2015), digital identity (Careja and Tapus 2023; Tapscott & Tapscott 2016), particular forms of capitalistic asymmetries (Srnicek & Williams 2015), shifting societal structures (Sandstrom 2017; Tapscott & Tapscott 2017), and exploring whether blockchain could be used for social good (Semenzin 2023) or, as Dávila (2023) points out, for more "radical purposes, beyond individual profit [Crypto] and more towards collective autonomy."

Rapid technological changes in the digital era demand a comprehensive understanding that extends beyond technical expertise. The development of blockchain technology and data ownership requires interdisciplinary knowledge and skills to address societal needs effectively. Delving into these topics and discussing the various promises of blockchain can be pivotal in gaining a more comprehensive understanding of its nature and social aspirations. Sociologists, in particular, play a crucial role in understanding the various implications of blockchain on societal structures, power dynamics, and individual agency in terms of self-sovereign identity, as well as on the notion of trust.

Therefore, this research explores the topics of data ownership, digital identity, and (future) blockchain applications from a sociological perspective and by employing a Science and Technology Studies (STS) framework. The study situates this exploration within the context of capitalism. Investigating these topics through an STS lens will allow us to examine and unravel sociotechnical imaginaries (Jasanoff & Kim 2015) surrounding data ownership, digital identity, and blockchain technology, along with their possible implications for existing hierarchical power dynamics.

The structure of this thesis is presented on the following page:

Chapter 1 begins with an introduction to the general topic of this thesis by presenting an overview of its eight distinct chapters: introduction, theoretical background, blockchain technology, sensitizing concepts, methodology, results, discussion, and conclusion.

Chapter 2 provides the theoretical background for this study. It explores the historical trajectory of capitalism, focusing on the shift from industrial capitalism to digital capitalism over the course of the last century to better understand the challenges digital societies like ours face today. This chapter presents the essence of capitalism, the emergence of platforms as the new infrastructure of society, the business models of today's digital economy driven by the extraction imperative, and an initial brief overview of the promises that blockchain technology tends to carry for various businesses, branches, and particular issues.

Chapter 3 begins with the introduction of blockchain technology along with its characteristics and current state of research. This is followed by an exploration of the Internet's evolution – from Web 1.0 to Web 3.0 – alongside its challenges. Additionally, this chapter explores the broad sociological topic of trust and introduces the role of intermediaries within societies, the characteristics and role of smart contracts, the topic and definition of data ownership, and particular use cases of blockchain technology.

The sensitizing concepts that constitute the theoretical framework of this thesis are explored in Chapter 4. This includes the introduction of lenses employed for investigating the topics of data ownership, digital identity, and blockchain technology, thereby facilitating a better understanding of these intersecting topics. Chapter 4 also presents a general overview of both the sociological relevance of this research topic and the core focus of the research question: sociotechnical imaginaries.

Chapter 5 outlines the methodology, including qualitative research in general, grounded theory, and the specific research method applied in this study, along with details of the sampling and the data analysis of the collected data.

Chapter 6 presents the results of expert interviews. Chapter 7 follows with a discussion of these results, linking them with the existing literature.

This thesis culminates in Chapter 8, which presents the conclusion of the key findings. Furthermore, this chapter discusses the implications of the key findings, the limitations of the thesis, and proposes avenues for future research.

2 Theoretical Background

"Study the past if you would define the future." – Confucius

The world, its environment, and societies are not static but rather a constant process of change. Therefore, comprehending the historical development of societies over time is essential for understanding their present state. In the context of this thesis, this necessitates examining how societies have evolved throughout the progression of data within emerging digital environments, which will help to elucidate the challenges and multifaceted impacts societies face today. This understanding is crucial for making informed decisions and shaping the future effectively, and furthermore, it allows for a better examination of the role of technology in addressing these challenges.

2.1 The Evolution of Capitalism – From its Roots to modern Markets

"The magnitude of the profit whets his appetite for more profit." – Marx 1887: 276

"Man is dominated by the making of money, by acquisition as the ultimate purpose of his life. Economic acquisition is no longer subordinated to man as the means for the satisfaction of his material needs" – Weber 1904-1905/2001: 18

Both quotes refer to what Weber (1904-1905) identified as the essence and spirit of capitalism: the continuous drive for profit maximization and the accumulation of wealth. The consequences for societies and the economy have been profound and extensive. Capitalism's drive has propelled innovation forward, leading to economic growth and prosperity, predominantly in contemporary Western societies, and has triggered significant shifts in societal structures. Moreover, capitalism has long been synonymous with rapid changes in both technology and the means of production (Srnicek & Williams 2015: 109).

For example, agriculture began to be mechanized during the 19th century, and craftwork was reimagined with the implementation of machinery, enabling higher efficiency and productivity. This mechanization resulted in the replacement of skilled workers with machinery, which significantly reduced the demand for skilled workers. “Work became increasingly repetitive, deskilled and ruled by machinery – with greater demand for cheap unskilled laborers (particularly women and children).“ (Srnicek & Williams 2015: 109). Marx (1887) exemplified the effects of the introduction of machinery, using England in 1861 as an example: mechanization, on the one hand, increased efficiency but displaced many workers, leading to high unemployment rates (309-310). The mechanization of industry and improved agriculture forced many workers to move out of traditional jobs (e.g. farmers) and to offer their labor-power cheaply to capitalists in order to survive. Marx (1887) noted that these people were “liberated” and freed from their old jobs, however, they consequently became available as cheap workers because they had no other choice but to sell their labor cheaply (270, 309-314). In addition, it was low wages in combination with ever-longer working hours that allowed capitalists to create greater surplus value. “It was in fact by the cheapness of the human sweat and the human blood, which were converted into commodities, that the markets were constantly being extended, and continue daily to be extended,” Marx writes (1887: 310).

Over time, in the early 20th century, new technologies eliminated the need for repetitive work being performed by humans. Consequently, the demand for skilled workers shifted into other parts of the economy where, for example, office technologies such as photocopiers or new software were introduced and had to be overseen by knowledgeable people. The continuous introduction of new technologies is driven by the systemic imperatives of generalized markets (Srnicek 2017). This means that when economic agents try to sell their products to other suppliers, competition arises, causing the necessity to reduce production costs in relation to prices. A significant way to achieve this is through the adoption of the most efficient techniques and technologies. Thus, the „logic of accumulation“ (ibid. 12), which is reducing costs and implementing the most efficient technologies, and “the intensification of the means of production, growth, and competition“ (Zuboff 2019: 337) while aiming to generate relentless profits, has become an imperative for the majority of businesses. Furthermore, “In the effort to cut costs, beat out competitors, control workers, reduce turnover time, and gain market share, capitalists are incentivized to continually transform the labor process.“ (Srnicek 2017: 12) The schematic model of capitalism not only demands constant technological change but eventually also causes societal shifts. Every time novel technologies are implemented to increase efficiency and productivity, certain changes occur throughout societal structures, affecting different members of societies to varying extents.

Throughout history, people have been replaced by advancing technologies in various ways and subjected to economic and physical exploitation by capitalists, resulting in the widening of the gap between the wealthy and the impoverished. The implementation of novel technologies invariably alters societal dynamics and affects how people work and interact. Under the logic of the capitalist mode of production, driven by accumulation, innovation, and profit maximization, such changes are further intensified, ultimately reshaping the notions of the economy and labor as a whole. Consequently, these changes and capitalistic dynamics disproportionately impact those who have no power and do not have a say, implying inequalities. Therefore, capitalism perpetuates major societal change. These changes predominantly benefit capitalists who either sit in the driving seat and drive these changes or own the means of production, which makes them superior to those who rely on employment and lack ownership rights. According to Marx, such asymmetries in both power and ownership are what capitalism has caused fundamentally: "centralized means of production, and (…) concentrated property in a few hands." (Marx 1994: 163) Marx explained the asymmetries between the proletarians and the bourgeoise, positing that proletarians have been used as a commodity so that the capital of the bourgeoise can increase due to divided labor.

For Marx, labor refers to human activity that produces value (Marx 1887). A capitalist, however, does not aim solely to create value in terms of use value, which represents the exact value of the compensation (wages) the laborer receives for selling their labor power to the capitalist; this compensation then allows laborers to survive by covering basic needs (e.g. food, shelter, etc.). Instead, the capitalist aims to produce surplus value (Marx 1844/1932: 131), which is produced by the laborer, creating more value than what they are getting paid for. As a result, the capitalist profits from the value that is produced during the worker's "unpaid-time" (Marx 1844/1932: 131-139). In Marx's words:

> The action of labour-power, therefore, not only reproduces its own value, but produces value over and above it. This surplus-value is the difference between the value of the product and the value of the elements consumed in the formation of that product, in other words, of the means of production and the labour-power. – Marx 1887: 146

The proletarians, Marx writes, "(…) are daily and hourly enslaved by the machine, by the overlooked, and above all, by the individual bourgeoise manufacturer himself." (1994: 165) Thereby, it is the laborer who "constantly produces material, objective wealth, but in the form of capital, of an alien power that dominates and exploits him" (Marx 1887: 401). This concept is further discussed by Marx (1844/1959) in *Economic and philosophic manuscripts of 1844* in the context of the "objectification of labor". Marx explained that the worker's product of labor is labor itself which "has been embodied in an object" which ultimately appears as a "loss of realization for the workers; objectification as *loss of the object and bondage to it*; appropriation as *estrangement,* as *alienation*." (29) Consequently, the worker relates to the product of his own labor "as to an alien object." (ibid.) It is private property, Marx argued, that eventually becomes "the product, the result, the necessary consequence of alienated labor, of the external relation of the worker to nature and to himself." (1844/1959: 33) Marx (1844/1959) explains alienation further:

> The product is after all but the summary of the activity, of production. If then the product of labor is alienation, production itself must be active alienation, the alienation of activity, the activity of alienation. In the estrangement of the object of labor is merely summarized the estrangement, the alienation, in the activity of labor itself. (30)

Labor under capitalism is transformed into a dehumanizing experience. According to Marx, the reason for this is that labor is not a fulfillment for the workers who can express their creativity but rather becomes objectified in the form of a product, owned by the capitalist. This results in alienation of laborers from not only the product itself but also from themselves and others, which both engenders and reinforces private property, facilitated by the capitalists who own the means of production and buy the cheap labor power of the workers (ibid.). It is particularly the essence of private property that needs to be changed in order to mitigate the asymmetries and to achieve freedom, according to Marx (1844/1959). Private property, according to Marx, causes *alienation* of the majority on the one side and the generation of capital for minorities on the other (ibid.). The effects of both are what Marx identifies as capitalism (see Marx & Engels 1848).

These effects, along with continuous technological advancements, have continued to evolve in the modern era. Today, this is happening at a rapid pace, leading to unprecedented outcomes and new challenges to rise. Srnicek & Williams (2015) summarize this succinctly: „We move faster – capitalism demands it; yet we go nowhere.“ (181). The implementation and utilization of technologies is generally a double-edged sword. The side effects of technological development and implementation can either be *negative*, leading to deskilling humans and the replacement of laborers, or they can be nurturing and beneficial by providing possibilities for mankind to flourish and thrive. Therefore, technology is neither inherently good nor bad. Its impact crucially depends on the ways in which technologies are utilized and on the purposes behind their use.

This brief elaboration on capitalism's dynamics and its driving forces will be discussed in Chapter 7 in the context of data ownership and blockchain technology, including topics such as trust, estrangement, and (centralized) private property.

2.2 From Industrial Capitalism to Digital Capitalism

"The progress of the privatization of property creates at each stage a class who own the means of producing a surplus from it, and a producing class dispossessed of it."
– Wark 2004: [100]

After a brief overview of the basics and logics of capitalism and its dynamics at play within market economies, the following section delves into the evolution and transition from industrial capitalism to capitalism's modern modes in today's digital economy. Discussing these two modes of capitalism will help grasp core distinctions and underline its fundamental logic.

Besides innovation, competition, and scarcity, Schumpeter (1943) has stressed in his works that „monopolistic competitors“ and *creative destruction* to be fundamental to the functioning of capitalism. Schumpeter (1943) found that traditional monopolistic firms follow the economy's logic of scarcity, which means that when products and goods are scarce and high in demand, prices can rise, followed by potential increased profit accumulation (Staab 2021). Moreover, Lionel Robbins (1932) stated that economic action is characterized by scarcity, emphasizing that only scarce products and goods are eventually profitable (see Staab 2021: 80). High demand for scarce products in a market environment characterized by competition and its fear urges businesses to constantly fight to improve and come up with newer products and lower prices to achieve revenue and market shares. This inherent logic of capitalism intensifies competition and profit maximization and, therefore, makes innovation and growth in both productivity and efficiency necessary among competitors, eventually resulting in disruption and societal change (Zuboff 2019).

Innovation, competition, disruption, and subsequent shifting societal structures were core characteristics of the First Industrial Revolution in the late 18th century, as the manufacturing and production processes underwent significant transformations. Owing to innovation, the application of novel technologies, and the mechanization of entire industries, new factories have emerged, resulting in increased productivity and efficiency. With the introduction of advanced technologies, production costs were reduced even further during the Second Industrial Revolution. Over the course of the late 19th and early 20th century innovation and specific technologies had vast impacts on telecommunication, transportation, and manufacturing processes (Staab 2021). This period saw fundamental economic transformations with the emergence of "Fordism", a concept centered around the idea of a balanced combination of efficient mass production and the equivalent mass consumption. Consequently, large-scale corporations have emerged, with capitalists owning the means of production, leading to unprecedented economic profitability on the one hand but significant changes in both life and labor on the other. This has resulted in societal transformation, exploitation, inequalities, and the rise of industrial capitalism. However, over time, this logic of the Fordist epoch in the 20th century changed as economic growth collapsed due to market saturation from the 1960s onwards (Staab 2021). When demand is decreasing and the market increasingly saturates, when there is less productivity and fewer products being sold, capitalism’s thrive is weakened. However, this does not imply that capitalism is about to collapse and that society promptly enters a post-capitalistic world. Instead, referring to the aforementioned issues with private property and its direct effects of *alienation* for the majority on one side and the generation of capital for the minority on the other, the bourgeoise (or capitalism in general) obviously aims to uphold its status, and hence the asymmetries. By exerting power and by leveraging continuous technological advancements and socio-economic advantages, the bourgeoise perpetuates alienation and capital accumulation, thereby nurturing capitalism’s thrive. Marx & Engels (1848) explain this in *The Communist Manifesto* as follows:

> The bourgeoise cannot exist without constantly revolutionizing the instruments of production, and thereby the relations of production, and with them the whole relations of society …. All fixed, fast-frozen relations, with their train of ancient and venerable prejudices and opinions, are swept away, all new-formed ones become antiquated before they can ossify. (1848/1969: 16)

Therefore, capitalism’s inherent need is to „occasionally“ reinvent itself in order to thrive, especially after a crisis. These fundamental ideas were later extended by Joseph Schumpeter. Schumpeter (1943) introduced the phrase *creative destruction,* which means a

> process of industrial mutation… that incessantly revolutionizes the economic structure *from within*, incessantly destroying the old one, incessantly creating a new one. This process of Creative Destruction is the essential fact about capitalism. It is what capitalism consists in and what every capitalist concern has got to live in. (82-83)

With that in mind, during the economic downturn in the midst of the 20th century, it was innovation and the discovery of new paths for the economy to grow that were considered to be the answers needed to overcome this crisis, eventually facilitating both *creative destruction* and capitalism to thrive again.

Digital network technologies in particular have played a pivotal role in facilitating this process by pushing three major characteristics within the emerging digital economy forward that would later imply significant changes throughout society: networking, decentralization and control (Staab 2021: 55) First, it was the integration of supply chains that led to transparent and ever more efficient work processes and enabled cost savings in planning, coordination, and logistics; second, the decentralization of particular work processes allowed outsourcing and the introduction of self-service systems through which the working costs significantly decreased because of “working customers”; third, early adopters of network technologies recognized the potentials of generating profits through the control of markets, which was to make users dependent on proprietary software and make their software usage a routine so that they will never leave (Staab 2021: 55-58). Networking, decentralization, and control then nurtured the future macrotrends of capitalistic reorganization, which are rationalization and automation of additional work areas, globalization of value chains, public investments, commodification and privatization of public goods, and financialization of the economy. (Staab 2021: 58-67).

The introduction of digital network technologies at this specific time also marks the beginning of the digitalization of capitalism (Staab 2021: 55) and the progressively emerging era of post-industrialism, characterized by a shift from traditional manufacturing-based economies to service-based economies with digital innovation, information technologies, and ubiquitous connectivity and availability at its core, ultimately resulting in significant shifts within society. Such consequences of the evolving digital capitalism include, for instance, that digital connections are perceived as a necessary means for social participation (Zuboff 2019: 455). Everyone who does not have an Internet connection is, to some extent, unable to engage with the connected world, and is therefore excluded and left behind. Making decisions about who is “good enough,” or allowed to be provided with Internet connection thus able to participate globally and who is not, represents a privilege some authorities are capable of perpetuating, stressing the underlying power dynamics. This highlights not only the asymmetries in both participation and knowledge but also the widening gap between the privileged and the impoverished. As discussed in Section 2.1, some are superior to others, some decide, others follow, some possess, others do not. In general, the Internet, along with the ubiquitous connection and tremendous data provision to the capitalists of today’s digital world, exemplifies the necessity to study and discuss the actual beneficiaries and impacts of technologies. By examining these aspects and effects, the fundamental characteristic of technologies can once again be highlighted: the inherent nature of technologies is neither good nor bad; its value depends on what they are being used for. In addition, the often-hidden power dynamics technologies entail are pushed and facilitated by their human masters, whose interests and values can vary vastly. These power dynamics can ultimately facilitate *creative destruction* and lead to the reorganization of capitalistic dynamics to different extents.

2.3 Data Extraction Imperative

> *"Again and again, a ruling class arises that controls the surplus over bare necessity and enforces new necessities on those peoples who produce this very means of escaping necessity."* – *Wark 2004: [010]*

In the evolving digital age, creative destruction and its inherent drive to restructure capitalistic dynamics have also resulted in significant shifts in both societal structures and dynamics within the evolving digital age. The three aforementioned major characteristics (networking, decentralization, control) along with the emergence of post-industrial societies, the Internet, and other newly developed technologies, have given rise to a multitude of possibilities and challenges for societies and economies. Steadily, the dependency on the Internet, digital communications, and digital infrastructures increased. From a capitalistic viewpoint, these newly discovered paths for potential economic growth were necessary because of the previously described economic downtrend. Since then, capitalism has entered a new sequence in its own history. Capitalism has shifted its focus to a newly discovered resource (Zuboff 2019) centered on the idea of collecting and analyzing information about customers and their consumer habits, even „after a product was sold." (Deguchi et al. 2020: 18) „With a long decline in manufacturing profitability, capitalism has turned to data as one way to maintain economic growth." (Srnicek 2017: 6) It was innovation, automation, algorithmic decision-making, technological development, and a certain degree of necessity facilitated by the dot-com bust that let emerge a whole new market (Zuboff 2019). During the dot-com boom and bust in the 1990s, the Internet, digital technologies, and platforms gained massive attention, causing many businesses to build their entire business models upon data collection (Srnicek 2017: 36). A major historical turning point represents the significant shift from industrial capitalism to digital capitalism. The restructured industrial capitalism, now digital capitalism (Schiller 2000; Srnicek & Williams 2015; Staab 2021), subsequently reshaped labor, production, information-sharing processes, and ultimately the economy. Over time, this not only facilitated the emergence of new markets and technology companies, which subsequently allowed economies to thrive again, but also paved the way for more specific forms of capitalism, which are: Platform Capitalism (Srnicek 2017) and Surveillance Capitalism (Zuboff 2019). The former, according to Srnicek (2017), refers to a new form of capitalism where digital platforms of today's world, such as Google, Facebook, and Amazon, act as intermediaries and monetize the infrastructure in which users interact and use their services. According to Zuboff (2019), the latter refers to another form of capitalism that revolves around the extensive extraction of users data by big tech companies, such as Google or Facebook, often without explicit consent and for corporate control and profit. Whether it is the old industrial capitalism or the novel forms of such in the modern world, what continues to be similar are the social relations within: for instance, some are superior to others; some possess more knowledge and power than others; some own and others do not; intensified working conditions; precarious circumstances and global exploitation; and the accumulation of wealth as an imperative. Thus, capitalistic constraints, private property in particular, continue to perpetuate social disparities and economic inequalities with one additional aspect: capitalism has further pushed into the private sector, moving beyond the traditional work within factories to now operate within individuals' leisure time, infiltrating into their homes, into their personal devices, and into almost every corner of life where interaction and time spending occur. This has opened up new opportunities and entire markets.

Some companies back then recognized the opportunities and started the race to harvest the digital resources in increasingly rapid and extensive ways. With the help of some emerging technologies, such as Big Data, AI, and IoT, the tech sector grew further and began to dominate the economy. It has been since the aggressive data accumulation processes of *Big Tech* that enabled capitalism to expand exponentially. Within this context, the word *Big Tech* describes a „watchword for corporate surveillance, monopoly, and market power" and „is usually associated with major companies like Amazon, Apple, Google, Alphabet, Microsoft and Facebook/Meta" (Birch & Bronson 2022: 1). These companies build their entire businesses around the accumulation and distribution of data, driven by the „extraction imperative“ (Zuboff 2019). *Big Tech's* main goal is to monetize user attention. In doing so, their algorithms detect and collect as much data as possible to prepare the best datasets, often for sale to third parties and advertisers. These datasets represent highly predictive consumer habits, meaning that the more data a firm accumulates, the more specific and individualized the service, product, or ad becomes, guaranteeing tailored „solutions to meet consumer's preferences“ (Quach et al. 2022: 1314). Tailored solutions enable companies to „offer the right product, right value at the right touchpoint to the end-user [using the] right approach," as the head of product marketing in an electronics firm stated (ibid.). This strategy not only increases companies' profitability but also enhances their performance, subsequently raising awareness, allowing speculative assumptions about future potentials and revenues, and attracting additional capital from investors, which eventually adds up to a higher valuation of the company itself, as well as increasing market power. Currently, the most valuable companies worldwide are valued for their data. The datasets these companies own are derived from particular practices and situations of human interactions, and over time, they have been incrementally transformed from the physical into the digital realm through the application of capitalism's means of digitalization, guided by its inherent urge to reinvent itself. Particular companies have been working on transitioning from physical infrastructures and practices into digital versions, allowing them to extract and control data with greater ease. "Their sheer scale" of the five Big Tech companies which now represent around 25 percent of the US & S&P 500 by market capitalization "(…) is often used to explain their dominance." (Birch & Bronson 2021: 3) Big Tech's success in transitioning from physical into digital infrastructures and in gaining market dominance is facilitated by network-effects, winner-takes-all dynamics, and financial leverage, eventually leading to monopolization as a consequence of their claimed scale (ibid.). For example, Google has transformed the physical bookstore and traditional library into a digital version, Facebook has transformed friendships into digital connections, Amazon has transformed the traditional store into a massive online store, etc. Notably, these companies were the most successful in doing so, thereby maintaining status and dominance and consequently exhibiting monopolistic characteristics.

The most valuable data are derived from social interactions and consumer habits throughout Big Tech's vast online infrastructures. Whether it is liking, ranking, commenting, watching, saving, buying, or consuming content on the Internet: every interaction is monitored, users are constantly monitored and increasingly exploited, social interactions are digitized and often manipulated, and consumer behaviors are analyzed and monetized. In this data-driven economy, sociality is transformed into bits and further quantified (Mau 2019) to be monetized. It seems that the economic benefits far exceeded the social benefits. People outside of the digital are nudged into Big Tech's *proprietary markets* (Staab 2021), through clever marketing and by providing promising self-enhancing or addictive products and apps for *free*, all centered around the extraction and accumulation of behavioral data (see Ochs et al. 2021). One company that successfully developed and implemented such a strategy is Google. In the early 2000s, Google began to monitor users' actions, while using its search-service, and then further sold the distilled information of users' search behavior to third parties. Additional data, apart from information about the original search request, is referred to as *behavioral surplus* (Zuboff 2019). The importance and economic possibilities of this newly discovered "resource" became obvious when „the discovery of behavioral surplus had produced a stunning 3,590 percent increase in revenue (Google) in less than four years." (Zuboff 2019: 87) Behavioral surplus, from then on, became the core asset of today's modern markets. Whether it is the amount of time spent watching a video, the pace used when scrolling through an app, the reaction time when clicking on a link after receiving an ad, or the patterns of switching between apps, everything is being monitored and user interaction data systematically extracted. All these interactions are dependent on one specific infrastructure – the platform. A platform is a „place" in the digital where consumers and product owners meet, where producers provide their products and services to the users, and the platform acts as an intermediary between different groups of actors. It is a place where social interactions take place and where platform owners monitor and govern everything in a centralized manner, typically with limited transparency. Additionally, the platform represents the aforementioned "necessary invention" capitalism had to come up with during its own reinvention. As a result, this reinvented capitalism – *Platform Capitalism* according to Srnicek (2017) – disrupts societal structures, diminishes old forces, constraints, and dynamics while creating new ones, revolutionizes both the *instruments of production* (Marx) and the *relations of society* (Marx & Engels 1848), facilitates the evolvement of new infrastructures, and develops novel ways of maximizing profits and accumulating wealth to ensure economic growth (again).

2.4 Platforms – The new Infrastructures of Society

In the beginnings of the 21st century, „The platform has emerged as a new business model, capable of extracting and controlling immense amounts of data, and with this shift we have seen the rise of large monopolistic firms.“ (Srnicek 2017: 6). In this specific era of platforms (Srnicek 2017: 92), in which surveillance and the extraction of data from everyone, everywhere, from everything, at almost every time is at its core, a new class emerges and dominates the economy. Srnicek (2017) writes: “On the other side of the class relation, some argue that the economy today is dominated by a new class, which does not own the means of production but rather has ownership over information.” (38) Srnicek (2017) thereby refers to Wark’s (2004) *A Hacker Manifesto,* which critically discusses the impacts of the commodification of information and intellectual property on society, ruled by a new class.

According to Srnicek (2017), today’s owners of information are predominantly platform owners. However, they are not merely owners of information; rather, „(…) these companies are becoming owners of the infrastructure of society.“ (ibid. 92) It is their „prominence over manufacturing, logistics, and design, by providing the basic landscape upon which the rest of the industry operates,” enabling them to emerge as the means to lead and control industries (ibid. 92). As platforms expand their operations into almost every sector and branch while purchasing other companies to stock up their capacities, they are establishing vast proprietary markets (Staab 2021), whereby they have full control over everything happening within. These proprietary markets provide activities, services, and experiences to their customers in a convenient and joyful way so that customers do not perceive themselves as lacking something or feel the urge to switch to a competitor. Platform owners incentivize other companies to build their applications on their infrastructure, which ultimately means more activities for users, hence more data, and more possibilities to generate profit. Furthermore, what makes them impactful and powerful is their digital nature, which enables them to operate in any digital environment where interaction occurs (Srnicek 2017: 44). However, the essential function platforms perform is the mediation between actors. A platform positions itself between different users while providing the infrastructure for all their interactions and activities to occur, thereby affording itself the capacity to record and monitor all interactions. Despite this, platform owners maintain complete authority over the mechanisms of interaction, product and service development, data access, and sharing processes, as they set the rules for this infrastructure (ibid. 47). Platform ownership can be understood as the „ownership of software (the 2 billion lines of code for Google, or the 20 million lines of code for Facebook) and hardware (servers, data centres, smartphones, etc.) built on open-source material.“ (Srnicek 2017: 48)

In sum, platforms are a new type of firm with their key business model built upon the extraction and control of data. With the power and concentration of ownership, it becomes evident that platforms have a tendency towards monopolization (Srnicek 2017: 45). Furthermore, due to the single point of failure and due to humans’ greed and strive for (more) power, the concentration of ownership becomes a threat to societies. In the context of this thesis, centralized ownership enables platform owners to have full control and power over data, implying severe effects for societies, such as power imbalances, privacy concerns, a lack of transparency, manipulation, or corruption. As history has shown, according to Marx (1973), private ownership has been „the“ problem which facilitated exploitation and allowed capitalism to thrive. Whether it was the industrialists who owned the means of production during the 19th and early 20th century or the capitalists during the late 20th and early 21st century who had gained ownership over information – it has always been the class struggle between collective capital and collective labor (Marx 1887: 164), between the class of capitalists and the working class, between those who own and those who do not own (Marx 1973).

Based on this theoretical background, one could ask whether there is even a chance for societies to escape the ever-reinventing capitalistic constraints. What can digital societies do to break out of platforms’ rules of economy? What is needed to *regulate* the extensive accumulation and capitalization of sensitive personal data? How can imbalances in power and control over data, private property issues, platformization and monopolization, or asymmetries in both accessing and sharing information be tackled

2.5 The Regulation of Data Ownership through technological Means

„If we want to prevent the concentration of wealth and power in the hands of a small elite, the key is to regulate the ownership of data.“ – Harari 2019: 93

According to Harari (2019), and based on the previously described challenges in today's world, if digital societies like ours eventually seek to challenge digital capitalism, flatten imbalances in power over data, or break up existing capitalistic structures or centralized dynamics, the focus, apparently, needs to be on the notion of data ownership. By building a human-centered *system, network, or community* in which individuals are not only at the core but also in full control over their own data (data sovereignty), the power over data can eventually be returned to the users. In other words, shifting from a centralized system (platform) – where power, knowledge, and data are concentrated – to a more democratic one – where fewer asymmetries in data accessing and sharing exist – enables users to have full control, thereby allowing them to determine how their data is curated, processed, and shared in the digital (Tapscott & Tapscott 2016). This vision appears straightforward and libertarian. Nevertheless, it is crucial to engage in discussions of this nature in contemporary society. This necessity arises from the fact that the debate about digital data and its ownership has only gained prominence in the last few decades. Consequently, societies are still in the early stages of these developments, relative to the decades ahead, in which digital technologies and data will increasingly shape future societies. Through critical discussions and appropriate analytical means, societies can gain a deeper understanding of the implications of these developments. Research, analysis, and thought-provoking discourse, among other methods, can facilitate this and allow for more accurate assessments of the impacts emerging technologies and innovations have and potentially may have on societies (Askarany 2016; Teng et al. 2022). Therefore, a central argument of this thesis posits the inevitability of engaging in discussions about blockchain technology and its promise to offer alternatives to the centralized organizations, mechanisms, and dynamics that have evolved over recent decades – dominant paradigms that society has apparently accepted largely. Thus, it is critical to have such conversations sooner rather than later.

The concept and idea of a democratic, decentralized system in which users own their data could offer a viable alternative to platforms' centralized systems. The following chapter investigates this thoroughly, particularly the extent to which the following core characteristics of platforms can be challenged: concentration, centralization, and control of information. In addition, this thesis further examines whether this approach can address the asymmetries and imbalances in access, power, control, and ownership of information inherent in the business models of today's Big Tech companies. As described in Chapter 2, these companies nudge people into their proprietary markets, extract information from interactions, and then sell highly predictive user habits to third parties for tremendous economic profits, all without the user's consent or compensation. The imaginary of a democratic, decentralized network of participants who collectively operate and ensure security as a network while advocating for data sovereignty and leveraging their verifiably owned digital identity could potentially facilitate a shift within our digital landscapes. This shift could be enabled by building and enhancing the lacking layer of the Internet (Chapter 4) for digital ownership and digital identity purposes through the application of appropriate technology, which will be explored in Chapter 3 (Blockchain Technology). This also underscores the rationale for this thesis. The objective is to examine whether blockchain technology can serve as a means to address these issues.

This research explores these topics through an STS lens, aiming to provide answers to the guiding research question introduced in Chapter 5. Throughout the thesis, the researcher focuses on addressing specific questions regarding the challenges and problems described in Chapter 2 and Chapter 3 and on providing an overview of blockchain's potential role, particularly regarding data ownership, digital identity, and shifting power dynamics. Due to blockchain's relatively nascent development status (Ragnedda & Destefanis 2020; Voshmgir 2020; Tapscott & Tapscott 2017; Yli-Huumo 2016) and the lack of literature regarding its societal impacts in particular, an additional objective of this research is to fill this gap and provide answers about the technology's potential role in challenging prevailing capitalistic constraints and platform's "rules of the game."

The potential for a paradigm shift in digital data ownership and control warrants further investigation. This study aims to examine the feasibility of transitioning from centralized data infrastructures to decentralized systems that empower individual users. The key questions include the following: What technological and societal factors are needed to facilitate this shift? How can such a system be structured and implemented? What are the potential implications for individuals and society?

The answers to these questions are explored in the following chapters. This chapter now delves into the various promises associated with blockchain technology and provides a brief overview of its current perception in academia. This will help us to get a first glimpse of the various possible implications and potentialities of blockchain technology. Subsequently, the thesis discusses blockchain's potential role in digital identity and data ownership purposes (Chapter 7).

For instance, Dublon & Paradiso (2014) suggest that „the law could give a person ownership or control of data generated in his or her vicinity; a person could then choose to encrypt or restrict those data from entering the network.“ (see Zuboff 2019: 223) Technology, specifically certain rules that can be programmed into code resembling the law (De Filippi & Wright 2018), could thereby serve as a means to facilitate this shift and the regulation of data ownership. With the rise of blockchain technology and smart contracts in combination with enhanced AI systems, novel concepts of data ownership arise, whereby societies may enter an era in which new forms of power and control over data and privacy emerge and where the kind of trust changes (e.g. De Filippi et al. 2020; Freeman et al. 2020; Ragnedda & Detefanis 2020; Jasanoff 2016). Some literature argue that blockchain technology facilitates the creation of a new architecture of trust (Alston et al. 2021: 2; Werbach 2018), while others contend that blockchain will become „the most important and most revolutionary digital innovation since the inception of the internet“ (Tapscott & Tapscott 2016: 225; see also: Zheng et al. 2018). Tapscott & Tapscott (2017) recognize blockchain's potentials in upending business models and disrupting industries, and argue that it is „pushing us to challenge how we have structured society“ (5). Is this shift and development in reorganizing society „people have been waiting for since the internet came," as Sandstrom (2017: 6) states? Additionally, could this technology be an appropriate tool to create more flexible and fairer spaces of interaction with less centralized authorities, representing „(...) the promise that many early Internet visionaries hope[d] for," as Wright & De Filippi (2015: 19) state? Furthermore, as blockchain is often associated with the revolution of both organizational hierarchies and labor, as well as with the possibilities of giving back power and freedom in terms of data sovereignty to the people, we may ask whether blockchain could represent an approach for tackling one of the biggest indictments of capitalism, which is „(...) that it enables the freedom to act for only a vanishingly small few“? (Srnicek & Williams 2015: 79)

The goal of this thesis is to find answers to these questions and beyond. The following chapter will elaborate on the characteristics of blockchain technology, what the democratization of information means, how this could be done in practice, and whether blockchain could represent a solution in regulating ownership, despite particular prejudices and criticism.

3 Blockchain Technology

"We demonstrated that the Web had failed instead of served humanity, as it was supposed to have done, and failed in many places. The increasing centralization of the Web ended up producing – with no deliberate action of the people who designed the platform – a large-scale emergent phenomenon which is anti-human." – Tim Berners-Lee (Brooker 2018, Vanity Fair)

The following chapter elaborates on the main characteristics of blockchain and the role that this emerging technology might play in one of the most pressing topics digital societies like ours face today when it comes to digital ownership. In examining blockchain's potential, this chapter aims to shed light on how societies can use this technology to redefine the understanding of owning and controlling digital identities, assets, and data.

3.1 What is Blockchain Technology?

Blockchain is a complex technology based on cryptographic and highly mathematical computations, of which network participants make use to validate, process, and store transactions on the network. Because explaining its entire technological process would far exceed the scope and purpose of this thesis, the following will use simplified terms and explanations.

3.1.1 Characteristics & Design

Despite the various explanations and interpretations found in the literature, Treiblmaier (2018) succinctly captures the fundamentals and describes blockchain as "a digital, decentralized and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamper-proof records." (547)

Blockchain is a relatively new technology that has gained significant attention owing to its much-discussed application of cryptocurrencies. The interest was particularly sparked by Bitcoin, the first decentralized cryptocurrency made available to the public as open-source software in 2009 (Nakamoto 2009). It is important to note that the underlying technologies that made the creation of Bitcoin possible have existed for at least 10 years prior (Pisa & Juden 2017: 6). Public key encryption invented by Diffie & Hellman (1976), digital time stamping (Haber & Stornetta 1991), and hashcash proof of work (Back 2002) represent some of the core technologies that existed before the invention of Bitcoin. However, these were combined later by Satoshi Nakamoto, the pseudonymous inventor(s) of Bitcoin, with an additional feature of incentivizing participants via a protocol (Pisa & Juden 2017: 6). Additionally, the true power of blockchain is based on the interaction of three core elements: distributed ledger, consensus protocol, and novel data structures (7). Because of the complexity of their fundamental functioning, these elements are described briefly in the following chapter.

A ledger, in this context, refers to a computer file representing a book basically that stores all the information about transactions, time-stamped in chronological order. Common traditional computer services run on centralized networks and store and control the flow of information through a central hub or server, distributing the information to other computers called "clients" (ibid.). Blockchain systems run on peer-to-peer (P2P) networks in which all computers (nodes) function as a network, distributing and receiving information as a client and simultaneously as a server, thereby avoiding a single point of failure (Fig. 1).

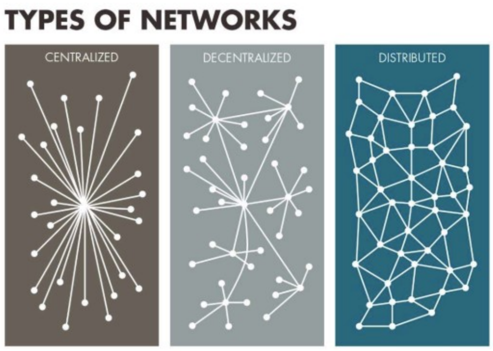

Figure 1: Types of Networks (Pisa & Juden 2017: 7)

Every time a transaction is verified by the network participants (nodes), which occurs by agreeing upon several criteria – called *consensus mechanism* – the transaction is stored cryptographically on the ledger (Voshmgir 2020: 39). Subsequent to the process of reaching consensus, the chronologically ordered transactions are grouped into blocks, linked with the previous block of transactions via a string of random numbers and letters (called *hash*), thereby building an irreversible chain of blocks, ensuring that it is secured from tampering and revision. Ultimately, every computer (node) receives the latest version from the node that finds the hash through the complex and highly mathematical computation processes required for linking the blocks. The ledger is updated on each participant's node, waiting for the next transaction to be verified and stored on the blockchain forever (Fig. 2). This process of verifying transactions, storing, and then adding transactions as a block to the chain is referred to as the *consensus mechanism* known as *proof of work,* which is used by the Bitcoin network in particular.

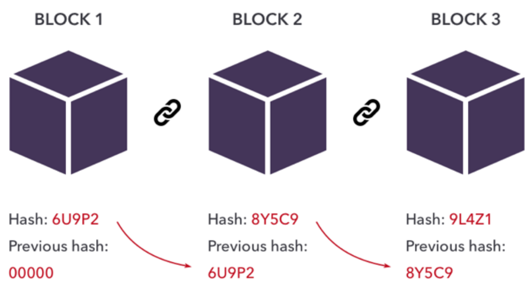

Figure 2: The Structure of Blockchain (ig.com, accessed 2nd August 2024)

As blockchains evolve, their original purpose (referring to the Bitcoin blockchain) of merely storing information about transactions also evolves. This includes Ethereum (more in Section 4.3) which "provides a built-in programming language and an open-ended platform that allows users to create decentralized applications (known as *dapps*) of unlimited variety. In other words, Ethereum is a programmable blockchain, which is why it is often referred to as the world's first distributed computer (…)" (Pisa & Juden 2017: 11). It allows users to place self-executing scripts, called *smart contracts* (more in Section 4.3), on a blockchain (12). This highlights the various mechanisms, applications, and states of blockchains, implying that in the future different blockchains might exist, each serving different solutions to different problems.

Since 2009 the discussion about whether blockchain technology – the underpinning technology of all cryptocurrencies – is beneficial for societies or not, has been controversial and has sparked diverse perspectives among stakeholders. Some compare it with a hype (Pisa

& Juden 2017), some highlight the considerable risks of scams within the crypto Bubble (Chergarova et al. 2022), while others label crypto in general as a “Giant Ponzi Scheme” (Mortazavi 2021). An expert interviewed within the study conducted by Treiblmaier & Umlauff (2019) stated that “Blockchain is just part of the digitalization process (…)” and that “it is an evolution, not a revolution” (14). Conversely, proponents argue that cryptocurrencies are beneficial, as they facilitate disruption of the financial sector (Larios-Hernández 2017; Peters & Panayi 2015), therefore potentially posing an alternative to traditional banking and FIAT systems (Georgeson 2018). While some call it a “blueprint for a new economy” (Swan 2015), others truly consider blockchain technology and its characteristics itself as revolutionary and disrupting (Tapscott & Tapscott 2016) and also one of the most significant technologies ever invented by humanity (markmetry.medium.com, accessed August 2nd). What makes blockchain so revolutionary, which challenges might this technology address, and what is the current state of academic research in this field?

3.1.2 Current State of Research

To better illustrate the current development, research, and adoption status of blockchain technology and its applications, the following section presents various charts for visual representation. Over the last few years, blockchain technology and its application have gained considerable attention in the academic literature. Most existing literature and studies focus on the finance industry (Janssen et al. 2020). Rigorous and theory-based academic research in this field, however, is still lacking (Treiblmaier & Umlauff 2019: 20). The literature expects blockchain’s impact on society and the economy to be huge, even though the technology is still in its early adoption phase across industries (Osborne & Laing 2021) and still in its infancy in leading academic journals (Treiblmaier 2019), with its true future potential just starting to be explored (Rozas et al. 2021).

Before the significant increase in interest and number of publications on blockchain technology, the main focus was on the financial aspect and potential implications for the finance industry. However, over time the interest shifted to other sectors, such as supply chain management (SCM). As illustrated in Fig. 3, since the invention of Bitcoin in 2008 until around 2017, no relevant articles were published regarding SCM (Duan et al. 2023). However, since 2017, the number of articles focusing on further applications, such as smart contracts within supply chain management, has been increasing exponentially (e.g. Ying et al., 2022; Asokan et al., 2022).

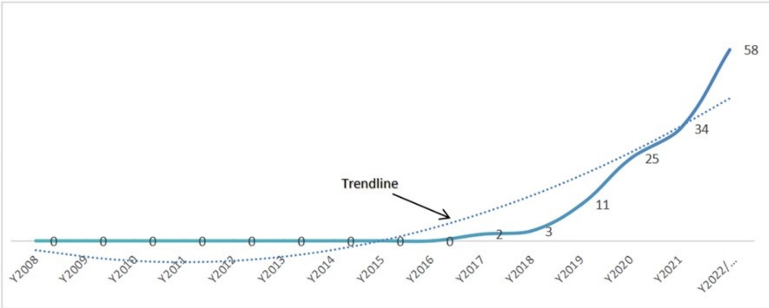

Figure 3:Publications of Blockchain Technology in Supply Chain Management (Duan et al. 2023)

In addition to its applications in supply chain management and despite its current limitations and uncertainties, blockchain tends to hold promises for transformative shifts across various sectors (e.g. Tapscott & Tapscott 2016). Therefore, research in particular ought to further elucidate its potential benefits and address challenges thoroughly. Similar to other innovations, it takes time to fully identify and understand the societal benefits and risks. The temporal aspect is crucial because it allows potential adopters to assess the characteristics of innovation, including relative advantage, compatibility with existing systems, and complexity, representing key factors that influence the adoption process (Teng et al. 2022). For instance, the Internet nowadays unquestionably represents a core part of our lives. However, prior to its exponential adoption from the 2000s onwards, it took societies several years to identify use cases and applications enabled by this new type of infrastructure and to gain a more comprehensive understanding of its implications. One of the advantages of the Internet is its capacity to connect people from all over the world. However, as previously discussed in Section 2.1, technology can be used in either way: for the "good" or for the "bad." A notable example is the emergence of surveillance capitalists (Zuboff 2019) who recognize the power and true value hidden beneath the surface of the Internet infrastructure. The surveillance capitalists made use of data insights in extensive ways, which enabled them to establish some of the most valuable companies in human history, all of which built upon exploitation and monetization of the resource gathered from connected people. Whether these data-extracting and application-providing companies (Big Tech) are actually beneficial or harmful remains a subject for another discussion.

Compared to the adoption phases of the Internet, blockchain technology is still in a very early stage of adoption (Osborne & Laing 2019). Woodside et al. (2017) state in their study's conclusion that blockchain is within the innovation stage in terms of its application in multinational enterprises, though it could see "growing normalization and acceptance, and at an inflection point akin to the Internet of the 1990s." (Woodside et al. 2017) Unfortunately, no chart or numbers are found in the literature that illustrate this comparison between the adoption of blockchain technology and that of the Internet. It is crucial to recognize that a comparison between blockchain as a technology and the Internet as a technology would obviously be far more meaningful than comparing only the adoption of cryptocurrencies with that of the Internet. This is because cryptocurrencies represent just one of many applications of blockchain technology, just as there are many different applications built upon and leveraging the Internet layer. Therefore, a holistic comparison of the two technologies, including their applications, would allow for more direct comparisons and more insightful conclusions. For illustration purposes though, and to better grasp the adoption stages and the growing interest in cryptocurrencies – the first application of blockchain technology – the following figure shows the adoption of cryptocurrencies in comparison to the adoption phase of the Internet. These two have been compared for a while, and as shown in Fig. 4, a captivating trend can be observed:

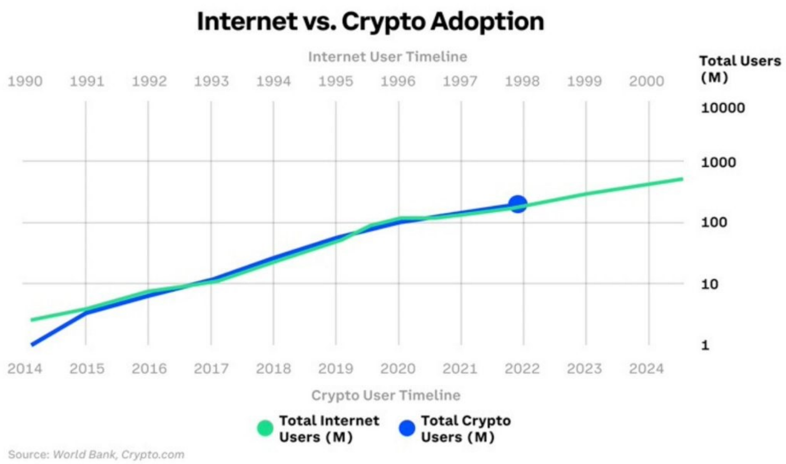

Figure 4: Comparison of Internet and Cryptocurrency Adoption from 2014- 2024 (Wan 2021)

The Internet has gained since its implementation in the 1990s up until today about 5.5 billion users, "onboarding" 67% of the world's population in just 34 years. Fig. 4 illustrates that over a time span of 14 years, cryptocurrency adoption by users follows a trend similar to the adoption of the Internet. From January 2023 to December 2023, the worldwide number of cryptocurrency owners grew from 432 million to 580 million (crypto.com, accessed 18th June 2024), which represents today approximately 6.8% of the world population (triple-a.io, accessed 1st August 2024). Notably, as illustrated in Fig. 5, the growth in ownership of cryptocurrencies – which is about a 99% compound annual growth rate (CAGR) – has already exceeded the growth rates of traditional payment methods – approximately 8% CAGR – from 2018 to 2023 and has surpassed payment giants such as American Express or PayPal (triple-a.io, accessed 1st August 2024).

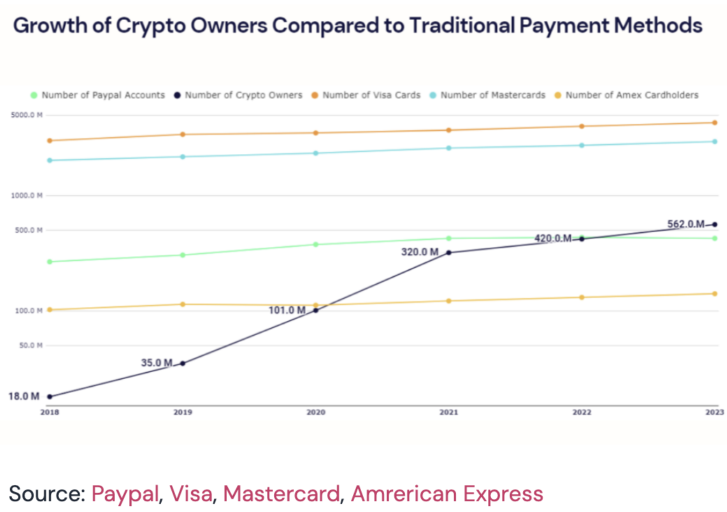

Figure 5: Growth of Crypto Owners Compared to Traditional Payment Methods (triple-a.io, accessed 1st August 2024)

To better picture where societies currently stand in terms of cryptocurrency adoption, we can adapt the 6.8% of global users that own cryptocurrencies to Roger's "Diffusion of Innovation Theory" (1962), illustrated by the bell curve shown in Fig. 6. The bell curve, in general, aims to illustrate that the full adoption by the masses of an innovation within a social system happens in consecutive stages rather than simultaneously. Adoption of an innovation is conceptualized as a process in which certain individuals show greater propensity to adopt this kind of innovation compared to others (Rogers 2003). According to Roger's bell curve, cryptocurrency adoption is somewhere in or between the “innovators” and “early adopters” stage, with an expected global owner rate of reaching 1 billion within the next 5 to 10 years (e.g. cointelegraph.com, accessed 10th June 2024; nasdaq.com, accessed 10th July 2024), assuming cryptocurrencies are eventually fully adopted by the masses.

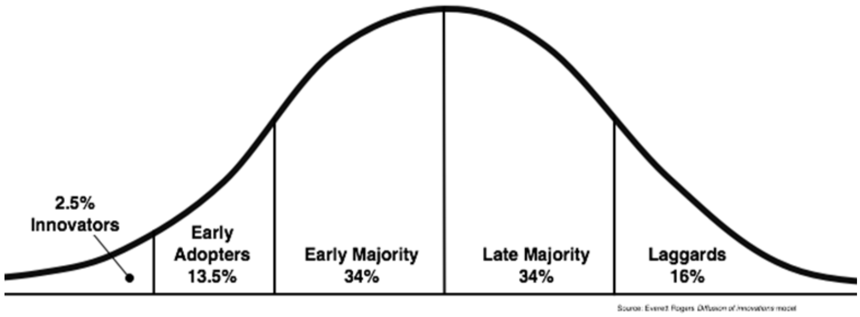

Figure 6: Innovation Adoption Curve (sphweb.bumc.bu.edu, accessed 1st August 2024)

Despite these developments and numbers, there remains a “substantial time lag” of blockchain-related publications in leading academic journals in comparison to industry adoption, according to Treiblmaier (2019:1). The is primarily attributed to the technology’s complexity along with “poorly understood and unclear use cases.” (2) However, this is changing because publications that target a broader audience beyond just the finance sector and cryptocurrencies are emerging. The authors speculate about potential future applications (ibid.) that are based on blockchains characteristics (7) and discuss use cases that cover a wide range of industries and topics (Treiblmaier 2019; Treiblmaier and Beck 2019a,b; Tapscott & Tapscott 2016; Wright & De Filippi 2015; Yli-Huumo et al. 2016). These include transportation and supply chain management (Bahga & Madisetti 2017; Treiblmaier & Beck 2019a,b), banking (Dai & Vasarhelyi 2017), traceability (Dieterich et al. 2023), media and entertainment (Prathi 2022), education (Mougayar 2016), tourism (Önder & Treiblmaier 2018), agriculture (Manski 2017), public and consumer services and the IoT (Schlatt et al. 2016), governance (Morabito 2017), work (Teiblmaier & Umlauff 2019), art (McConaghy et al. 2017), voting (Fuso et al. 2018), smart contracts (Schlatt et al. 2016), ICO and crowdfunding (Manski 2017), gaming (Treiblmaier & Zeinzinger 2018), energy market and sustainability (Strücker et al. 2019; Veith 2023), identity management (Liu et al 2017), decentralized privacy (Zyskind et al. 2015), ownership (McConaghy et al. 2017), and digital identity (Careja & Tapus 2023).

Therefore, similar to the Internet's trajectory, there is still a long way to go for blockchain-based applications to be explored and eventually adopted by the masses. Osborne & Laing (2021) state that „the truly important question is what value the technology can create in the longer term, and that, at present, is unquantifiable" (Osborne & Laing 2021: 231). As a result, the majority of future use cases, such as data ownership, still need to be studied and determined.

3.2 The Traditional Internet and (trusted) Intermediation

"The 24/7 internet connection means we're never really free and we always feel behind. The Internet also continually entices us to explore its options through hyperlinks and ads so we can spend a lot of time on things for which we have little to show, adding to our unrest." – Tricia Rhodes (biblegateway.com, accessed 1st August)

The following will outline some of the issues and problems that have arisen with the evolving Internet since the 1990s. Such an elaboration is necessary in the context of this thesis, as it will help to better grasp the role of technological developments, innovations, and shifting societal narratives in addressing particular problems caused by the Internet. Furthermore, this understanding may contribute to the development of an Internet layer that serves human needs and desires, rather than the opposite scenario, in which humans merely serve Big Tech' needs and desires. Consequently, two approaches will be elaborated, highlighting not only the problems that emerged over the last three decades but also providing fundamental arguments for leveraging new technological applications, such as blockchain, for addressing problems as such. From one perspective, there is the technological aspect that warrants investigation, revealing a crucial deficiency in the traditional Internet infrastructure. From another perspective, there is the societal aspect, which focuses on one of the most fundamental elements of human life: trust. Specifically, this revolves around trust in social media platforms and other centralized entities that tend to decline. However, the notion of trust might be redefined or even replaced by the creation of a *trustless* system enabled by technology. Therefore, it is worth discussing the characteristics of blockchain and its role in both serving as a viable solution for building and redefining trust among the Internet participants as well as for mitigating the limitations of the traditional Internet.

3.2.1 The Evolution of the World Wide Web and its missing Layer

First, in examining and in order to identify the potential role of blockchain applications in the future, the following elaborates on the Internet's technological properties and fundamentals. This approach, focusing on a technological perspective, will unfold the core deficiency of the traditional Internet that blockchain advocates aim to address.

In 1962, a novel information-sharing technology was believed to evolve when J.C.R. Licklider envisioned an "Intergalactic Computer Network" that would revolutionize the way of sharing information forever. The first version of this new computer network was called ARPANET and was launched in 1969, representing a new approach to a network that is resistant to single-strike attacks, which would allow sending messages in the form of packets within its decentralized architecture and network of computers (René & Mapes 2019: 19). In the 1980s, Berners-Lee was inspired by similar ideas that made him envision an advanced version of the ARPANET, which was based on the core idea of "anything being potentially connected to anything" (Berners-Lee 2000: 1). Berners-Lee envisioned a network of interconnected websites, a "global brain" (Berners-Lee 2000: 298) that facilitates inclusiveness, participation, and equal access to information among actors. This pushed a narrative, evoked around the vision of a "web as an inclusive information network without borders, hierarchies, or limits" (Mager 2010: 44). Additionally, it was the web's technical infrastructure that further facilitated the emergence of the vision of a "decentralized network of information that would enable more freedom than hierarchical classification systems ever could." (ibid.) However, this vision of a decentralized network with democratic values inscribed vanished as soon as with the emergence of firms that established themselves as sort of the "gatekeepers" that increasingly regulate the access to web information, such as Google (Diaz 2008). Firms of the early Internet in the 1990s contributed to the development of the first stage of the evolution of the Internet, called Web 1.0. Web 1.0 was basically characterized by reading and consuming content from websites (Dávila 2023; René & Mapes 2019; Voshmgir 2020).

Later, over the course of the 2000s, together with the emergence of social media, users from then on were able to create and share their content with the public through their digital profiles and accounts. This novel way of interacting in the evolving Web 2.0 era was enabled and guided by platforms, connecting producers and consumers. In this role, platforms function as intermediaries, meaning that they are in full control of how digital interactions occur. What has been missing since the rapid developments in platformization (Srnicek 2017), social media, and exponential content creation is the individual ownership of content and data. The traditional Internet layer of Web 1.0 and Web 2.0 lacks a native identity or account infrastructure (René & Mapes 2019: 87). One reasonable argument for why the early visionaries of the Internet did not build a common identity layer within its infrastructure that would allow actors to literally own the information on the web could be derived from their initial vision of the Internet, which was a decentralized network with democratic values and equal access to information, without borders, hierarchies, or limits (Berners-Lee 2000; Mager 2010; René & Mapes 2019). Therefore, there was no room for considering and promoting a concept of digital ownership, as it would have been the complete opposite of what had been envisioned. However, this changed over time as tech firms under digital capitalism established themselves as the aforementioned "gatekeepers" of information access. The lack of a common account infrastructure was taken as an advantage by modern capitalists, facilitating capitalism's reinvention centered around extensive data monetization and control. Consequently, this:

> forces users to authenticate themselves with each and every service provider to access a provider's service. It also requires users to have separate accounts for different interaction modes: browsing, communicating, sharing, buying, and so on. As a result, all of the value of the data associated with such an account is owned, controlled, and monetized by third parties. – René & Mapes 2019: 87

Furthermore, neither Web 1.0 nor Web 2.0 provides a "reliable real-time validation of users, assets, and spaces, or their identity, ownership, and permissions for various interactions and transactions." (ibid.) This deficiency sets the stage for Web 3.0. In Web 3.0, alongside the rise of augmented reality (AR) and virtual reality (VR) (René & Mapes 2019: 32), technological advancements facilitate the development of the layer lacking for identity and account management. Users are now able to verifiably own something in the digital, which has technologically not been possible before. With the advent of Web 3.0 and its core technology, blockchain, the notion of owning something digitally is undergoing a profound redefinition.

The core distinction between traditional Internet applications in Web 1.0 and Web 2.0, and blockchain applications in Web 3.0, lies in the fundamental way of functioning. In both Web 1.0 and Web 2.0, the Internet primarily functions as a platform for sharing digital information, referring to firms such as Google or Facebook. Whereas in the evolving Web 3.0 space, the platform is built upon blockchain technology, primarily functioning as a platform for sharing digital value. Moreover, the ways in which the backend and frontend function marks another crucial distinction. A traditional application in Web 2.0 consists of a backend that functions through code and a frontend that users interact with when engaging with the application (Dávila 2023: 82). In practice, this means, for instance that Facebook's frontend is what users interact with, such as news feeds, personal profiles, and friends' profiles. The backend is entirely controlled and owned by the firm. Platforms like Facebook own vast databases, including all the data from users that the frontend retrieves information from to subsequently display to users in the form of news feeds, profiles, etc. In contrast, in a decentralized application (dapp), the blockchain functions as the backend, meaning that not a centralized platform (Facebook) is in control of the data, but rather everyone who is interacting with the blockchain is allowed to take advantage of the data stored with it. This capability is partially enabled by the *permissionless* nature of blockchain, which allows anyone to build and create frontend applications or implement *smart contracts* (4.3). Depending on how the dapp or smart contract is designed, user interactions do not rely on any centralized firm to be processed (ibid.), nor do users have to trust each other or the firm, thereby promoting a *trustless* system (see Sections 4.2.2; 4.3 and Chapter 7).

The concept of a trustless system sounds quite unthinkable. This is because in the physical world, a "verifiable and trusted identity is crucial when it comes to enabling transactions, interactions, and transportation between people, places, or things" (René & Mapes 2019: 137). "An identity (…)" René & Mapes (2019) state "(…) is a social tool, one that fundamentally relies on trust in the system and method used to establish and verify the identity." (135) However, the ways in which we identify ourselves along with the methods used have changed over time (135), primarily due to developments associated with the Fourth Industrial Revolution. As more of the physical world gets digitized (Mau 2019) and the number of digital interactions increases, the processes of self-identification have undergone significant changes. Consequently, the digital representation of one's personal identity has become an increasingly essential part of human life. However, in the absence of an identity layer, the ownership of a digital identity subsequent to user registration and acceptance of the firm's terms and conditions implies that a third party is in control of this account; thus, the digital identity. This dependence on centralized firms and entities for identity management presents manifold risks, such as (digital) identity theft, data breaches, or censorship (identity.com, accessed 20th May 2024). In Web 2.0, companies such as Facebook manage user's identity, by placing themselves in the driver's seat. These companies, therefore, have the authority to decide whether to seize the account, delete personal pictures or content if not aligned with the firm's rules, stop particular interactions and communication, or store, curate, and sell the data generated with this particular digital identity (Voshmgir 2020: 286). Additionally, data privacy and control represent issues particularly inherent in Web 2.0-based social media platforms. These firms' goal is to own the market rather than to compete within it (Dávila 2023: 111), and seek to extend their proprietary markets (Staab 2021). In this role, personal information and user behavior, such as buying habits, content preferences, sexual orientation, race, gender, political views, and amount of time spent on scrolling, are monitored and stored on the centralized servers of those companies, which further serve as the basis for advertising (Voshmgir 2020: 286). The power asymmetries in this constellation are obvious: users depend on the platform, trusting its authority to control profiles and adhering to its rules in order to use its services. Users, thereby, continuously send requests (technologically), for example, to like a specific posting, while the platform – owning all the information and profiles of the requesting users – decides whether to permit this action. Technology, blockchain in particular, entails the potential to mitigate these asymmetries by shifting the power over data from intermediaries such as Big Tech's platforms back to the people, which will be discussed in Section 4.5 (e.g. Lee 2019; René & Mapes 2019; Tapscott & Tapscott 2016; Voshmgir 2020). Eventually, blockchain technology promises to reduce information asymmetries by offering an alternative that breaks "today's increasing reliance on centralized entities that control access to information." (CVVC 2023) Serving as a tool, blockchain facilitates "transformative shifts" in how societies manage today's vast amount of information (ibid.), while excluding centralized *trusted* third parties (ibid.).

The notion of a trusted third party introduces the second aspect that blockchain advocates aim to address, thereby addressing the deficiencies and limitations of the traditional Internet (Web 1.0 and Web 2.0).

3.2.2 Trust (no) one – Intermediation and the Importance of Trust

The starting point of this second discussion is social interaction, followed by the introduction of institutions and the role of trust within. Georg Simmel (1908) argued that social order and society are not natural or simply given. This refers to the fact, as stated in Chapter 2, that societies are not static but rather in a constant process of change, meaning that societies are continuously produced and reproduced by social interactions. In his considerations concerning "How is Society possible?" (1910), Simmel refers to a process called "Wechselwirkung" (Simmel 1908: 5). This process means that individuals interact with each other and influence each other's actions simultaneously. Whenever there is social interaction, there is "Wechselwirkung" between individuals, which subsequently produces society. Therefore, society evolves everywhere, where various individuals interact (ibid.), and these social interactions mark the fabric of society. Social interactions, along with their full complexities, represent the subject matter of sociology: the social relationships of individuals with other individuals and how these relationships connect to society. According to Max Weber (1978), a defining criterion for social relationships is "that there should be at least a minimum of mutual orientation of the action of each to that of the others." (27) Moreover, the subjective meaning does not need to be the same for all the individuals involved; hence, *reciprocity* is not needed in this sense (ibid.). In the context of social relations, referring to relations between interacting individuals or groups, Znaniecki (1965) described in his book *Social Relations and Social Role*s that there are two basic kinds of interactions: cooperation and conflict (15-17). Regarding the latter, conflicts occur in many forms and extents within societies, having a "disorganizing influence (…) on social relations as organized systems (…)" (91-92). Both, but the former – cooperation – in particular, represent major topics of interest in sociological research. Moreover, human cooperation is an essential element for the functioning and very existence of human collectivity and has taken many forms – from tribes to guilds, to enterprises, to nation states, to platforms (CVVC 2023).

According to Émile Durkheim, as he notes in his book De la Division du travail social (1893/2014), there are two forms of cooperation in particular, which both have a special role in that sense that they hold society together and tie the individual to society: mechanical solidarity and organic solidarity (Durkheim 1893/2014: xvi; 135). Mechanical solidarity refers to early societies characterized by *likeness*. This means that because early societies tended to be small-scale communities, less complex, localized in villages or rural areas, and with a very limited division of labor, people in such societies felt connected because of the similar roles, values, and beliefs they had (xvi). Durkheim argued that people within such societies cooperate almost automatically or *instinctually* (68) with each other, driven by their shared *collective consciousness* (63). In contrast, organic solidarity is found in more complex, modern societies characterized by diverse and specialized roles. Hence, there are more differences between people within society, highlighting an increase in *individualism* (Giddens 1971: 77). Human cooperation within such societies arises from the internal, interdependent functioning of modern, industrial societies characterized by the interdependences of people and their interests, "(…) providing the conditions under which modern individuals could come into being." (Durkheim 1893/2014: xxviii; see also Norbert Elias 1982) In addition, even though distinct and in competition with one another, modern individuals act "in concert" (Durkheim 1893/2014: 167). Therefore, it can be argued that, although "mechanical solidarity generally bind[s] men together less strongly than organic solidarity" (Durkheim 1893/2014: 119), both forms of solidarity facilitate human cooperation and, therefore, represent essential elements for social order and holding society together.

"Although Durkheim never used the concept of trust," as Misztal stated in the paper *The Notion of Trust in Social Theory (1992)*, he emphasized on collective order, which he believed overall "to be dependent upon the stabilizing influence of common norms and values" (Misztal 1992: 8). In small communities, members share beliefs, common values, and norms; and hence, collective consciousness contributes to solidarity and social order. However, the bigger these communities become, the more complex the relationships become, leading to decreasing collective consciousness, increasing uncertainty among its members, and eventually affecting cooperation and social order. Therefore, as shared beliefs, common values, norms, and collective consciousness (mechanical solidarity) become more abstract, community members of more complex societies (organic solidarity) need to make use of other means to ensure social order. This is when societies began to represent common values and beliefs in the form of collective representations, such as symbols, flags, sentiments, and institutions (Misztal 1992: 9). Collective representations define what society's "mutual relations ought to be" (ibid.), and allow the establishment of a denser web of social relationships to cooperate, to create social solidarity, and consequently social order (Misztal 1992: 9). Social solidarity and, consequently, social order are established, reinforced, and maintained by abstract symbols, flags, sentiments, emblems, and institutions

(Misztal 1992: 9). Moreover, as Misztal (1992) noted, it is trust that ultimately preserves social order. Trust is commonly perceived as an “collective attribute” and assumed to play some “important social functions,” such as increasing group solidarity or social cohesion, and reducing complexity (Misztal 1992: 13).

Based on this elaboration, collective representations facilitate the creation of social order, and trust preserves social order, eventually facilitating trade and exchange (Pisa & Juden 2017: 5) within more complex societies and beyond. Institutions, as a form of collective representation, act as intermediaries between actors by providing the essential infrastructure that not only reduces the risks of uncertainty but also enables trade and exchange between those parties without the need to have them to trust each other. Traditional trusted third parties, such as governments, centralized legislative and judiciary systems, banks, and other centralized organizations, are needed for the specific processes that organize society (Wright & De Filippi 2015). However, this also highlights the strong dependencies and hierarchal power dynamics. This can be observed with the modern forms of institutions in the context of platforms: when users purchase goods online, they rely not only on the infrastructure for doing so but also on credit card firms or banks to verify and process the payment (ibid.); when users send money from one account to another, both – sender and receiver – rely on banks and money service businesses to oversee the transaction, which in some cases can take up to 4-5 business days to be processed, including the fees charged by intermediaries for their services; but also in the physical world for claiming asset ownership, centralized authorities like governments play an essential role (ibid.). Institutions, therefore, have a vital role ascribed which is their ability to ensure trust within society by providing infrastructure and services so that strangers can interact without the need to trust each other (Pisa & Juden 2017). Such a role as an intermediary is especially crucial as our world becomes ever more complex, interconnected, globalized, and interactions between people more impersonal.

Today, as argued above, nation states and platforms represent the modern dominant institutions that coordinate human interaction (CVVC 2023), acting as intermediaries, ensuring trust and the functioning of today’s service-based economy. Over time, these institutions gained people’s *confidence* by proving the functioning of these complex systems, allowing strangers to interact on a global scale. It is confidence, because „(...) people do not perceive the risk that their expectations might remain unfulfilled (...)“ (De Filippi, Mannan & Reijers 2020: 3) when interacting with others through non-human systems such as banks or other institutions. Such interactions, as Luhmann (2000) argued, entail neither risk nor uncertainty. Luhmann (2000) further distinguished these situations from those that entail such characteristics, known as *situations of trust*. In situations of trust, there is also a certain degree of unpredictability given in that sense, that a trustee could „act against the interests of the trustor – which is especially true in the case of information and power asymmetries“ (De Filippi, Mannan & Reijers 2020: 3). Importantly, acting against the interests of the trustor can occur in situations of both trust and confidence, as history has shown. Over time, we have outsourced trust to those entities who believe to be trustworthy when it comes to dealing with medical or personal data, finances, digital friendship connections, etc. However, due to particular events such as Cambridge Analytics (Voshmgir 2020: 286), the global banking crisis in 2008, or the decreasing value of the world currencies caused by the central banks inflating the money supply (e.g. van der Cruijsen et al. 2023), trust in those centralized entities tends to decline (Atkinson et al. 2019: 4). Additionally, over the last years, proponents of Big Tech have pushed the term "techlash," referring to a general fear and animus toward Big Tech companies and innovations grounded in IT (Atkinson et al. 2019). It is particularly trust in search engine companies and social media platforms, as Edelman (edelman.com, accessed 7th July 2024) reports, that is declining significantly, from 53% who trusted these companies in 2017 to 42% in 2018 (4).

Trust is a societal essential but complex concept that has already been discussed by various theorists, including Simmel (1900), Hobbes (1985), Parsons (1970), Giddens (1990), and Luhmann (1979). Simmel, for instance, argued that "without the trust that people have in each other, society itself would disintegrate (…) and very few relationships would endure (Simmel 1978: 179). Similarly, Parsons (1970) stated that it is the notion of trust in particular, which he believed to be essential for establishing solidary groups (142). Another theorist, Hobbes, envisioned in *Leviathan (1985)* the *state of nature*. According to Hobbes (1985), in such a state there are no rules, no law, or any social order, but fears and conflict, which eventually leads to anarchic conditions. Therefore, conflict is caused by competition, glory, and *diffidence* (Ch. 13, 88) – the lack of trust in others. The only hope for people to establish safety and social order is through the establishment of a *mighty power* over the community (Hobbes 1985). Hobbes advocated for the very foundation of contract theory which is "the confidence that power would not be exercised against the people's interest." (Misztal 1992: 7). For Rousseau (1762), in contrast, it is civilization itself and the establishment of institutions that have corrupted society. He viewed a pre-civilized state of human society, without a ruling mighty power over the community, as a peaceful and idyllic situation (see Reijers et al. 2016: 139). Only when people established institutions, including private property and money, corrupt societies emerged and facilitated injustices and inequalities between people (ibid.). These ideas, perceptions, and concepts indicate various different and early debates on the notion of trust and its role.

Nowadays, in some cases, confidence in institutions, central authorities, and social media platforms in particular (Atkinson et al. 2019) has declined due to health and financial crises, economic imbalances, political turmoil, digital dictatorship regimes, fraud, or the misuse of people's data (e.g. ibid.; economist.com, accessed 24th May 2024; eurofound.europa.eu, accessed 14th June 2024; gallup.com, 3rd June 2024). These examples represent a predicament, which Hobbes refers to as descriptions of „state of nature" where once well-trusted actors become ‚strangers´ acting in selfish ways to the detriment of trustors. The pressing question arises: How can once trusted institutions that have, in some cases, intentionally betrayed people's trust, such as banks in 2008 or Facebook (Cambridge Analytica), regain users' confidence in their infrastructure?

Blockchain advocates would contend that institutions cannot be trusted (again). Blockchain advocates might follow a radical approach, which would be to dismantle institutions, thereby avoiding centralized entities and building interconnected, decentralized, self-governing, and *trustless* systems or communities based on technological infrastructure without interference from corrupted or self-interest-driven third parties. Blockchain advocates believe *their* technology can provide a viable response to these questions and the aforementioned predicament. The response suggests a shift from centralized to decentralized systems, in which data and information-sharing processes are no longer stored and managed by a single point of control but rather distributed within a more democratic system, processed and controlled by participants operating within a network. Thus, a new „architecture of trust" (Werbach 2018) evolves designed with just a view lines of code, enabling new digital forms of trust (Alston et al. 2021: 2). With the implementation of blockchain, trust is distributed, meaning that it does not necessitate high levels of confidence in single authorities (Treiblmaier 2019: 4). The need for trusted third parties, therefore, vanishes, offering a viable solution to issues of mistrust and uncertainty. According to the blockchain community, human nature and especially the notion of trust in humans are envisioned to be the corrupting factors in contemporary civilizations (O`Dwyer 2015). Considering today's misuses of data in terms of extracting, analyzing, curating, and selling users' data without their consent, managed and controlled by centralized and monopolistic data-driven businesses, such as Big Tech's operating platforms, the debate about whether users can trust these firms is widely spread and a contentious one.

Trust, as explored, plays a vital role in today's economy, particularly when it comes to transferring data throughout the digital. Intermediaries, such as banks or platforms, provide infrastructure and technological means that enable the transfer of value and data, stating that users can trust them and their business operations. However, the several examples of companies, banks, governments, or platforms misusing users' trust push the debate about the true role of these intermediaries forward, promoting a conversation and asking whether we need such intermediation at all. Moreover, as illustrated, fully trusting central authorities is not always a good option. This raises the question of whether building a trustless system in which trust apparently becomes obsolete due to technology and code is the way to go. Some argue that because trust in humans is undesirable, it should be made redundant (see O'Dwyer 2015). By leveraging the appropriate technological means, there is an ongoing discussion about establishing a network or system in which the notion of trust in central authorities or humans in general is replaced by the notion of trust in code (ibid). For example, Ragnedda & Destefanis (2020) argue that with blockchain technology, a groundbreaking instrument can be applied to deliver a „new" trust model envisaged by *smart contracts* (4).

3.3 Smart Contracts

In 1994, computer scientist Nick Szabo introduced the term smart contract, postulating that the digital revolution would eventually automate functions resembling those of legal contracts, which would facilitate global free markets (Dávila 2023; Gord 2016). Although this thesis aims to avoid using technical terms and explanations about how blockchains and smart contracts function – which would require not only technical knowledge but also computer science understanding – it is indispensable to briefly describe the fundamental characteristics of smart contracts in a simplified manner. This fundamental understanding will help to better grasp the ways and extent to which smart contracts can potentially be applied in practice for building a self-regulating decentralized network of participants, without dependence on governments, platforms, or other central entities when it comes to data management.

The blockchain landscape is vast and diverse. As of 2024, more than 1,000 distinct blockchains have been developed since the emergence of Bitcoin (coinpaper.com, accessed June 26th 2024), many of which have their own smart contracts that work similarly. Despite this fact and for a better illustration, this thesis aims to make the topic of blockchain and smart contract applications for data ownership purposes more tangible by generalizing smart contracts, using Ethereum as an example. Ethereum, the second largest blockchain by market capitalization, sitting at approximately USD 320 billion (Statista, accessed 25th September 2024), has approximately 500,000 active users globally (etherscan.io, accessed 28th June 2024). The Ethereum Foundation, a non-profit organization responsible for overseeing the development of the Ethereum blockchain, defines a smart contract as:

> simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain. Smart contracts are a type of the Ethereum account. This means they have a balance and they can send transactions over the network. However, they`re not controlled by a user, instead they are developed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible. (ethereum.org, accessed 14th June 2024)

Voshmgir (2020: 105) states that "a smart contract is a rights management tool that can formalize and execute agreements between untrusted participants over the Internet, and comes with inbuilt compliance and controlling." Dávila (2023) describes an Ethereum smart contract as "a facilitator of an automatically enforceable event that has many different outcomes depending on the inputs of the contract and how other accounts on the network are interacting with it." (81) Similar to a traditional computer program or script, a smart contract simply relies on IF-THEN statements, meaning that IF a certain condition is met, THEN a specific next step or function is initiated. What differentiates a smart contract from a traditional legal contract fundamentally is that "the enforcement of the consequences of the conditions being met is automatic" (ibid.). In contrast, a traditional legal contract relies on the enforcement of a central authority or legal jurisdiction, such as a government. In practice, trusted intermediaries in Web 2.0, such as Amazon, Airbnb, or Uber, settle the contracts between actors by which the transactions are secured while receiving settlement fees for their services. This Web 2.0 business model, according to Voshmgir (2020: 105), is a result of the lack of both a trustful native value-settlement layer and a user-centric identity system, shaped by the early visions of the Internet (Mager 2010; René & Mapes 2019). A possible alternative to this business model represents the implementation of smart contracts. Smart contracts, implemented within a user-centric identity system, allow the formalization of relationships between users and their assets in a P2P manner (Voshmgir 2020: 105). Moreover, in Web 3.0, by utilizing the identity layer, owners of blockchain-based identities – also known as decentralized identities represented by a wallet address – can interact directly with smart contracts without the need for intermediation. Within this context, one crucial differentiation between traditional systems and blockchain systems is that the former relies on actors "that validate, maintain and enforce contracts between people (e.g. accountancy and legal systems)" (Reijers et al. 2016: 136) whereas the latter, smart contracts as a blockchain application, have social and functional properties built within the system (ibid.). Use cases for such can be found in banking, the Internet of Things, insurance, fine art, energy, education, mobility, e-government, security, and privacy, and many more (Voshmgir 2020: 107; Zheng et al. 2018). In all these different branches and use cases, blockchain believers envision that whenever an intermediary intervenes, agreements, processes, tasks, or payments can be collectively and automatically managed via smart contracts. Proponents of smart contracts even envision a future, according to Taghdiri (2019), "where commerce takes place exclusively using smart contracts" (178). Voshmgir (2020) states, that "many traditional intermediaries, like lawyers, brokers, and bankers, or public administrators, and Internet platforms might no longer be necessary, or at least some of their services might become obsolete." (107) Ragnedda & Destefanis (2020) explain, the idea „is to get rid of a central control authority, entity or organization which both parties must trust and delegate such a role to the correct execution of a computer program." (ibid.) Smart contracts rest on blockchains' functional characteristics of transparency, immutability, and decentralized, enabling all transactions and information-sharing processes to be stored on a public ledger through a tamper-proofed mechanism (Wright & De Filippi 2015: 19). Smart contracts enable particular actions to be enforced automatically and facilitate self-organizing networks, all defined through a pre-set of rules and legal provisions programmed in a code (Wright & De Filippi 2015: 11).

Smart contracts, Voshmgir (2020) explains, “can provide a native settlement layer for the sharing economy, currently brokered and processed by Internet platform operators” who own a “disproportionate part” of users’ data and its economic value (108). When implemented properly, smart contracts could enable “smart access control” between two parties who do not trust each other which could ultimately lead to a “sharing economy on steroids.” (ibid.) According to Voshmigr (2020), such an economy means that all Internet-connected devices, such as cars, apartments, TVs, washing machines, fridges, bicycles, or other IoT devices – once they have their own blockchain address assigned (or a decentralized identifier (DID)) – could be managed by smart contracts (108). The devices can then interact with each other, facilitating machine-to-machine interactions with no human interference. This would not only automate processes and allow tasks and contracts to self-execute in real time, but would also imply great cost savings while ensuring high levels of security. However, from an academic standpoint, smart contracts are still at an early stage and are far from being adopted by the masses. Therefore, smart contracts and their use cases need to be studied and explored more by researchers. This is particularly true in areas such as scalability, flexibility, and data privacy (Mohanta et al. 2018; Swan 2015). Given that blockchain technology research is currently in its infancies, studying specific case studies according to Treiblmaier’s recommendations (2019) will “systematically generate knowledge on which future research can build” (13). This approach suggests that researchers need to provide a rationale for the use of blockchain in general, define the blockchain type for the use case, describe the blockchain characteristics that are relevant for the use case and how they are implemented, provide a critical evaluation of the results, and embed the results into a broader context, thus enabling incremental research (see Treiblmaier 2019: 13).

This thesis is further motivated by the aim to provide knowledge and research results to a broader audience, to identify and reflect on blockchain’s both characteristics and applications, and to provide an overview of blockchain use cases with regard to data ownership. Furthermore, this thesis aims to contribute to incremental research that benefits blockchain’s critical academic evaluations in the future. In doing so, the following sections will examine specific uses cases for smart contract applications with regard to data ownership.

3.4 Blockchain, Digital Identities, and Smart Contracts: Redefining Data Ownership

"The Internet is a Decentralization Engine. But it is one that reaches its true potential in its next incarnation- Web 3.0." – René & Mapes 2019: 153

Before delving into the next section and exploring use cases regarding data ownership, summarizing the previous sections will help to better understand the aforementioned deficiencies of the traditional Internet and examine the potential solutions and role that blockchain technology promises to play. In addition, this section further engages with the explanation of ownership in general, how ownership could be regulated technologically, the role of smart contracts, and the introduction of some projects working on decentralized identities and decentralized data marketplaces, in which users have full control over their own data, facilitating self-sovereign identities (SSI).

3.4.1 From Then to Now – A Summary

If we recall from Chapter 7 (Theoretical Background), capitalism was able to survive the economic downtrend in the 1960s and expanded further because of its plasticity (Zuboff 2020: 520), by reinventing itself (Staab 2021), and by means of creative destruction (Schumpeter 1943). At the end of the 20th century and the beginning of the 21st century, the introduction of digital information-sharing, network, and telecommunication technologies in particular facilitated the expansion of capitalism's dominant mode of production (Dávila 2023: 111). This mode is characterized by offering services for free while aiming to stay profitable and align with the central imperatives of wealth accumulation, profit maximization, competition, economic growth, and the relentless drive for labor productivity through the technological elaboration of production (Zuboff 2020: 345). By using typical Web 2.0 services and applications that are built around the commodification of users' attention (Dávila 2023: 155), the content creators and data generators – essentially the platform users – continuously provide data to platform owners, while receiving nothing in return for their "work" (Dávila 2023: 148), except the free service or app they interact with. This, over the course of the evolving digital era, facilitated the emergence of a new class that does not own the means of production – as it has been over the course of the Industrial Revolution throughout the past centuries – but rather has ownership over information (Srnicek 2017; Wark 2004).

The new class of capitalists drives their inherent extraction imperative (Zuboff 2020) into almost every corner of society, primarily benefiting from claims of ownership of data. The capitalists of today's digital realm under digital capitalism feast not only on users' behavior (Zuboff 2020: 194), while selling behavioral surplus for tremendous economic profit, but also entirely neglect soaring inequalities and power asymmetries. This includes restricted access to the Internet and digital infrastructure, limited access to information and knowledge, and user exploitation. This is also why digital capitalism is described as a "machine for producing social inequalities" (Staab 2021: 301), promoting new societal forms of rule (139), driven by Big Tech companies of the existing Web 2.0 world. Big Tech in particular acknowledges the potentials of extracting, storing, analyzing, and distributing data in a centralized manner. The concentration of knowledge, data, and power not only highlights embedded power dynamics but also enables Big Tech companies to stay profitable while building and expanding their proprietary markets, which form today's digital and societal infrastructures for interaction. Moreover, capitalism can be described as a centralization machine (Dávila 2023: 145), primarily due to the mechanisms and dynamics of its operation. This description highlights an intriguing development of the Internet and its usage: the original purpose, as designed in the early 1970s, was to decentralize the "flow and access of information" (René & Mapes 2019: 153; see Berners-Lee 2000; Mager 2010). The initial aim was to allow interaction and information exchange between a decentralized network of computers (nodes), finding the optimal route between the sender and receiver (René & Mapes 2019: 19). The Internet, based on its early implementation and in fundamental contrast to capitalism's logic, was considered as a "decentralization engine" but has lost much of the "distributed spirit of the original design principles" (René & Mapes 2019: 21). This happened over time, primarily due to capitalists, Big Tech, and governments leveraging the surveillance, centralization, and monetization of web users and their data (ibid.). The development of the Internet and its usage under the logic of digital capitalism exemplifies how some actors made use of this technology for their own interests to the detriments of others. Again, this underscores that the inherent nature of technology is neither good nor bad per se, but that the impacts and outcomes crucially depend on the purposes and values behind its usage.

As explored in this chapter, blockchain tends to provide a solution to some of the deficiencies and limitations of the traditional Internet. The lack of a technological layer in the traditional Internet (Web 2.0) is a primary example for how blockchain proponents envision future applications of their technology. By providing the missing layer within the evolving Web 3.0 space, blockchain technology facilitates decentralized digital identities and self-sovereign identities, smart contract applications, and the processes of sharing and transferring value throughout the digital realm without the need for intermediation. Second, it is the societal „problem" of trust in the digital realm which blockchain tends to redefine by introducing trustless or trustfree systems (see Greiner & Wang 2015), utilizing the blockchain to create a verified, immutable, and available record of transactions that is governed by the system itself." (Treiblmaier 2019: 4) This indicates that users within such systems or networks do not have to rely on trust, neither in institutions nor in people, but in technology. Consequently, they simply transact and interact to obtain the desired service. Furthermore, by leveraging a more decentralized architecture and technological stack, new economic business models emerge (Dávila 2023: 84) (more in Section 4.4.4 and Chapter 7). This can facilitate both purpose-driven ecosystems (see Voshmgir 2020: 108) and disruption across the Web 2.0 landscape. Within such systems users can directly benefit from their online activities by receiving compensation in the form of "network tokens" (e.g. Steemit), without any centralized platform providers involved (108), and without the need to pay fees for their intermediation services, as demonstrated by a project called Mycelia (Taghdiri 2019: 185). This example will be explored in the following section.

3.4.2 Web 2.0 in Practice – The music industry's mess house

To better understand the inequalities and asymmetries embedded in existing Web 2.0, the following explores an example from the music industry. This elaboration on Web 2.0, in which platforms act as intermediaries and take fees for their services while accumulating, storing, and selling users' data, can also be applied to various other industries, including video streaming, social media, sports, and the health sector. It is important to note that the following example refers to a modern business model that has only been made possible by the digitization of music. This fundamental shift over time has led to the emergence of new revenue models centered on the idea of selling streams instead of physical goods, such as CD. For illustration purposes, the following explores a real-world example of the financial deficiencies content creators face due to controlled intermediation. In general, it is particularly the issue of an underlying information access asymmetry that “compromises the relationship between content creators and intermediaries (i.e., labels, publishers, and streaming services)” (Taghdiri 2019: 173). Taghdiri (2019) describes this relational constellation as an *archaic system*, in which intermediaries take transactional fees for their intermediation services “without any reasonable present day justification” (173). The asymmetry in information access and compensation is particularly common in the music industry. Artists, musicians, and other participants consider existing royalty payment systems to be outdated (WIPO 2021:15) and demand new, more equitable business models. Following reports, the average musician makes $23.40 for every $1,000 of their music sold, which is about a two percent net profit (see Byun 2014: 180). Frankly, such a royalty payment model, called „big pool“ or „market-centric-model“ (WIPO 2021:4), does not appreciate content creators’ work at all. Notably, many musicians and artists push toward transparency and fairness, including Paul McCartney, Duran Duran, Taylor Swift, and Dr. Dre (Heap 2017). This is because streaming platforms, labels, publishers, and other middlemen cut off huge percentages to distribute and manage the artists’ content and business (Taghdiri 2019: 180), while perpetuating an inequitable arrangement between the involved parties. This not only demonstrates inequitable business relations but also underscores both economic and power imbalances, exploitation, and a failure in managing and processing data and information through third parties in a balanced way.

However, given the current state of research and development, smart contracts have potential to impact the music industry by challenging existing imbalances, as demonstrated, and by disrupting revenue business models that primarily benefit intermediaries. Smart contracts can ultimately help „to get the music industry’s messy house in order,” as Heap states (2017). There is already a decent amount of literature arguing that blockchain and smart contracts, in particular, are technologies with potential for transforming or revolutionizing the music industry (see e.g. Aitken 2016; Caretta 2020; Dickson 2017; Heap 2017; O’Dair 2017; Sharma 2017; Taghdiri 2019; Wallach 2014). The implementation of smart contracts could eliminate the reliance of content creators on intermediaries, such as purchasing platforms or financial brokers. The vision is that smart contracts enable direct interactions between content creators and their community, which allows them to sell products without intermediation and in a straight-forward manner (Perez & Heap 2016). In contrast to the existing market-centric model, this facilitates a more artist-centric model through the utilization of blockchain-based smart contracts. Therefore, smart contracts allow artists to sell their products directly to the fan community by leveraging the benefits of *tokenization*. With tokenization, which refers to the „process of digitally representing an existing, off-chain asset on a distributed ledger“ (Osborne et al. 2021: 219), a new music track, or an album could therefore be digitized and represented as a token. Such a token exists on a blockchain, cannot be replicated, proves ownership, and ultimately allows the artist to provide the track represented by a token to the community, which enables the entire processes of buying, selling, and trading the token without any interference of third parties. Moreover, the artist can decide how, when, and at what exact price the token will go public, ultimately eliminating reliance and mitigating power dynamics within the music industry of Web 2.0. *Mycelia*, an innovative music-sharing platform, exemplifies this idea by utilizing the core principle of blockchain technology. This includes a decentralized ledger that stores all the information from artists' songs in an accurate, global database while providing ultimate transparency, allowing for secure peer-to-peer transactions (Taghdiri 2019: 185). This eventually facilitates the creation of a more dynamic, efficient, transparent, balanced, and enjoyable music industry, encompassing benefits for both artists and fans.

Owing to blockchain's secure nature, the gap between content creators and consumers can be bridged and intermediaries eliminated while facilitating quick, efficient, and seamless transactions and ensuring transparency (Taghdiri 2019: 178). Notably, the potential of smart contracts extends beyond the music industry. In various sectors and business use cases, smart contracts could pose a promising solution in reducing the need for intermediation (ibid.). However, one mandatory aspect before smart contracts can fully reach their true potential – and before users or machines initiate the processes of both sharing digital information or transferring value throughout the digital – is verifiable ownership. This is especially important when intending to buy, sell, or transfer digital goods. Without any verifiable ownership, intellectual property, music, art, or any other digital good may be at risk of issues such as fraud, mismanagement, or the "double-spending-problem." Blockchain, along with its smart contract applications, promise solutions to these concerns.

To grasp blockchain's potential and promises, it is important to understand precisely what ownership means. To answer this question, the following will explore the topic of ownership in more depth, elaborate on core definitions, and further aim to integrate this understanding into the discussion of potential blockchain applications.

3.4.3 Defining (Data) Ownership

In recent years, the subject of data ownership (DO), including its research, development, and real-world implementation, has gained increasing attention. At least since the emergence of Big Tech and social media, the debate about the data these companies own and the profits they generate from it has intensified. Under the extraction imperative of capitalism's modern mode of production, information that was previously insignificant gained attention and value owing to its digitization. Information that has not been valuable prior to digitalization, and hence, before the transformation processes from the physical to the digital realm, ultimately gains significance and value. This is primarily due to evolving technologies and the increasing tendency of companies, institutions, and organizations to accumulate vast amounts of information. By generating insights from raw information through the process of analyzing it with the help of Big Data and Artificial Intelligence applications, they generate value, ascribe it to digitized data, and then further sell it. Importantly, as soon as digitalized information *gets* its value, the issue of data ownership arises. However, data ownership as a subject has no unified view, making it difficult to summarize its notion in one definition. Data ownership extends beyond simply considering complete control over the data and its rights. Instead, it encompasses control over access, creation, generation, modification, analysis, use, sell, or deletion, in addition to the right to grant rights over the data to others (see Asswad & Gómez 2021: 2). According to Asswad & Gómez (2021), "one of the major complications is the perception of data ownership and the willingness of data holders to share their data." (ibid.) The notion of owning data differs vastly and varies from industry to individuals, to use cases, to strategic marketing decisions, all of which come with individual interests, values, and purposes for the further usage of data. This raises the question of how data ownership is conceptualized by various stakeholders, as well as who can legitimately claim ownership of data. Furthermore, it is essential to examine which entities effectively possess ownership rights: content creators, platform or service providers, data analysts, AI machines, marketing agencies, or even Internet of Things devices. Asswad & Gómez (2021) provide an answer in their paper: based on their results, the authors concluded that there is no single right answer to the question about who should own the data. In order to answer this question, they argue, many different aspects need to be taken into consideration and further stress that data ownership is "always dependent on the case and its requirements including legal, ethical, organizational, and technical requirements." (26) This highlights the complexity of data ownership. Nevertheless, the following aims to provide more clarity.

An important aspect to consider is that the perception of owning digital information differs considerably from the concept of traditional property ownership in the physical world. Property ownership, according to Hart (2002: 3) "is the rights to use, control the use, and remain in control of whatever is owned, without the interference from others." This definition seems straightforward; however, it might not be fully applicable to ownership over data. This is because data is often characterized by "intangibility, non-exclusivity, usage-tolerance (do not deteriorate through use), and age susceptibility (do often deteriorate with age)." (Asswad & Gómez 2021: 3). Therefore, data ownership cannot be considered as and equated with property ownership and needs further deliberations. Data ownership is mainly associated with and integrated into information systems or database management systems that involve the control dimension of a database. Within this control dimension, Asswad & Gómez (2021) describe that data ownership "is often confused between "ownership" and "use" privileges." (4) While use privileges are primarily concerned with the right to access, modify, create, and manipulate data, ownership privileges concern the right to control these privileges. The authors further state that "even if the user is granted the same rights as the owner, the authority to grant, alter or withdraw these privileges is what distinguishes the owner." (5) To add another layer of complexity, this distinction between use and ownership privileges does not consider the actual owner of the data, which in some cases can lose ownership privileges whenever a central authority, such as a platform, decides to interfere or revoke the owner's ability to grant privileges. To elucidate this further, Saarikko et al. (2017) highlight that in some cases, regarding the IoT sector, it is the user who generated the IoT data that has the right of ownership; in other cases, it is the person or firm that collected and analyzed the data that is allowed to claim its ownership. Therefore, the owner is not always the exclusive owner of the data if the data is stored on a centralized server and also if the platform or centralized authority decides, for instance, to seize the account or restrict access to services and applications. This highlights again existing power dynamics and asymmetries in access and control, as explored in Section 4.2.1. Additionally, according to Saarikko et al. (2017), and as Asswad & Gómez (2021) state, "there is no single approach suitable for all cases and that we have to accept the fact that for now, data ownership will be tackled differently in different contracts and in different businesses and countries" (4). Given this, the way of defining ownership, its allocation, and how different stakeholders deal with it remains ambiguous, unclear, and controversial. The different stakeholders involved further complexify this elaboration on data ownership because everyone involved in the data value-creation chain seeks to claim some sort of ownership. Therefore, granting individual rights over data to different stakeholders differs significantly and is unclear.

One approach through which stakeholders and initiators seek more clarity and regulation of data is the General Data Privacy Regulation (GDPR), which became effective on May 25, 2018. The GDPR represents a specific EU legal framework that concerns the protection of the data generated by individuals within the EU and by those that transact within the EU; the regulation of its ownership, however, remains unclear and has not been addressed sufficiently (Janeček 2018). The fact, that the GDPR "was written with a centralized entity in mind that has the power to control access rights" (Treiblmaier 2019: 5), highlights the lack of considering blockchain technology as a potential solution for ownership and data management. It remains unclear how blockchain technology will comport with the GDPR (see Posadas 2018), nor is the ownership of data subject to its regulatory considerations. This is despite blockchain's potential "to strengthen cybersecurity and privacy by deterring cybercriminals and unauthorized data manipulators" (Treiblmaier 2019: 5.) and enable full control of data. This raises questions as to why these topics have not been sufficiently addressed. In addition, Van Asbroeck et al. (2017) also criticize this when they mention in their overview of the EU legal framework regarding data ownership that in Europe there is a lack of clear regulation "where personal data cannot be owned but rather protected from access or use by anyone other than the data subject to whom the data refer." (Asswad & Gómez 2021: 8) To illustrate this unclarity and lack of directness, Mineraud et al. (2016) evaluated in their analysis about how the IoT landscape deals with issues like ownership, privacy, and security of IoT data. The analysis revealed that data ownership data ownership is a "major concern" for most IoT platforms and that it is "rarely fully guaranteed." (8) This is because many platforms store the generated data on their centralized servers without encryption and often without disclosing security measures (4), which again underscores the inherent power dynamics as well as some parts of the issue with centralized ownership (Section 2.1) and private property (Marx 1844/1932; Marx & Engels 1848). Mineraud et al. (2016) further argue that full data ownership is only granted when data is stored locally, and suggest that future IoT solutions must have algorithms and mechanisms for the data owner to provide "access only to a predefined set of resources, and that the raw data must remain under control of the end-user." (5) Solutions regarding this will be explored in the following section.

3.4.4 Web 3.0 in Practice – The implementation of Blockchain Technology

As explored, data ownership is a vague concept without a clear definition. For illustration purposes and to better frame and grasp data ownership in a more tangible way, the following will focus on providing a clearer understanding of data ownership and further discuss upon the use cases in practice and the role blockchain technology plays within. Blockchain technology, along with its characteristics, provides a possible solution for addressing issues regarding the management of data, as explored in the paper written by Karafiloski & Mishev (2017). Their paper, moreover, highlights the possibilities that the decentralized nature of blockchain-based applications entails for addressing issues such as data security, privacy, DI/SSI, and data ownership.

For the purpose of this thesis and to better envision practical applications of blockchain technology, data ownership requires a clearer definition. Therefore, and according to the findings and standpoint of the study conducted by Asswad & Gómez (2021), data ownership is:

> the possession of data and the control of data including the ability to grant rights over data to others, taking into account the type of data, the legal and ethical aspects, the responsibility for data, and the needed requirements to preserve and achieve this possession. (25)

This includes the possession of complete control over the data and its rights, access, creation, generation, modification, analysis, use, sale, or deletion (2). For the purpose of this thesis, data ownership – based on the definition above – also encompasses full ownership and control of the data associated with one's persona generated while using services and platforms. Consequently, this means that whenever a user interacts with an application, data is generated, which the user verifiably is in full control of. Users, therefore, are the actual owners and can claim the aforementioned ownership and use privileges.

The idea of leveraging the potential of blockchain-based implementation for data ownership purposes was investigated by Liang et al. (2017). In this study, the authors propose a "user-centric and blockchain-based health data sharing and collaboration solution." (10) The solution described by the authors is a mobile user-controlled system that leverages blockchain-based smart contracts while ensuring security and privacy preservation (Androulaki et al. 2018; Cachin 2016; Liang et al. 2017). Enabled by blockchain technology, every time a company or other authority is interested in the user's data, requests have to be made in order to get access to the data and its usage, which the user, as the owner of the data, grants, denies, or revokes (Asswad & Gómez 2021: 10). Notably, every interaction, whether it is data collection, upload, request, or access to its sharing, is recorded and permanently stored on the blockchain, ensuring integrity and trustworthiness (11). Another blockchain-based implementation in the health sector is MedRec (Azaria et al. 2016), a decentralized record management system in which patients are in full control of their electronic medical records (EMRs). Additionally, patients have the capability to grant access to and share their data, which is fully anonymized. Interested stakeholders can participate in the blockchain network as nodes and can access the data "in return for securing the integrity of the blockchain via a proof of work." (Asswad & Gómez 2021: 11) Blockchain, thereby, enables secure P2P interactions without any intermediation, while ensuring both privacy and a reliable, trustworthy way to exchange data.

Especially when it comes to sensitive personal or health data, blockchain claims to provide security, integrity, and the ability to own and control the data. In addition, as users spend more time on the Internet and, consequently, data generation, a secure infrastructure that allows access, ownership, management, and exchange of data becomes indispensable. In response to this need, companies such as *Ocean Protocol* are developing a promising solution by providing a decentralized data marketplace where users can interact within a secure infrastructure based on blockchain technology's characteristics. The firm acknowledges the vast latent value of data, which is often not used because it is stored on centralized servers. According to MacKinsey (2016), about 90 percent of all the digital data societies ever created has been generated over the course of the past two years; however, only about 1 percent of the data has been analyzed, and a massive 99% is sitting dormant and locked on centralized servers. "It's a valuable resource that isn't being used", one of the founders of Ocean argues (Ocean Protocol 2017). Ocean's idea is to make use of that data. Their vision: everyone should benefit from the data produced on a daily basis by allowing users to fully own their data, store and control it, grant access to others, and sell the data for compensation (ibid.). In addition, the firm argues that "data can be used to power innovation and lead to breakthroughs that save lives, reduce costs, and improve the quality of our environment. But right now, data is locked up.” (Ocean Protocol 2017) Therefore, Ocean Protocol allows interested parties, such as scientists, to access the massive amounts of data provided by users, and AI helps to identify patterns, make conclusions, and unravel insights and valuable information for broader society without violating anyone’s privacy. Data owners can derive benefits through not only the provision of datasets but also through their sale to organizations or individuals while receiving token payments (see Lee 2019: 782), representing the native means of exchange of the Protocol (ocenprotocol.com, accessed 9th July). Ocean Protocol demonstrates how two trending topics, blockchain and AI, intersect by providing a decentralized data exchange protocol that connects the data hives with AI hives: users that generate data can benefit from leveraging token economics (Voshmgir 2020: 108).

Besides companies, there are countries, such as Estonia, that acknowledge the importance of ownership in the evolving digital realm. Estonia, where emerging technologies such as blockchain are applied to regulate various parts of the country, is being considered a role model for governments and gives „(...) an entirely different outlook on what a truly human-centric society entails for digital citizens.“ (E-Estonia, accessed 18th July 2024) The Estonian government implemented blockchain-based applications into their digital infrastructure through their national project called E-Estonia, which aims to enhance institutional services (Alexopoulos et al. 2021; Semenzin et al. 2022), including the provision of a secure e-voting system. Furthermore, at the institutional level, Semenzin et al. (2022) state, “blockchain’s potentialities regarding transparency and data ownership, among others, can be claimed (…) as key to fostering more participatory approaches toward governance and returning the control of the data to the citizens.” (5; see Asswad & Gómez 2021) One of Estonia’s public digital services leveraging blockchain’s potentialities is its eHealth system. This system enables patients to access their health data through the national ID and signature and grants them both accessing and revoking their data at any time and for any case (Asswad & Gómez 2021: 11). By leveraging blockchain technology and its characteristics of immutability, transparency, and decentralized, the Estonian government demonstrates that citizens can be sure about their data being safe and secure and therefore to trust their government (ibid.). However, with the implementation of blockchain applications, the often-praised characteristic of transparency also raises questions about a potential loss of privacy, as every interaction and transaction is stored as information on the blockchain and therefore visible to everyone. In addition to that, another potential negative side effect may also be the widening of the “digital divide” that could be caused by a lack of technological skills (Treiblmaier & Umlauff 2019: 12), eventually leading to people being left out. Both potential risks are examined and discussed in the following chapters.

Whether they are companies, fund managers, or investment firms such as BlackRock, Vanguard, or Fidelity, within the health sector or other industries, or even governments – the interest in the topic of data ownership, blockchain-based applications, and their characteristics is increasing rapidly. The preceding sections aimed to provide more clarity regarding the concept of data ownership, explored the role of blockchain and its promising application of smart contracts, and examined how this technology is currently being applied and may be applied in the future.

Now, the following questions arise: Where are we heading? Is blockchain technology the appropriate tool for addressing the challenges of digital ownership and digital identity management? How do experts perceive and envision the future of digital ownership and the role of blockchain applications? The following chapters will delve into these questions and examine what it could mean to build the missing identity layer and a user-centric model with the help of blockchain and what its impacts on societies might be. Moreover, the results will ultimately contribute to the understanding of owning digital data from a user perspective within a user-centric system (decentralized identity/SSI) by applying blockchain-based applications, such as smart contracts (more in Chapter 7). Examining these issues and answering these questions will contribute to a better understanding of blockchain’s potential in offering alternative models that promote a more balanced distribution of value, shifting power dynamics, and robust data ownership frameworks.

4 Sensitizing Concepts

This chapter delves into the conceptual framework of the thesis. The following frameworks allow us to examine the topics of data ownership, digital identity, and blockchain technology through various conceptual lenses, thereby playing a crucial role in comprehending these intersecting topics. In particular, this chapter explores the sociological relevance of the subject matter and introduces key concepts, including Science and Technology Studies (STS) and (socio-technical) imaginaries. These concepts provide the theoretical foundation for approaching the topic of data ownership and analyzing how blockchain technology might help redefine societal structures and the notion of trust, facilitate decentralized digital identities and self-sovereign identities, and flatten existing power dynamics within digital societies.

4.1 Sociological Relevance

Rapid technological developments and their manifold implications in today's digital era compel societies worldwide to adapt to transformation at an unprecedented pace. Over the last three decades, the emergence of the Internet, platform economy (Srnicek 2017), and various information and surveillance technologies, have led to significant changes in the management, control, distribution, storage ,and analysis of data. Mau (2019) exemplifies this as follows:

> The use of new indicators, data and numerical notations to identify, describe and evaluate the self is gradually transforming the social society into a metric one. Data make visible and define who we are, where we stand, how we are seen by others, and what our expectations should be. (11)

The ongoing development of technology and data in general has changed not only the economy as a whole and influenced the ways in which the topics of data ownership and digital identity are perceived and dealt with, but has also introduced new methods and applications, influencing the ways in which humans perceive themselves and the world, causing profound changes within societies. Such changes with all the implications, however, cannot be understood solely by technical expertise; they demand interdisciplinary knowledge and skills to effectively meet the needs of societies and develop solutions that serve the greater good. As a result, sociologists play an important role in grasping and understanding the various implications on societal structures, power dynamics, and individual agency in terms of self-sovereign identity, as well as on the notion of trust. Moreover, examination through a sociological lens allows us to gain deeper insights into these transformations and the extent to which societies are affected, eventually providing the necessary knowledge, understanding, and tools for navigating these transformative shifts. This includes analytical skills that sociologists bring to the table, such as a profound analysis of shifting power relations between different actors in today's digital world dominated by Big Tech companies. Therefore, sociologists can examine these shifts between individuals, corporations, governments, and other authorities involved. This allows us to reveal new forms of social control, power dynamics, and resistance in terms of movements, advocating for a more decentralized, bottom-up approach that gives users more control over their information rather than adhering to the rules set by central authorities and Big Tech. In addition, the intersection of blockchain technology, data ownership, and digital-self-sovereign identity raises questions regarding privacy and surveillance. Sociologists can investigate how this emerging technology mitigates, protects, or exacerbates surveillance practices. In providing more clarity and a deeper understanding of privacy and transparency, particularly within blockchain applications, sociologists can further contribute to broader debates about these topics and help develop frameworks and policies regarding surveillance and privacy in today's digital era. Moreover, as blockchain tends to promise transformative shifts in how users interact and transact on the Internet, by removing and waiving the aspect of trust, sociologists can analyze the implications of trust-less systems on human interaction. However, it is especially the shift from trust in social and economic institutions to trust in technology to which sociologists can contribute their critical thinking (see Chapter 7).

Another crucial contribution sociologists can make is a thorough analysis of the various cultural narratives and sociotechnical imaginaries that shape and are shaped by technology. This includes an investigation of the ways in which these imaginaries influence policy-making decisions, public as well as corporate strategies, politically-driven motives, academia and research, and individual behaviors.

Therefore, in the context of this thesis, sociologists play a vital role in providing more clarity, insights, and a greater understanding of the potential societal implications of blockchain technology redefining data ownership. Furthermore, understanding the potential implications allows us to investigate the potential transformative shifts in societal structures, power relations, and individual data management.

4.2 Science and Technology Studies (STS)

As described in Chapter 2, this research explores the topics of data ownership, digital identity, and potential (future) blockchain applications through a Science and Technology Studies (STS) lens, with a particular focus on the historical trajectory of capitalism and its impacts on the emergence of Big Tech's operating business models. This is, according to some literature, what STS as a field has "not really engaged analytically or empirically with," as Birch & Bronson (2022) state. However, there is a growing interest in this topic, particularly on the so-called "politics of scaling" (see Avle et al. 2020, also Pfotenhauer et al. 2021) and "politics of modularity" (see Birch & Bronson 2022) which aim to unpack ways to intervene in Big Tech's expanding digital ecosystems (ibid.). This, in particular, marks the ideal fit for this thesis, namely, to unfold Big Tech's operating strategies and business models under capitalism's modern mode of production in order to further examine and provide alternatives to these ever-expanding, proprietary, monopolistic, and data extraction-oriented firms. This research, guided by an STS lens, will unravel sociotechnical imaginaries (Jasanoff & Kim 2015) regarding DO, DI, and blockchain and its potential implications on existing hierarchal power dynamics. In general, applying an STS lens allows to "unpack the dimensions of Big Tech" (Birch & Bronson 2022: 10) by examining and unfolding their hidden strategies and implications for societies. It is an analytical and empirical toolset that STS scholars may apply to think systematically about how Big Tech operates (ibid.). This approach allows to ultimately unpack the organizational practices and boundaries that arise from their extensive focus on user activity, individuals' privacy and life, and data extraction practices. Importantly, STS not only describe and problematize such practices but also existing and emerging unequal power dynamics. Rather, with the knowledge gathered through thorough research, STS scholars can "intervene politically in ongoing debates about the impacts (of) Big Tech" and "support democratic, responsible, publicly-engaged, and inclusive outcomes" (Birch & Bronson 2022: 8).

4.3 (Sociotechnical) Imaginaries

"These superhighways – or, more accurately, networks of distributed intelligence – will allow us to share information, to connect, and to communicate as a global community. From these connections we will derive robust and sustainable economic progress, strong democracies, better solutions to global and local environmental challenges, improved health care, and, ultimately, a greater sense of shared stewardship of our small planet."

– Gore 1994

This statement originates from a speech given by US Vice President Al Gore in 1994 (Flanders 2023, accessed 26th August 2024) and illustrates the making of a *sociotechnical imaginary* of the Internet. It highlights the visions and thoughts regarding the Internet as an emerging global communication infrastructure in its early phase. Interestingly, even though these thoughts represent early-stage visions articulated by a single, albeit influential individual, they have been negotiated, legitimized, and ultimately embraced by broader society over the past decades. Eventually, these thoughts guided the development, advancement, and implementation of this new communication infrastructure significantly and have established as collectively shared and stabilized visions within society. Imaginaries, therefore, can be understood as visions of the future that simultaneously shape collective understanding and guide technological development (Jasanoff 2015). Importantly, these imaginaries regarding the Internet and its applications could have shaped our digital world in completely different ways. Astrid Mager (2012) exemplified this in her work *Algorithmic Ideology* as she writes "if mass media and activists initiated a more critical debate about search engines and the myriad of data they collect, store and process, big players such as Google would be destabilized." (14) This highlights that technology itself does not steer its own path but instead is driven and shaped by imaginaries – including values, purposes, and intentions – of actors before transitioning into collectively accepted visions of the future. However, even when imaginaries become stabilized visions within society, actors have the ability to "renegotiate," starting "off social or political interventions and pave the way towards change." (ibid.) Hence, when there is strong resistance and rejection, power relationships can be transformed (Castells 2009: 11), allowing for the shaping of alternative versions of our digital future. Therefore, it is important to examine the ways and extent to which sociotechnical imaginaries are envisioned, stabilized, and established as collectively held visions by broader society to understand where to intervene and how to push change forward.

For the purpose of this thesis, which is to provide an overview of the different imaginaries of different actors within the field regarding data ownership and the role (blockchain) technology plays within, the following briefly introduces and discusses imaginaries as concepts.

Science and technology studies (STS) in particular have increasingly focused on the investigation of imaginaries over the last few decades (McNeil et al. 2017: 435). This is because "the use of this concept seems to offer new ways to investigate the relationships among science, technology, and society" (ibid.). With concepts of imaginaries, a framework can be developed and applied that allows the study, analysis, and interpretation of actors' reality as well as their thoughts, images, aspirations, and visions about the future. Smith (2009) describes an imaginary as "a particular, often complex view of the world that comes to shape agendas, research trajectories, projects, and policies." (462). Importantly, imaginaries happen to exist in multiple forms in play within societies. They provide a profound lens through which the visions and aspirations that drive technological innovation and societal shift can be examined. Such sociotechnical imaginaries, as Jasanoff (2015: 6) explains, are "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology." This not only implies that imaginaries are social in any sense, but also suggests that our world is not simply given, but continuously "reimagined, or re-performed, in the projection, production, implementation, and uptake of sociotechnical imaginaries." (McNeil et al. 2017: 449) The world, therefore, is and has been envisioned in particular ways, at particular moments in time and by particular actors "who have the capacity to materialize these abstractions." (Smith 2009: 463) Additionally, imaginaries both shape and are shaped by agendas, research trajectories, projects, and policies (Smith 2009: 462), as well as social, political, or technological realities, meaning they enact and are enacted (McNeil et al. 2017: 448). Examining and understanding imaginaries allows researchers to make sense of the world (ibid.), and therefore play an essential role in understanding and comprehending societies' development and states. Additionally, with such an understanding of how societies envision their reality and future, examining sociotechnical imaginaries allows us to further comprehend the role of technology and to guide technological trajectories.

To exemplify the role of sociotechnical imaginaries and put it in context of this thesis, it can be useful to address the following questions: Why is data ownership not addressed sufficiently in the GDPR? What has led to the development of Big Tech's successful business models under the logic of digital capitalism's modern modes of production?

As explored in Chapter 4, one reason for Big Tech's success and today's issues around data management and ownership can partly be attributed to the lack of technological means and layers for account management on the traditional Internet. This lack was once acknowledged as an issue by actors later in the evolving Internet, which from then on – especially in the context of blockchain technology debates (e.g. René & Mapes 2019; Tapscott & Tapscott 2016; Voshmgir 2020) – has become one major topic of interest. Importantly, the traditional Internet does not entail an identity layer for data management purposes because early visionaries did not consider this in their imaginaries. Rather, early Internet visionaries imagined a decentralized network of computers with democratic values and equal access to information, without borders, hierarchies, or limits; hence, there was no intention to implement technological means for data ownership (Berners-Lee 2000; Mager 2010). This highlights the fact that if some thoughts and visions are not considered – implying that other considerations are "more important" – legitimized, established, or accepted as shared visions by broader society, the direction of the technology's development fundamentally diverges. In addition, as stated above, it is possible for several imaginaries to coexist. In the context of the Internet, this means that more than one imaginary existed. However, because "there is competition over imaginaries as different stakeholders promote different visions in policy and political discourse" (Guay & Birch 2022: 3), some imaginaries were successfully established within broader society, while others did not (see Mager 2012). The reason for this is that according to Jessop (2004: 7), some actors within society, such as governments, public stakeholders, courts, and regulators (Jasanoff 2015: 6), are able to manipulate their power and knowledge. This causes them to become capable of establishing their preferred political-economic order by elevating and promoting a particular imaginary (ibid.).

Today's data ownership policies, initiatives, and frameworks are not solely caused by technological decisions or technological systems per se. Rather, the developments around data ownership reflect socio-technical settlements that Jasanoff (2015: 14) describes as the "mutual emergences in how one thinks the world is and what one determines it ought to be." Therefore, owing to recent technological advancements in blockchain technology and its promises in transforming data ownership and digital identity, examining future imaginaries of data ownership can fundamentally contribute to a better understanding and, ultimately, facilitate more effective and controlled guidance of current and future developments. Furthermore, examining, analyzing, and understanding the sociotechnical imaginaries of different actors within the field of data ownership and blockchain technology helps to frame the debate about blockchain as a possible technological solution to existing issues around data management, digital identity, and unequal power and information-access relations. Furthermore, the discussion on the sociotechnical imaginaries of data ownership and the role of technology (to be presented in Chapter 7) explores how different actors envision blockchain, along with its potential benefits and risks. Additionally, this discussion explores how such imaginaries inform society's understanding of digital transformations and contribute to a possible redefinition of the notion of data ownership in the evolving digital world. With the right understanding of sociotechnical imaginaries, societies can better anticipate the societal implications of a redefined notion of data ownership, as well as the challenges and opportunities that blockchain technology brings along.

In general, by integrating and following these sensitizing concepts, this approach contributes to a theoretical foundation for examining how actors imagine data ownership in the future, as well as for identifying and discussing the role blockchain technology might play in reshaping the understanding of data ownership and digital identity. A precise elaboration of both how grounded theory was applied within this research and the different codes and categories that were generated will be explored in the following Chapter 6.

5 Methodology

The previous chapters framed the context for this research by exploring the theoretical background, the topic of blockchain technology along with its characteristics, followed by the introduction of the conceptual framework, including key concepts such as STS and (socio-technical) imaginaries, all of which serve as the theoretical foundation for this thesis. The questions of why this research can be situated in qualitative, interpretative empirical field studies, what Grounded Theory (GT) means, and why it was applied as the approach of choice for the answering of the research questions(s), will be answered in the following. This includes the introduction of the research method "semi-structured interviews," followed by the elaboration on how this method has been applied specifically. It is important to note that before the researcher delved into the research topic, a deep understanding of both the issues around data ownership and the fundamentals of blockchain technology was indispensable and had been acquired through an extensive literature review. This understanding enabled the researcher to set the research purpose followed by the development of both the preliminary research question(s) and the interview structure (see Kaiser 2014: 55). Furthermore, the data extracted from the interviews ultimately were transcribed, analyzed, coded, and categorized utilizing content analysis guidelines, which will be elucidated in this chapter. Subsequently, the categories are linked to the existing literature and discussed in Chapter 7. This analysis and discussion will allow us to answer the research question(s) and contribute to the existing literature on blockchain applications in the data management domain. The following elaborates on this in depth, beginning with a brief introduction to qualitative research

5.1 Qualitative Research

As stated in previous Chapter 1 and Chapter 3, blockchain development and its implementation are still in an early stage. Although blockchain is widely recognized in the finance sector and in the context of cryptocurrencies (e.g. Dávila 2023; Tapscott & Tapscott 2016; Janssen et al. 2020), the discourse on its application regarding data ownership and digital identity remains vague. The topics of data ownership (e.g. Asswad & Gómez 2021), digital identity (e.g. Clarke 1994; thex.press accessed 15th August), and information-sharing systems without trusted authorities (e.g. Chaum 1981), however, represent topics scholars have been investigating for decades.

Due to limited literature on this research topic and scarce real-world examples of blockchain technology implementation for data management, the researcher decided to follow a qualitative research approach in order to answer the research question(s). This is because qualitative research is an approach of interest that allows researchers to understand what people or experts think and mean (Strauss & Corbin 1990: 11), especially when limited information about a concerning research topic exists (Kaiser 2014). Qualitative research includes any type of research that produces findings that are not derived from existing theories, statistics, or other means of quantification (Strauss & Corbin 1990: 10-11). Therefore, qualitative methods are applied for the exploration of areas about which little is known (Stern 1980) in order to build new theories regarding the research topic. In doing so, there are three components of qualitative research that researchers must bear in mind throughout the study: the data retrieved from interviews, observations, documents, records, and films (ibid. 11-12); the procedures of conceptualizing, interpreting, reducing, organizing, and relating data, also known as coding (ibid. 12); the written and verbal reports for articles in scientific journals, talks, or books (ibid.). The manner in which these three components should be addressed when conducting qualitative research, particularly grounded theory, is elucidated in the following section.

5.2 Grounded Theory

The research method applied in this thesis is Grounded Theory (GT). Developed by Barney G. Glaser & Anselm L. Strauss – introduced in their seminal work *The Discovery of Grounded Theory* (1967) – this methodology aims to develop new theories based on empirical data. Grounded theory is a qualitative research method that allows the formulation of new theories based on iterative collection and analysis of data derived from real-world cases. Hence, GT is not concerned with proving or disproving a hypothesis but rather with developing new theories based on the data collected and analyzed (Glaser & Strauss 1967). This ultimately allows for a deeper understanding of the studied phenomenon. Therefore, in GT, the processes of data collection, analysis, interpretation, and eventual theory building are closely related (Strauss & Corbin 1990: 12). Grounded theory represents a well-known approach within the spectrum of qualitative research that allows to formulate new theories based on the systematic processes of gathering, analyzing, and interpreting data. Grounded theory is understood as an approach that does not seek to build new theories by simply working in a process following distinct steps. Rather, by following an inductive reasoning process, this approach means that researchers work in a cyclical manner (ibid.). The steps of collecting and analyzing data occur simultaneously, whereby researchers aim to identify patterns and themes from which theories can be built and derived iteratively. During the open coding process, researchers generate codes by breaking down and categorizing the data into distinct categories and codes (102). Data collection should continue until the categories reach saturation, which is called *theoretical saturation* (61). Theoretical saturation means that researchers constantly compare codes and categories until no new information is emerging about a specific category (ibid.). This will eventually facilitate the development of robust theoretical concepts regarding the subject matter. Once theoretical saturation is reached, a theory based on this data can be developed. A theory derived from data "is more likely to resemble the "reality" than is theory derived by putting together a series of concepts based on experience or solely through speculation." (ibid.). Furthermore, this provides insights, enhances understanding, and contributes to the creation of a meaningful guide to action.

5.3 Reserach Question(s)

Given that social-science-studies are underrepresented in the literature on blockchain technology and its application for data ownership purposes, it is overdue to examine this kind of technology and its possible effects on societies, particularly from sociological and STS perspectives. The researcher's interests were both experts' imaginaries regarding data ownership and the ways in which the notion of DO has been and can be changed through technology. Hence, to answer these research interests, the following research questions have been formulated: Consisting of one research question and three sub-questions, the researcher kept these questions in mind throughout this research.

The research questions will be presented on the following pages and state as follows:

What are the future imaginaries of different actors within the digital economy regarding data ownership and the role of emerging technologies, such as blockchain, in digital societies?

The main research question seeks to collect data from interviews conducted with four experts who operate within the digital economy and possess knowledge that allows us to answer the research questions. Through this approach, the researcher aims to gather knowledge and comprehend the perspectives of different actors from various industries regarding the future of data ownership and the role of blockchain technology.

The following sub-questions further contribute to a better understanding and answering of the main research question.

SQ1: How might the utilization of blockchain technology affect the distribution of power over data?

According to the literature, blockchain technology entails the potential to mitigate unequal power dynamics in data-related processes. Therefore, asking experts about current applications of blockchain and their visions about future use cases in information-sharing systems, will allow us to better grasp the actual implications on existing power dynamics.

SQ2: What does blockchain technology offer or imply to digital societies in the pursuit of a more equitable digital economy?

Although blockchain prophets attribute various potentials and characteristics to blockchain, the actual implications for society are not yet clear owing to the technology's infant status. Moreover, due to some narratives of the Web 3.0 space regarding blockchain being revolutionary and facilitating democratic systems, it is crucial to examine the actual implications and outcomes blockchain might engender, as well as the contemporary issues and challenges the technology potentially addresses.

SQ3: To what extent does blockchain technology enable the creation and operation of decentralized, trustless systems?

This question aims to address whether blockchain enables the creation of trustless systems. Furthermore, it discusses the actual role of trusted intermediaries and institutions, and asks critically whether these roles can be replaced by smart contracts and code.

5.4 Expert Interview

Because the guiding research question cannot be answered simply by analyzing the existing literature, direct conversations with different experts through interviews are indispensable. This allows to directly gather exclusive knowledge from an expert (Kaiser 2014: 6), including views, opinions, and thoughts about the topic of interest. To gather information, knowledge, and imaginaries from the person who claims to have knowledge beyond “everyday knowledge” (ibid. 36), expert interviews constitute an appropriate method. For this research, the semi-structured expert interview was the preferred method. The researcher thereby followed an exploratory research approach, meaning that there were no theories or hypothesis to be proven, but rather new ones generated (Strauss & Corbin 1990). Because of that methodological approach, this thesis can be situated in the field of interpretative empirical field studies. Conducting empirical field studies, especially expert interviews, requires certain criteria to follow, which are derived from the literature by both Kaiser (2014) and Gläser & Laudel (2006), and will be elaborated upon throughout this chapter.

Before formulating the interview questions, it is crucial to operationalize the purpose of the research and, hence, the research question itself. Operationalizing in this context translates the research topic into the cultural context of the interview partner, allowing to reveal valuable information necessary to answer the research question (Gläser & Laudel 2006: 110; Kaiser 2024: 55). In other words, the researcher aims to make the research question – the underlying research problem – observable by formulating the interview questions in a way that the guiding research question can be answered (Kaiser 2014: 56). The interview questions are indeed specific but do not need to be asked in a specific order or wording, which is why the method is called semi-structured interviews (ibid. 30). Semi-structured means that the interviewer follows a flexible but focused approach, guided by a previously generated pool of questions (ibid. 35). Semi-structured interviews are designed to gather specific information that one can never access in any other way (ibid. 31). Furthermore, this method allows for targeted knowledge that is presumed to be exclusive to the interviewed person. The researcher, thereby, explores new areas and insights by asking questions either derived from the preformulated set or arising directly in the conversation (ibid. 35). Additionally, the ways in which questions are asked depend on the interview situation and can be adapted accordingly (ibid. 52). For this research, the researcher developed an interview guide consisting of eight blocks of questions applied in three interviews, including IP1, IP2, and IP4 (see 5.6, 5.7; Appendix), and four blocks of questions for the interview with IP3 (see 5.6, 5.7; Appendix).

The following eight blocks represent the main topics that the researcher attempted to cover within the conversation with IP1, IP2, and IP4: meaning of data, data ownership, quote, blockchain technology in general, blockchain technology's role in data ownership, including risks and potentials, trust, open and additional questions, and future imaginaries.

The following four blocks represent the main topics the researcher attempted to cover within the conversation with the State Secretary for Digitalization of Austria: Daten, Datenbesitz, Digital Identity und Ausblick (see Appendix).

Importantly, in generating a guideline and the structure of the interview as presented, it is crucial to follow certain guidelines. One of the guidelines is to begin the interview with an introduction to frame the whole interview setting, followed by a whole set of narrative interview questions (ibid. 63-64). Furthermore, it is important to allow the expert to not only answer the interviewer's questions but also to talk about topics that the expert considers worth mentioning and, therefore, allow room to dive-in to that as well. The interview should include an open ending in which the expert is welcomed to discuss any topics regarding the research topic that were not covered during the interview. It is important that the interviewee has the chance to speak freely, with neither constraints nor less room for answering. The less the interviewer guides the interviewee, the better, meaning that more insights and hidden information can be revealed (Kaiser 2014: 52-55). Hence, it is generally not about gathering information that is usually available to the public, but rather information that is hidden and only accessible by talking to experts from a specific field (ibid. 31). Furthermore, the researcher must work in theory-guided mode. This means, on the one hand, that answering the research question always needs to stay in focus, while within the subsequent analysis, the researcher links its prior knowledge about the subject matter with the findings (ibid. 6-7). This, at the same time, also represents one of the core quality criteria of qualitative expert interviews (ibid. 144). It is important to note that to ensure that the collected information is suitable for subsequent analysis, the researcher must carefully consider the questions in advance. Hence, the researcher cannot simply ask questions randomly. The questions should be semi-structured and ordered in a logical manner to address particular topics. However, as already mentioned, the order of the questions can vary but ought to be inherently coherent. In addition, it is vital to be aware of neutrality and openness regarding the research findings as well as other systems of relevance and patterns of interpretation (ibid. 9). Thus, the questions must not be biased or influenced by the researcher's standpoint or personal experience. Any emotional attachment or personal convictions can therefore be particularly threatening and counterproductive for both the interview situation and the analysis, and ultimately the research itself (ibid.). Objectivity, for these reasons, is not only essential within the interview process but rather throughout the entire research process. Objectivity, besides theory-guidance, represents one of the core criteria of interpretative social sciences (Kaiser 2014). The last criterion is known as the intersubjective comprehensibility of the data collection and analysis procedures (Kaiser 2014: 6), meaning that the researcher needs to disclose every process from collecting data to its analysis and interpretation so that others can comprehend the individual course of actions.

5.5 Sampling

To answer the research question(s), the researcher decided to conduct semi-structured interviews with actors engaged in either blockchain technology (for data ownership and/or digital identity purposes) or topics related to data ownership and/or digital identity. The final sample consisted of four experts within the fields of politics, economics, and sciences. The information obtained from these experts was categorized using Mayring's data analysis (2010) and will be discussed later in Section 5.6.

An important part of this research was the expert selection process. This required reflective thinking, as randomly selecting experts might lead to distortion of the research processes (Kaiser 2014: 70). Therefore, the methods by which experts should be selected, as well as the criteria determining expert status, represent two core aspects that require critical consideration. Before describing the individual interview partners and the ways in which they were contacted, it is crucial to define who is eligible to be an expert for an interview. An expert is considered to be an individual who possess certain privileged information and responsibilities that are needed to answer the research question and, therefore, find „solutions“ to the researcher's subject (Pfadenhauer 2009). The experts eligible for this research were selected from the fields of politics, economics, and sciences. The reason for this broad sample, spanning across different fields and industries, is that imaginaries in general are "not limited to nation states but can (also) be articulated by other organized groups, such as corporations, social movements, and professional societies." (Jasanoff 2015: 456) Therefore, the research question itself – concerning the imaginaries of different actors regarding data ownership and the potential role of blockchain technology – was formulated in a way so that it does not limit the diversity of potential interview partners. Interviewing such a diverse sample, as presented later, allows for a better understanding of what actors with different backgrounds and professions envision in terms of data ownership and blockchain technology application. This reveals insights into how the topic is perceived across industries and fields. By considering, analyzing, and comparing the experts' individual experiences and imaginaries, a broader discussion about the topic can be facilitated, eventually leading to newly generated knowledge, theories, and avenues for future research. For this research, the researcher selected experts who either work on blockchain technology-related solutions concering data ownership or on topics related to data ownership and/or digital identity. This selection was made because both groups represent experts who possess relevant insights and, therefore, contribute adequate knowledge to this study. In other words, that data derived from the experts either contributes valuable information to the general understanding of data ownership and digital data management or fills the gap in the literature regarding blockchain technology application for data ownership use cases. Hence, one of the researcher's aims was to contribute to the existing literature by providing insights from experts within the digital economy who have either experience with blockchain technology, data ownership, digital identity, or all three. These considerations, together with extensive literature research, led to the final sample of interview partners. The final sample consisted of actors with backgrounds or active roles in politics, sciences, and business. The potential interview partners were contacted through different channels. Some were contacted through contact formulas on their websites, some via LinkedIn, and others through third contacts and e-mails. Altogether, the researcher contacted 15 potential interview partners. However, only six replied, of which only four agreed on doing an interview. Hence, the final sample for this research consisted of two actors from economics, one actor from Austrian politics, and one from the sciences:

5.5.1 Economics

Interviewing actors who operate as business owners or product developers provides valuable insights into the realm of real-world applications. The first interview was conducted with the Product Growth Manager at Ocean Protocol. This company was chosen because of its already mature phase of developing an infrastructure for users who aim to own digital data by themselves. The second interview was conducted with the CEO of a digital identity company, which is currently in the beta phase of providing a digital infrastructure in which users verifiably own their data. The reason for interviewing these two actors is predominately the valuable insights into their practices, but also the challenges they face in the real world. Furthermore, their individual motivation and approach significantly contribute to a better understanding of how different businesses operate in building and providing solutions to existing issues regarding data ownership. Since businesses often drive innovation (Smith & Stirling 2018), interviewing them allows to further identify trends and explore real-world applications together with their hurdles, as well as potential future areas for research. Real-world examples also make technologies more tangible for others, which ultimately facilitates a better understanding of where and how such technologies can be applied and what their impacts are.

5.5.2 Politics

Claudia Plakolm, Austria's current State Secretary for Digitalization, was the third person interviewed. The State Secretary's expertise and vision of Austria's future are valuable contributions to the discussion around data management. For this thesis, this is an important perspective to consider, particularly because governments typically seek to manage and provide their services in a centralized, top-down manner, acting as intermediaries, as seen with Austria's initiative called ID-Austria (oesterreich.gv.at, accessed 18th August). Whereas the blockchain narrative originally stems from a more decentralized, bottom-up approach, eliminating intermediaries and central actors (e.g. Semenzin et al. 2022: 2). This represents an ambiguity that results in blockchain being envisioned in multiple and often contradictory socio-technical imaginaries (see Jasanoff & Kim 2015). A governmental standpoint therefore brings a controversial and more objective perspective into the discussion, allowing us to examine whether we need blockchain technology for data ownership at all, whether data ownership is manageable only by governments and in a top-down manner, or whether there are even synergies and possibilities in merging these two.

5.5.3 Sciences

Interviews with scientists in this field allows us to deepen and enrich the research thanks to their interdisciplinary perspectives and knowledge. This is particularly crucial, as the topic of data ownership itself intersects with various disciplines, such as computer science, social sciences, law, and ethics. Combining these perspectives can further encourage discussions about, for instance, data privacy, accountability, technical implementations, and limitations or consent, which eventually helps to identify and guide future areas of research. A Senior Researcher at the Austrian Blockchain Center was chosen for the final interview. Although the expert's research focus is primarily not data ownership, the expert was selected due to the deep understanding of the technical aspects of blockchain and the broad overview of current research trends the expert possesses, providing a critical academic perspective on the subject matter of this research.

5.6 Expert Interviews

The four interviews were conducted over a period of five months, from March to July. Two of the interviews were conducted online via Zoom, while the other two were conducted face-to-face. The rationale for conducting two online interviews was the geographical location of both interview partners at the time of the interview. The other two face-to-face interviews took place in Vienna: the one with State Secretary Plakolm at the Bundeskanzleramt; the other one at the Austrian Blockchain Center.

Three interviews were conducted in English; the one with State Secretary Plakolm in German. All four interviews were recorded using voice memos. The two online interviews, furthermore were recorded via screen recording. The researcher stored and handled all recordings ethically and with great care. After each interview, memos were produced for better comprehension.

The first interview was with the Product Growth Manager. Ocean Protocol is one of the leading companies in the data ownership realm, providing a digital infrastructure and a marketplace that allows users to actually own their datasets by leveraging blockchain technology and smart contracts. The interview took 1 hour and 22 minutes.

The second online interview was conducted with the CEO of the digital identity firm. Notably, due to the interviewee's talkativeness and subsequent temporal constraints, the interview had to be split into two sessions conducted on consecutive days. The first part took 1 hour and 38 minutes; the second part took 1 hour and 8 minutes.

The third interview was conducted with the State Secretary for Digitalization of Austria, Claudia Plakolm. The researcher was invited to the Bundeskanzleramt to conduct the interview and was granted nearly one hour to discuss and ask the State Secretary about her visions on data ownership, national projects such as ID-Austria, and the role of both technology and trust in establishing robust information-sharing infrastructures.

The final interview was conducted with a Senior Researcher working at the Austrian Blockchain Center (ABC Research GmbH) in Vienna. The interview took 1 hour.

5.7 Transcripts and Research Ethics

Subsequent to the interviews, the researcher used the recordings and additional memos to transform every interview into a transcript. Notably, the transcripts were generated with the help of an AI software tool specialized for transcribing interviews, which had overall its benefits in terms of efficiency improvements. The researcher proofread all of the transcripts generated by the AI tool carefully. It is important to note that the interview with State Secretary Plakolm was neither uploaded to the AI transcription website nor transcribed with the AI tool; a decision made based on the researcher's ethical considerations regarding integrity.

Regarding the anonymization of the interview partners, the researcher presented a consent form and asked the experts to read the form, tick the options of the statements they agree with, and sign the document. The statements the experts could choose from included four options: I wish to review the notes, transcripts, or other data collected during the research pertaining to my participation; I agree to be quoted directly; I agree to be quoted directly if my name is not published and a made-up name (pseudonym) is used; I agree that the researchers may publish documents that contain quotations by me (see Appendix). Even though the experts, except one, agreed upon using their names directly for quotations, the researcher decided to use only the expert's role for better understanding and readiness of the presentation of the results and the discussion overall. Only the name of the State Secretary for Digitalization is used and quoted directly.

Given the guidelines for anonymization, pseudonymization, and the agreements within the consent form, the following codes were generated for the presentation and discussion of the interview results:

Interview partner = IP

IP1 = Product Growth Manager (Ocean Protocol)

IP2= Chief Executive Officer (CEO) of a digital identity firm

IP3= State Secretary for Digitalization of Austria, Claudia Plakolm

IP4= Senior Researcher at Austrian Blockchain Center (ABC)

5.8 Generation of the Coding System

Following the transcription of the interviews, the researcher anonymized the interview partners by assigning their active roles. The next step, preceding the actual data analysis, involved the development of a coding system to facilitate the intersubjective comprehensibility of individual expert statements and allow for a better overview of the data collected from the interviews.

The software applied for the generation of codes is MAXQDA (Version 2024). This software allows to code the material, which means to link categories with text segments from the data. To do so, a coding system is indispensable and represents the central tool for the analysis (Mayring 2010: 49). This coding system served as the foundation for the subsequent analysis. 12 main categories were generated deductively, which required an operationalization process. In this process, the categories were derived from the researcher's considerations based on the literature reviewed and the available information. Subsequently, this contributed to the generation of the following 12 main categories (Mayring 2010: 83): Data, Web 2.0/Traditional Internet, Centralization, Decentralization, Power, GDPR, Data Ownership, Trust, Web 3.0, Digital Identity/DID/SSI, Blockchain Technology, Outlook (see Chapter 6 Fig. 7).

The next step involved delving into the raw data and linking the text segments that are relevant for the overall answering of the research question with the deductively generated codes. During this analytical process of linking raw data to the main categories, according to Strauss & Corbin (1998), the researcher identifies concepts and their properties (Strauss & Corbin 1998: 101-102). Based on this, the researcher inductively develops new sub-categories (Kaiser 2014), which pertain to a specific main category, "giving it further clarification and specification" (Strauss & Corbin 1998: 101). This process is also called "open coding" and means "data are broken down into discrete parts, closely examined, and compared for similarities and differences" and ultimately grouped conceptually "under more abstract concepts termed categories." (Strauss & Corbin 1998: 102) Thereby, the researcher strives to "open code" without any biases (Mayring 2010: 84), which ultimately contributes to gain more theoretical quality (Kaiser 2014: 116).

In sum, with the help of MAXQDA (Version 2024), the researcher developed 12 main categories deductively and 20 sub-categories inductively (see Chapter 6 Fig. 7), which ultimately allows us to inductively conclude and develop theories (Mayring 2000).

5.9 Data Analysis (Mayring 2010)

The qualitative content analysis developed by Mayring (2010) represents another crucial part of qualitative research that was conducted after the interviews were transcribed (Kaiser 2014: 98). Qualitative analysis in general, according to Strauss & Corbin (1990), is a "process of interpretation, carried out for the purpose of discovering concepts and relationships in raw data and then organizing these into a theoretical explanatory scheme." (11) It is a balanced interplay between researchers and data (13). Analyzing content is one of the most crucial aspects of research. Although there are different methods that can be applied, the researcher decided to apply Marring's (2010) content analysis for this research. The content analysis by Mayring (2010) allows to further deepen, analyze, discuss, and connect the individual information to make final assumptions. The results of such analysis serve as the foundation for answering the research questions. As mentioned, it is important to note that qualitative research studies do not follow any hypothesis but rather are guided by a specific research question, which the researcher consistently considers throughout the study (Kaiser 2014; Mayring 2010; Strauss & Corbin 1990). For this thesis, interviews represent the appropriate method to answer the research question(s). Given the multifaceted and diverse nature of information gathered from interviews, the content analysis by Mayring (2014) represents an effective method for a step-by-step reduction of that information. Subsequently, that information can be categorized, thereby facilitating inductive conclusion and acquiring knowledge. Through the analysis and summarizing of the content as presented, a direct comparison between the interviews becomes possible, allowing for the extraction of similarities and disparities. Particularly regarding topics about which little is known, Mayring's (2000) content analysis facilitates both the discovery of novel information and the development of theories. For these reasons, Mayring's (2000; 2010; 2014) content analysis was selected as the appropriate method for analyzing the subject of data ownership and the role of blockchain technology, as well as for developing new theories in this regard.

6 Results

The following chapter explores the raw data collected from four distinct interviews and presents a structured overview of 12 inductively developed main categories along with 20 inductively developed sub-categories (Fig. 1).

Categories are the "cornerstones of a developing theory and provide the means by which a theory can be integrated." (Strauss & Corbin 1999: 7) Overall, categories help to find similarities and disparities within the raw data, which ultimately allows to inductively conclude, gain knowledge, and develop theories (Mayring 2000). In the following chapter, the categories serve as a guide for connecting and presenting the results, facilitating the intersubjective comprehensibility of the connections between the experts' statements.

In addition to the categories, recalling the main research question from Chapter 5 - "What are the future imaginaries of different actors within the digital economy regarding data ownership and the role of emerging technologies, such as blockchain, in digital societies?" – will further help to navigate this chapter.

In presenting the interview results, the researcher decided to use pseudonyms, except for the State Secretary's statements (see Chapter 5). All four experts are cited using either their roles or the following identifiers:

Interview partner = IP

IP1 = Product Growth Manager (Ocean Protocol)

IP2 = Chief Executive Officer (CEO) of a digital identity firm

IP3 = State Secretary for Digitalization of Austria, Claudia Plakolm

IP4 = Senior Researcher at Austrian Blockchain Center (ABC)

DATA
- Definition
- Meaning for Societes
- Kind of Data

WEB 2.0/ TRADITIONAL INTERNET

CENTRALIZATION

DECENTRALIZATION

POWER

GDPR

DATA OWNERSHIP
- Description and Meaning
- Who owns the Data
- Imaginaries
- Quote
- Problems and Issues

TRUST
- Technology Aspect
- Governance Aspect

WEB 3.0

Digital Identity/ DID/ SSI
- ID Austria

BLOCKCHAIN TECHNOLOGY
- Definition
- Characteristics
- Applications
- Imaginary
- Smart Contracts
- Risks & Concerns
- Benefits & Advantages

OUTLOOK
- Trends/ Current Developments/ Future Research
- Imaginary 2050

Figure 7: Results Overview (Own Representation)

6.1 Data

One of the most commonly used terms in this thesis is data. Every interview partner uses this term on a daily basis, though, its “Definition” and understanding diverge among the experts (IP1:4,10,16; IP2:7; IP3:4; IP4:4). The Product Growth Manager explained that data is not exclusively digital, existing in the physical world, and independent of digital devices (IP1:4). The expert defined data as any information that aids in decision-making and enhances accuracy in daily activities (ibid.). Similarly, State Secretary Claudia Plakolm explained that data can appear in various types and formats, including numbers, text, pictures, statistics, and information, both structured and unstructured. The State Secretary stated that data basically represents both the most important resource within our society and the foundation for progress and economic progress. Additionally, data is used for improvements in efficiency and decision-making on a daily basis and entails great innovation potential (IP3:4). The CEO of the digital identity firm emphasized that data could mean different things and stressed the difference between personal and commercial data (IP2:7). Similarly, the Senior Researcher at the Austrian Blockchain Center (ABC) argued that there are different aspects of data, including work-related data, personal or medical data, and data for research (IP4:4).

Regarding the **"Meaning of Data for Societies"** State Secretary Plakolm stated that data plays a crucial role in today's society, which stems from her belief that data is both an information carrier and a driver for efficiency and progress. Furthermore, data can be considered a resource that must be handled with caution (IP3:4,6). One crucial aspect that the State Secretary referred to is the "area of conflict" between data security and data protection. This area of conflict emerges as a conflict between data usage and data protection/security, between effective use of data and the methods applied for data analysis and processing. The State Secretary believes that these aspects are crucial for innovation and efficiency improvements in various sectors (IP3:4).

In the context of advancements and improving processes, the Senior Researcher explained that we are living in an era of AI taking over many processes, which generally requires a lot of information because AI is data-driven (IP4:8). Moreover, data is needed to train such AI models, as described by the expert in regards to medical data: "When you have a lot of data, you can see which behavior caused which disease and which medication works the best" (IP4:8). The expert concluded "(…) it (data) is like the basis to improve processes. I think not only with AI but also with conventional research." (ibid.)

AI development, the processes of digitalization, and other technological developments have been happening dynamically at an increasingly rapid pace, as the State Secretary stated (IP3:18). Recent developments in AI and ChatGPT allow users to better assess the impacts of using such tools. The primary premise in the usage must be that transparency, security, and safety are always guaranteed (ibid.). In contrast to what State Secretary Plakolm stated, the Product Growth Manager presumed that "people do not really know what data is" (IP1:12), though they share their data because they believe to get something back of value, not necessarily in monetary terms but also emotionally (IP1:8). Similarly, the Senior Researcher stated that people share their data with large platforms out of convenience and they do not really understand the effects, which represents the problem of today's society (IP4:12). The expert added, "That's the problem. People are not much aware or if they are aware they may not care about it too much, at least a majority and say, okay, I don't have anything to hide." (IP4:12)

6.2 Web 2.0 and the traditional Internet

In Web 2.0, businesses that built their business models around data monetization operate on the traditional Internet and lock the data into centralized databases, which is only accessible "partially with email and a password" (IP1:16), ultimately making data the property of those businesses (IP2:7). The CEO of the digital identity firm described the difference between owning information in the physical world and digital world: "in the physical world, you are the owner of the information (…) you have the power to selectively disclose your information" and the ability to show, for instance, the driver's license whenever it is required. "My driver's license is in my control (…) not in the control of other people" and in the digital world "we don't have that" the expert added (IP2:9). The reason for this is, according to IP2, that the Internet was created to connect a small number of computers and was not designed for what we have today, namely that the Internet nowadays is used by the world population, international commerce, and the economy. The missing piece here is the trust or identity framework as it exists in the physical world (IP2:9). The expert explained that "with my passport in the physical world, I can travel to other countries, I can cross the boarders, I can go to a bank and identify myself" and such a system does not exist in the digital realm (ibid.). Moreover, every time a "relationship" is being established in the digital world, a new identification process is needed, together with new credentials. This is what companies of traditional Web 2.0 are doing: to create their own trusted framework to which everything is tied and "if you jump to another bubble – you go to Uber – you have to recreate exactly the same and this is because in the Internet or digital space we don’t have a layer, a common layer to deal with trust and identity.” (IP2:9) Now, according to the expert, “if we remove most of that (…) trust framework from Amazon or Uber,” by implementing a digital identity layer, “we are removing part of the value they created,” which would cause trouble as they would need to switch to another business model (ibid.). This is why the CEO stated that there is a lot of resistance of these companies such as Google, Amazon, and Facebook, but other companies who have not worked on data monetization over the last decades, such as Microsoft, are now working on a digital trust framework, self-sovereign-identity, or similar solutions as they see this as an “opportunity to do a new business but also (…) to do some damage to their competitors.” (IP2:9)

6.3 Centralization and Decentralization

Within these bubbles, as the CEO named it, the Senior Researcher argued that people accept the terms and conditions without really thinking of the consequences, which allow the firms to track users’ actions and behavior within this environment (IP2:41; IP4:12). This can lead to a “transparent citizen” as seen in China; people are surveilled (IP3:12), which ultimately reduces the freedom of the individual, the State Secretary emphasized (ibid.). These governments or big companies store and manage data (IP1:16), and therefore know what users are doing or thinking, which may eventually be used against them in the future. This is what the Product Growth Manager argued to be “the main problem at the moment with these big providers” (ibid.) In addition to that, the Senior Researcher explained that data in today’s world is not really connected, meaning that “you have data on Facebook, you have your data on Microsoft” but if the user wants to connect them it is “difficult” (IP4:12). This, together with the aspect of surveillance represents possible issues of **“Centralization”.** For these two reasons, the Senior Researcher stated that a “decentralized approach of data ownership might be interesting.” (IP4:12)

The Product Growth Manager described **“Decentralization”** as a “public good,” meaning that it is “something that is run by the people” and “things are working (…) because people make them work.” (48) The expert added that “decentralization actually provides an extra layer of stability if it’s sufficiently decentralized” (ibid.), however, we are still far away from “sufficiently decentralized” but “not too far” (ibid.). In this context, the CEO stated that when information or databases are decentralized, it “is at least more difficult” to attack them; the attacks are being more desensitized (IP2:46). The expert further explained that this is because, “if you hack a huge database, the benefit is huge, but if you need to hack every person in the world, probably the cost of the attack is bigger than the benefits that you have.” (IP2:46)

One crucial finding for the answering of the sub-research-question 1 regarding the implication of blockchain on the distribution of power (SQ1) is that decentralization fixes “at least partially the concentration of information and the control of the excessive control of information (…) so it’s going to undermine a part of the power that big players have today”, according to the CEO (IP2:82). Besides these opportunities of decentralization, the Senior Researcher mentioned critically that decentralization comes not without “**Problems**”. The expert compared Web 2.0 “where you have the big corporations” and Web 3.0 where “the power goes back to the individuals.” (IP4:20) Problems thereby may arise, because the majority of the people in Web 3.0 might not always be best educated in the field “so if you (…) ask the people how they want to share their data and you make a (democratic) vote on it, maybe you don’t get the best result because people are not informed.” (ibid.) Therefore, the expert added, there is always some sort of “compromises,” so it might would make sense if this vote happens in combination with regulation by the government (IP4:20).

Another problem and concern the Senior Researcher mentioned is fake news, which, in a decentralized world – where everybody can post anything in a forum such as Reddit – are difficult to identify as such. This would require some sort of reputation system to counteract manipulation and fake news, in which, for instance, timestamping a picture and storing it as a hash on a blockchain could be a possible solution (IP4:31).

When it comes to governmental services that manage the data of a country’s citizens, such services are typically provided in a centralized, top-down approach. This, if done inappropriately, could have severe impacts on societies and is considered very critically by the State Secretary (IP3:12). IP3 further argued that such systems, as seen with the Social-Credit-System in China, only serve to surveille individuals (IP3:41), and AI implemented within such systems is used without any ethical or moral principles (IP3:12). Therefore, the State Secretary is convinced that the adopted EU AI Act is a promising counterexample to the Chinese model because it is the first legal framework for AI that puts the human at the center and discloses where and how to use AI, opening up great potential (IP3:12). This, along with the ID-Austria initiative, are considered to be the fundamental differences between Austria and a Social-Credit-System as it exists in China (ibid.).

6.4 Power

Giving the power over information back to the people by utilizing technology represents one topic of interest described by every expert across different contexts and explanations (IP1:34; IP2:52; IP3:10,12; IP4:20) The topic of power will be discussed in Chapter 7.

6.5 GDPR

While discussing the regulation of data privacy, the Senior Researcher mentioned the **“GDPR”** (IP4:20). The expert believes that the GDPR needs to be adopted better to the decentralized world since blockchain is not sufficiently targeted within. The expert explained that there are “a lots of problems when we try to find decentralized solutions that are GDPR compliant because in HTTP, I always have the rights to delete data and basically you can call the company and say, you have my data, please delete it, but in blockchain you cannot do it by design because blockchain is immutable and should be immutable”. Moreover, “if you start editing from a blockchain, then you’ll lose this kind of trust because you don’t have this cryptographic proof anymore that everything was in order.” (IP4:20)

The State Secretary for Digitalization of Austria (IP3) also elaborated on the GDPR and “Datenschutz-Grundgesetz,” which she believes to be crucial guidelines that are needed for making the processes of data processing accessible, for making use of the potentials, and for guaranteeing transparency when it comes to the usage, processing, and curation of personal data (IP3:8). When the interviewer asked about the principles that should guide debates about data, the State Secretary explained that the fundamental rights and the common good of the users, together with the protection of privacy, freedom of expression, and other democratic principles, must always be secured and ensured (IP3:10). Another principle State Secretary Plakolm considered crucial is the one of data sovereignty, meaning that individuals have to have control over their data and to be informed about what happens with it and where it is available (IP3:4,10). Furthermore, it is about the quality of data, which IP3 emphasized as highly important. IP3 also referred to the idea of minimizing data as another principle, meaning to focus only on what is needed while guaranteeing transparency so that people can comprehend the processes (IP3:10).

6.6 Data Ownership

As explored in Chapter 4, data ownership has no unified definition, nor is it understood equally among the actors (4.4). The **“Definition and Meaning of Data Ownership”** also diverges among the interviewed experts. The Product Growth Manager of Ocean Protocol stated, that “whoever produces the data owns it” (IP1:14), and after describing a theoretical example regarding mining gold and owning land, the expert argued that – “in a capitalistic way” – “the owner of the data is whoever can use it better” (IP1:14). However, according to the expert, this is perceived to shift as societies gain a better understanding of what data is. The reason for this is that societies are becoming a bit “greedy in the sense that they want to be more attached to what they are producing.” (ibid.) The expert (IP1) used the term “produced” with caution as people do not, “realistically speaking” (ibid.), produce it but contribute or provide it. This is where it gets more “complicated” (IP1:14), because an organization, for instance, to which the data is provided “is providing insights and is doing all that stuff that costs money and time and knowledge (…) and so data is basically owned by both.” (ibid.) The question of **“Who owns the Data,”** is therefore an “ambiguous situation,” as IP1 explained. The CEO of the digital identity firm argued that at this point of time “the data belongs to the platform, because you gave the consent to do that” (IP2:41) The expert added, “today, we are operating in an unregulated space (…) there is no rules about the ownership of data on the Internet” (IP2:44). The Product Growth Manager described the ways in which data ownership is managed. It is managed in that sense that data is locked into centralized databases, only accessible “partially with email and a password” (IP1:16). Therefore, the specific email and password do not work with another database or platform and are “siloed within their own” which makes it more difficult to define who owns the data (ibid.).

State Secretary Plakolm **defined data ownership** as a dataset on which – metaphorically speaking – someone sits (IP3:8). Additionally, according to the State Secretary, data ownership refers to whoever and how someone controls the dataset, including the usage, storage, application, and processing of such; also, the legal abilities to decide how and for what the data can be processed and used for (IP3:8).

A core distinction highlighted by the Product Growth Manager is that data itself has multiple ownerships; privacy, in contrast, has only one ownership. In addition to that, IP1 stated that there is a difference between owning data and what you do with it (IP1:16). The CEO stated that within the digital identity space, the concept of “My information is mine” is being pushed forward. Interestingly, what the expert sees is a shift where governments and institutions, such as the World Bank, are getting on the same page and pushing this concept (IP2:7). “Personal information is property of the person” the expert argued (IP2:7), but stated that within the commercial sector, there is some resistance to this. This, as the CEO of the digital identity firm explained, is because many businesses of today are based on data monetization, therefore, it is not convenient for them to change the definition and start considering personal information as something that is not their property (IP2:7). The expert is “particularly sure” that this will change within the next 3 to 5 years, since the expert believes, that “for many governments the answer is: the ownership of data is in the person” which made him envision the scenario in which “big technology companies will be forced to adapt their business models to this new reality” (IP2:7).

The expert’s future **“Imaginaries”** of data ownership and the tools that are needed for building systems in this regard, represent the main topic of interest for the answering of the main research question, and state as follows: The Product Growth Manager considers besides a narrative or cultural shift also technology as essential for the future of data ownership (IP1:18,20). After technology adoption, which initially causes discomfort within society, a cultural shift follows. A better understanding of technology usage ultimately brings about a cultural shift (IP1:20).

Regarding the imagining of blockchain applications for data ownership use cases, the expert explained that cryptography, specifically combined with Web 3.0 and blockchain, are important tools. They effectively allow users to encrypt and decrypt data with consensus and traceability (IP1:18). This, ultimately, provides a “full spectrum of tools” and allows users to decide whether to share their data or not, whether to decrypt it or not. Additionally, with such a toolset of technologies, users know what happened with their data, who used it, how much it was used for, and for what purposes (IP1:18), referring to the idea of **self-sovereign identity**, which the Senior Researcher in the interview referred to as a “movement” (IP4:14).

The Senior Researcher at the ABC envisioned that “in an ideal world, I think it might be good that you have the control over your own data” but at the same time the expert also highlighted potential risks, noting that this comes with high responsibility when storing and controlling all personal data on a single server – this poses the risks of data loss (IP4:14). The expert then further promoted the conceptual idea of self-sovereign-identities, and argued that through SSI a person could give “selected companies or persons access“ to the datasets, reaching from medical data, to specific confirmations, financial or work-related data, to certificates (IP4:14). The expert added, that any kind of data “should be controlled by the person who is affected” (ibid.). However, this is not always clear, as many people can be involved or affected, such as in cooperations or within research groups (IP4:14). For the Senior Researcher, SSI or a decentralized approach of data management is the “more natural approach” as you don’t give the power into the few companies where it is not clear or disclosed what happens with the data in the background (IP4:16). The expert envisioned a system in which, for example, a doctor needs to ask for permission to access a person’s medical history and the owner of the data decides whether to permit access or not; similar to what happens today when an app asks for permission to get access to contacts or the camera (IP4:16). In addition, the Senior Researcher argued that this technological approach would decrease the hurdle of data management, as it clearly shows what kind of data is being used, for how long, and for what purpose (ibid.). However, this is not something that could be done from one day to the next, as it requires regulations and acceptance of different parties involved, the expert emphasized (ibid.). The expert then explained that this could be done, for instance, managed by a centralized server. However, this entails the risk of mistrust or corruption, which is why the Senior Researcher mentioned encryption as one possible solution in order to have some sort of control. Blockchain technology does not solve this alone and is “not the sole solution,” because it is not meant to store sensitive or huge datasets, but it rather can be used as an “addition” for coordination purposes or incentivizing users to share their data and get paid for sharing and providing data (IP4:16).

The Product Growth Manager of Ocean Protocol described his understanding of sufficient decentralization as a future imaginary in which phones are connected to a decentralized network of nodes, which in turn run as validators on the phones securing the network. The expert hopes that, in the future, decentralization allows devices to connect to a decentralized network in a way that there is really a zero point of failure (IP1:48). The expert further explained that traditional Web 2.0 “log in with Google thing” (IP1:52) is not portable in the sense that the user cannot take the data stored with this specific password and username to another log-in account (e.g. Meta) (IP1:16). For this reason, the expert hopes for a catalyst and imagined a solution that allows users to sign in with Ethereum as the smart contract protocol integrated with either Ocean Protocol or any other decentralized identifier (IP1:52). This, ultimately, eradicates the traditional "log in with Google thing" and paves the way for users to port their data from one app to another which the experts described as "a really interesting next step to bring decentralization and data together (…) for people." (ibid.) Similar to the aforementioned toolset of technologies –blockchain and cryptography in particular – this new sign-in with Ethereum solution will facilitate and bring forth a novel idea of data ownership among the people. This will probably happen in an indirect way because "people do not care about the technology (…) same as it is with WhatsApp or Google Meets" the CEO imagined (IP2:103).

The question regarding the mentioned "**Quote**" during the interviews – "If we want to prevent the concentration of wealth and power in the hands of a small elite, the key is to regulate the ownership of data" (Harari 2019: 93) – was answered by three experts. The Product Growth Manager explained: "I think it means that he (Harari) assumes that the owners of the data are the people. And um and so what he is hinting to probably is the people are selling their data to companies that want to use it (…) agreeable, disagreeable." (IP1:24) This is why the expert believes that in order to regulate that, a "feasible business model" is needed (IP1:26). However, according to the Product Growth Manager, the reason for why such a business model has not been developed yet is because of both "legacy" – things are working perfectly fine – and a missing cultural shift which takes time (IP1:26).

The Senior Researcher agreed on the quote and explained "for sure there's some truth in it"; due to concentration of data one has the power, "but it's not only the data (…) also you need to have capital, so it's still like a capitalistic world so without some starting capital the data is difficult to exploit" (IP4:18). The expert added, "I think that's what he (Harari) means, like who owns the data basically has like the power to exploit the data and decide what can be done with it" (ibid.). Furthermore, the expert described, that if we can break these companies who focus on data monetization – the expert referred to the term "monopolies" – "then it might be a more fair and democratic society (…) because people (then) could decide for themselves what to do with the data, maybe even monetize their own data and have like some income and not only share their data to get some kind of services like Facebook or Google for free, but also to have like some kind of income (…) or like some kind of extra benefits to share their data." (IP4:18) The CEO of the digital identity firm in this context envisioned that not in the near future but in the coming years, the business model wherein users pay with their privacy and information will switch to another model in which users monetize their data, co-existing with other models (IP2:41). This Web 3.0 model will not "kill" the other models, same as Web 2.0 did not kill Web 1.0 (ibid.). What is important, according to the CEO, is to find those ways that create the highest level of experience for the users, as we transition from the information economy further deeper into the experience economy, without having the users pay with their privacy (IP2:41). Companies that compete for the best experience for their users are what the CEO envisioned to be the core topic of interest of capitalism and the focus of new business models in the future, rather than data (IP2:82) "We are transitioning to a new form of capitalism – capitalism of experience" the expert argued (ibid.)

6.7 Trust

The topic of trust represents another essential aspect when discussing data ownership, blockchain technology, and digital identity services. Answers to sub-research question 3 (SQ3), will be primarily derived from the results presented in this section: the experts were asked about the role trust plays for them personally in today's digital world. Technologically speaking, the CEO described the importance of a trust framework: in the physical world, to enter a country, humans need to identify themselves with a passport – representing one part of the technological aspect – which is only valid through a specific governance framework – representing the governance aspect (IP2:18). These two aspects are crucial for the successful functioning of the trust framework, the expert explained. In other words, a person identifies with a passport that needs to be verified by someone authorized to do so for it to be a valid passport. Hence, to create a digital passport on the Internet on the new identity layer, according to the expert, it is both the technology and the governance aspect that are essential (ibid.). Additionally, within the governance aspect "the most important aspect are the trust registries," which are trusted entities that verify credentials, certificates, or passports (IP2:18-28). The CEO concluded that this is why technology is not going to create trust in the digital world. Furthermore, trust is never going to be purely technological, highlighting the need for "the human part in these equations." (IP2:95) Trust, the CEO further argued, is a human belief which you cannot simply put into a smart contract (ibid.). The Senior Researcher stated something similar to what the CEO described regarding the two complementary aspects, noting that although ”blockchain can be used as a trust layer” (IP4:20) to prove something, it is not the core solution for a trustless system, but rather a useful addition (IP4:16). Hence, the Senior Researcher explained that blockchain could help build a reputation system (IP4:31) based on timestamping, where “you can demonstrate that something is truly from a specific source and truly from a specific date (…) it can help, but it’s not the sole solution.” (IP4:33; see IP1:18-20).

When speaking about trust from a human perspective, the Product Growth Manager explained: “I think trust is fundamental but it's (…) really not being taken as, as it should.” This stems from the expert’s assumption that people trust everying they see because “people are lazy” (IP1:58). For this reason, the expert suggested that “we need solutions that really put it (trust) in front of their face” such as the Twitter verified badge or KYC (know-your-customer) verification symbols, allowing to show people who and where to trust (IP1:58). Regarding the question of whether people can trust centralized firms, banks, and governments dealing with personal data, the Product Growth Manager stated that, even though people and organizations change over time “I think we can trust them” and with enough confidence and for the better of the world “you should trust them” (IP1:60). The reason for this, the expert argued, is that people actually do not trust themselves and assumed that if “you have a million dollar in your bank (…) you still give it to the bank instead of keeping it at home because you trust them more.” (ibid.) The expert then mentioned the topic of self-custody, which refers to one of the core ideas within the crypto space and means that no one else should have the access keys to the cryptocurrencies except the one who owns it. In this context of holding “money,” the Product Growth Manager added that one has two choices: first, a person holds everything self-custody using a 12 word-secret-recovery-phrase (more in Chapter 7); and second, a person trusts someone else to manage and store the money, as with traditional banking. The expert stated: “People don’t trust themselves, they really don’t. So yes, you should trust them because if you don't trust them and you don't trust yourself, then what are you going to do? (…) But yeah, depends on, depends on the person.” (IP1:60)

From a governmental perspective and in regards to the previously mentioned “area of conflict”, the State Secretary explained that it is crucial to ensure that people trust the processes of analyzing, processing, and using data performed by governments. It must be guaranteed that people who provide their data can trust the processes and see what happens with their data at any time (ibid., 10). Therefore, the principles of data protection and transparency are considered to be core aspects, especially when it comes to services that require trust and are provided by governments (IP3:10). The State Secretary explained that such governmental services and other administrative services process a lot of data, which is why trust plays a vital role (IP3:12). Furthermore, it is important that people know their data is stored and processed securely, which is why transparency is also crucial (IP3:10). The best services and the most efficient administrative channels are worthless when people do not trust these services and the ways in which data is being processed, the State Secretary added (IP3:10).

6.8 Web 3.0

The idea of Web 3.0 is that different technologies, such as cryptography and blockchain, are linked to enable the decryption and encryption of data with consensus and traceability (IP1:18). This is contrary to how Web 2.0 businesses operate, representing one reason for their reluctance to adopt these technologies (IP2:9). Furthermore, in Web 3.0, trust is created in a digital way without third parties, as the CEO highlighted (IP2:12). Importantly, Web 3.0 will not replace all the applications of Web 2.0, with a decentralized version of it, the CEO argued (41). Rather, it will be more like a coexistence of different applications and versions, and blockchain is not the only technology needed for the Web 3.0 space (IP2:41). Combined with other technologies, as the Senior Researcher explained, a system based on data monetization can be created in which users are incentivized to provide their data and get paid in cryptocurrencies (IP4:18). The Senior Researcher referred to the idea of an iteration of the Internet – from Web 2.0, where big corporations are reigning, to Web 3.0, where the power goes back to the individuals (IP4:20).

6.9 Digital Identity/ DID/ SSI

The topic of digital identity, according to the CEO, is the "next big wave that we are going to see in the Web space (…) a sense of identity, decentralization, and identity in Web

3.0.” (IP2:5) The expert explained that companies that have not been in the business of data monetization over the last decades, such as Microsoft, are now entering the digital identity realm as they recognize new business ideas (IP2:9). Not only businesses but also governments are stepping in and address the topic of digital identity, as the CEO of the digital identity firm argued: “Governments and institutions” push the concept of “My information is mine” (IP2:7).

The State Secretary for Digitalization of Austria also mentioned digital identity and data sovereignty several times throughout the interview (IP3:10,12,20,26,28,47) and highlighted the initiative **ID-Austria,** which was developed a couple of years ago after a thorough data protection impact assessment (IP3:12). ID-Austria provides Austrian citizens with the possibility of digitally identifying themselves and can be used for administrative procedures and services. Thereby, the State Secretary explained that it is transparency, which is at the core, ensuring users see and become aware of the particular data used they provided and shared. Furthermore, minimizing data represents another core aspect within the ID-Austria initiative, ensuring only that data is used and processed, which is needed for a particular service or procedure (IP3:12). This is an important way to ensure trust and additionally enables efficient, uncomplicated, and barrier-free administrative procedures, as well as cost savings, the State Secretary stated (IP3:4,12). Moreover, this ID service ought to be as efficient and convenient as possible achieved through a once-only principle, meaning that information already known by the governmental administration should be intertwined and accessible with “a single key” (IP3:12).

Regarding the question of what the State Secretary for Digitalization precisely means when speaking of digital identity, IP3 replied that digital identity is the key and the tool for gradually making use of governments’ agency services, state services, and business services in a trustworthy and absolutely secure environment (IP3:20). Digital identity is our digital ID through which we can access these services and identify ourselves, and the user numbers demonstrate that it is being applied throughout Austria with great acceptance, IP3 added (ibid.). At this point, 2.7 million ID’s have already been generated in Austria so far, additional digital services have since been deployed, like the digital driver’s license, registration certificate, and age verification; and everything that will follow based on this will also be well utilized, State Secretary Plakolm explained (IP3:20).

The State Secretary added in the context of ID-Austria that Austria is internationally a forerunner with its own national digital identity. Furthermore, with the recently implemented eIDAS regulation in Europe, the State Secretary highlighted that this regulation paves the way for integrating the “strong” Austrian system (ID-Austria) into a unified certified wallet system that allows the verification of each other’s national wallets (IP3:26). Along with trust, transparency, and availability, it is also the aspect of knowledge that IP3 emphasized, considering it highly important in order to get the best out of such services. State Secretary Plakolm explained that besides knowing how to use and trust these services, it is crucial to address fears and concerns by educating and including all communities within society (ibid.). In Austria, for example, the State Secretary mentioned that two-thirds of the population between 16 and 74 years have good digital knowledge and good understanding in comparison to EU member states, where it is every second citizen. The State Secretary is committed to advance in this area so that everyone has a solid foundation of digital knowledge that enables them to navigate everyday life and use the “digitales Amt” and digital identity service, allowing them to access and use these services without barriers, regardless of location and time (IP3:26). The goal is, State Secretary Plakolm explained, to digitize every ID (IP3:26). Thereby, one vital aspect is to educate the population; and one way to do so is through the initiative “digitale Kompetenzoffensive,” which includes workshops for free, offered in every municipality in Austria where citizens get to ask and learn about basic digital skills and Austria’s public digital services, facilitating better understanding and inclusion (IP3:28). The so-called “Digi-Dolmetscher”, thereby function as vital elements, acting as translators, operating in two directions. Digit-Dolmetscher inform the government where improvement is needed, where uncertainties exist, and where more information and knowledge should be provided. Conversely, they also promote initiatives and organize events (IP3:28,35). Through this, fears and concerns can be addressed, people can be educated and informed, and inclusion can be facilitated, ultimately allowing everyone to grasp the potentials and make use of the chances of digitalization (IP3:37).

In contrast to the digital identity service that the Austrian government is promoting, are decentralized identifiers (DIDs). The CEO explained, “every day you use many different identifiers [such as] your email address, your passport number, your driver’s license and many others,” which are typically created by a central authority, like governments. “The key aspect of decentralized identifiers is that the decentralized identifier is created by you (…)

you control the entire lifecycle of the identifier from the creation to the expiration” (IP2:55). This is all tied to metadata, private and public keys, which require a public, decentralized infrastructure to enable its functioning, interchanges, and transactions among participants as well as to publish particular information associated with the identifier (ibid.). Blockchain technology, thereby, allows the storage of not information itself but rather a proof of a particular information associated with the DID, which represents the different states this particular DID transitioned to over time (IP2:55). States mean that when a DID was created, it has an original state that was stored as a proof on the blockchain; when the owner of the DID is required to prove a particular piece of information associated with this DID – for instance, a verified university degree – the owner signs a transaction to verify that degree. This signing, or proofing, is then stored as a proof on the blockchain, signifying a different state of the DID than before signing (IP2:55). The proof of the particular information – the signature on the university degree – however, also needs to be verified at some point, which is done by using a trust registry. In sum, this allows to backtrack the different states that a DID went through, which is why the CEO calls blockchain a “time chain”, allowing to timestamp different events, or states, in chronological order (IP2:55).

6.10 Blockchain Technology

The following section is fundamental to answering the main research question. The Product Growth Manager argued that there are still misconceptions regarding Web 3.0, crypto, and blockchain technology (IP1:28). When it comes to the **“Definition”** of blockchain technology, the experts provided various explanations. In fact, three out of the four experts interviewed gave different explanations of blockchain (IP1:28; IP2:48,55; IP4:20); the State Secretary only briefly touched upon this topic (IP3:39).

The Product Growth Manager explained: “So there's a lot of confusion but realistically speaking, like Blockchain is nothing more, well, it is probably much more but just to be simplistic, it's effectively a public, not even true because it could also be private, but it's effectively um public database so where you can see exactly the correlation between items within database. And then that database is pretty much um trustless because it's, it's being run by different people in the world.” (IP1:28) T

The CEO of the digital identity firm explained blockchain "is giving you a deterministic way to determine the order of a set of transactions at the end of the day (…) blockchain is as basic as this" (IP2:48) The expert added that blockchain cannot be considered a database; the only problem it resolves is to order events chronologically, which allows the creation of a financial system, digital cash like Bitcoin, and decentralized digital identity systems (IP2:48). Blockchain provides the capability to determine the order of events in a decentralized way, which is why the expert calls it rather "time chain" (IP2:55; see IP4:31).

The Senior Researcher explained that it is basically a transaction log that allows to store information about transactions (IP4:20). Similarly, the CEO argued, that blockchain was created to solve a specific problem, which is to reveal in a deterministically way the order of a batch of transactions "and this is the only problem that the blockchain fix[es]." (IP2:48) In contrast to what the CEO explained, the Senior Researcher further argued that blockchain, from a simple point of view, is some kind of infrastructure that is a combination of a decentralized database with a peer-to-peer system and cryptography, combined with some incentive mechanism, which comes from game theory (IP4:20). The expert explained that on top of this infrastructure, one can build trusted applications such as decentralized payment systems, such as Bitcoin. The expert added that there are no real limitations as to what can be done with blockchain and what is not. Therefore, it should be seen as an infrastructure, a cloud or database that has some specific properties and argued "it might not be as fast or as cheap as centralized systems, but if there is like the intend to democratize the system, to make it decentralized and not rely on a single party, then it's always a good idea to have a blockchain" but "it doesn't always make sense." (IP4:20)

Blockchain's **"Characteristics"** are, according to the experts, "traceability and transparency" (IP1:34), immutability (IP4:20), transparency, security, and safety (IP3:39). Blockchain further allows the creation of trust – at least in the works of the CEO – (IP2:12) and according to the Senior Researcher, it acts as a trust layer (IP4:20), with pseudonymity (IP4:25).

The sub-category **"Applications"** includes various possible or already existing use cases of blockchain technology. The Senior Researcher described existing "issues" around data management whereby blockchain could play a role. The expert described some examples as follows: medical data are highly sensitive, which he believes people do not want to share with anybody, except with doctors, for instance (ibid.). The e-card in Austria, for instance, is not “an ideal system” according to the expert, because the doctor you visit can see which medicaments other doctors prescribed, and you as a patient often do not know and see with whom the data is shared (IP4:4). With regard to the pandemic a couple of years ago, the expert further explained that it would have been interesting from a research perspective to do some kind of anonymous research on data, “like regarding vaccinations, or preconditions and so on” but it was not possible due to the sensitivity of the data (ibid.). The same is true for bank data, including the credit history of clients, but also for search history data, which might be interesting for advertisers. According to the expert, these examples represent possible use cases in which blockchain technology could play a role (4).

Already existing blockchain-based data sharing use cases and future **“Imaginaries”** of such, were also discussed in the interviews with the experts. The Product Growth Manager, for instance, described that the firm the expert is working at uses blockchain to help trace data whenever someone is taking the step of actually deciding to share it.” (IP1:34) Due to the fact that there are users who want to share their data while others do not, Ocean Protocol makes sure that if users wish to do so, they have a fully transparent visualization of the ways in which that data was used and shared (ibid.). They achieve this by making use of the two most prominent Ethereum tokens (ERC-721 and ERC-20) and bringing them together with a smart contract, merging them two into one (ibid.) The reason why Ocean Protocol needs both tokens is because this enables the firm to “orchestrate (…) who owns the data and (…) how it is being shared.” (IP1:34) When merged, an NFT (Non-Fungible-Token) is created and therefore “your data is your NFT” (ibid.). However, users’ data is not stored within the NFT; the NFT only contains the hash or metadata to the storage of the user’s data (IP1:34). Notably, the firm thereby allows users to individually decide whether to store their data in a centralized exchange or in a decentralized storage. Additionally, Ocean Protocol only stores a hash to the link of the storage, and if the user decides to sell the NFT, then the entire IP of that data is sold (IP1:34).

Renting the NFT is also an option that is enabled through the deployment of another ERC-20 token, representing the sort of license (ibid.). A license can be customized individually and can have different logics attached, and therefore can also be used for different use cases, such as for business or research purposes, which would have different interests and prices (IP1:34). One of the hurdles of this novel architecture is the price discovery mechanism, which involves attaching value and price to a particular dataset or NFT (IP1:36). However, the issue is that people do not know how much the data should be priced because they do not know how much someone is willing to pay for it (ibid). Additionally, these NFTs cannot be traded because the technology does not yet support this (ibid.) and smart contracts for this purpose are still “a bit clunky” (42). Thus, Ocean Protocol’s future long-term plan is “to attach financial instruments to data” and “(…) to create financial derivatives that are backed by data.” (34) One way to do so effectively in the future, according to the Product Growth Manager, is to use the ERC-20 tokens as tradable tokens, which is made possible by tokenizing datasets in which people ultimately can invest. The expert explained that in the future, one can invest in Tesla, for example, but as an additional option, one can also invest in a tokenized dataset in case the person believes this dataset to be used by others to, for instance, train and improve their AI models, which ultimately would have impacts on the dataset’s price (IP1:36), and eventually on the investment. The price discovery mechanism, therefore, is attached to the dataset, and its fluctuating value thereby is based on demand and supply (ibid.). To achieve this, Ocean Protocol will “definitely” use blockchain and smart contracts (IP1:42).

Another application of blockchain is the purpose of creating “a new architecture that gives control and prevent surveillance by design,” as the CEO of the digital identity firm explained (IP2:103). The company follows a technological approach that leverages the characteristics of and other technological advancements that are built on top of it. “What we are doing,” the CEO explained, “is to mix cryptographic tools in different ways to create a decentralized approach, so cryptographic and decentralized are two key elements from the technological point of view” (IP2:52), which also includes the technology called zero-knowledge-proof (ZK-proof) (IP2:50,52). Zero-knowledge-proof technology is important to “scale a blockchain, to create privacy (…) to have the ability, for example, to manage things like selective disclosure.” (IP2:34,50,52) Zero-knowledge means, as the CEO explained, that “if I had you to prove you that I am Argentinian, I don’t have to show you my passport; I can create a proof that I am Argentinian, and the key technology here is zero-knowledge-proof.” (IP2:52)

The Senior Researcher also mentioned ZK-proof technology in a use case wherin “I can prove that I’m over 18 without revealing my driver’s license. I can just prove, okay, there is a proof, cryptographically, that I have a birth date, uh, before that year, and it's signed by the government uh, but (…) you don't need to know, like, if I'm, like, 18, 25 or 40, so this can be very interesting I think." (IP4:37; IP2:34) ZK-proof technology also represents one big topic they are focusing on in the context of the digital product pass in the supply chain (IP4:37). The expert explained that with this technology, companies can share information without revealing all the information attached to a product, which otherwise could cause economic damage due to competition. Hence, it allows to prove that "I manufactured this batch of products according to the specification, but I don't give you an exact detail when I produce them." (IP4:37)

Except in combination with ZK-proof technology, blockchain in general allows the disclosure of insights and the chronological order of different events in the form of timestamps due to its transparency. For this reason, the CEO initially asked himself "whether governments will ever use this kind of technology as it puts them into a crystal box" allowing everyone to see what they are doing. For the expert's surprise "they are really open to adopt the technologies" (IP2:114). Furthermore, the expert still doesn't know the reason for this, but his company is about to close a deal with a provincial government which is considered to be one of the most corrupt provinces the expert's country "and this is like a Trojan House for the corrupt system" he added (IP2:114). The expert assumed that these companies are not thinking about the consequences such an implementation of these technologies might have for them (ibid.). "It's interesting because it's kind of a contradiction and it's crazy to think that [the] government is pushing to adopt this." (ibid.)

Another example of how blockchain technology is being applied for data sharing was described by the Senior Researcher, and will contribute to the answering of sub-research question 2 (SQ2). The expert replied to the quote by Harari, and mentioned the "Brave browser" which basically is a competitor to the Chrome and other browsers "where you select basically which data you want to share, which ads you want to get (…) and then you get paid in cryptocurrency whenever you consume such an ad" (IP4:18,20). This is like a "win-win-situation," as the Senior Researcher described it, because "the advertiser has a more strict, narrower focus, because the only people that are really interested in this topic will see the ad (…) and people who see the ad have a benefit because they get a few cents for it." This, the expert added, "might be a model (which) could also be transferred to other fields" (IP4:18), but highlighted to be careful with such as it could also be exploited by, for example, poor people who are willing to share sensitive data (ibid.). A similar system, in which users receive rewards for their actions, was also mentioned by the same expert later when the expert described a specific project in which users' recycling history – based on a point system – determines how many tokens one obtains (IP4:37).

Regarding the question about "How to trust on the Internet?" and which tools may be needed to translate "trust" in to the digital realm, **"Smart Contracts"** could serve as a potential solution according to some experts. The Product Growth Manager described a smart contract as an "automated software" that cannot be changed or altered as it is "deployed on a chain" (IP1:62). The expert added that it is about pre-defining rules of certain components and if something happens then something else happens which "is almost like providing you the guarantee that you can backtrack what you've done." (IP1:62) The same expert compared traditional legal contracts with smart contracts and argued that the former can be breached by people in contrast to the latter, which is automated and deployed on chain, therefore making them more robust (IP1:62). The reason for its robustness, the expert argued, is that no human can interfere (IP1:65-66). This does not mean that "everything can be ascribed in a smart contract"; and "Ethereum" with its smart contracts "is not the solution for every problem, every aspect of the human race," as the CEO emphasized (95). The expert further stated that although smart contracts are a useful tool, they are "for sure not going to be the law for humanity, at least for the next 10, 20, 30 years." (IP2:95) The Product Growth Manager, however, presumed that in the future "we're going to have some really, really solid open source smart contracts" (IP1:62) but mentioned "quantum computing" which could bring issues and risks of hacks (IP1:66).

Hence, blockchain technology along with its applications also entail **"Risks and Concerns"** according to the experts. The Senior Researcher described the issues that could arise from a lack of understanding and knowledge of a particular field. For example, a decentralized approach in democratic voting – such as on how to share data – could cause undesirable results (IP4:20). The Product Growth Manager mentioned the "blockchain trilemma," which means that it is hard to have all three characteristics of scalability, decentralized, and security/ or speed within a single blockchain system: "you got to compromise on something", the expert stated (IP1:44).

Scalability is also a concern that the CEO expressed (50); for the Senior Researcher it is the lack of knowledge within the space (20). The Product Growth Manager defined finding the balance between scalability and security as a considerable risks, in addition to the risk of centralization of a blockchain network (ibid.). Centralization of a network, the expert argued, could be achieved due to a specific amount of money involved, combined with human nature, which is to be a winner (ibid.). “My biggest concern eventually,” the expert stated, is that “there will always be governments or companies that will try to appropriate themselves of the power of the network.” (IP1:44)

Risks for the Senior Researcher exist in a false sense of security, which stems from the believe of thinking that “ok, it uses blockchain, so that’s why (…) it must be safe” (IP4:24). Once data is there, it is protected and cannot be manipulated, but one always has to ask “how the data gets into the blockchain,” the expert explained (IP4:24) Hence, it is about the quality of data that is being stored into a blockchain, which requires caution in regard to the principle of “garbage in, garbage out” (IP4:24).

Some of blockchain’s **“Benefits & Advantages”** can be summarized succinctly as follows: if fully decentralized, it provides an extra layer of stability (IP1:48); in combination with ZK-technology, it creates privacy and allows to selectively disclose information (IP2:52); it facilitates incentive mechanisms (IP4:25), rewards systems (IP4:16) and decentralized identity systems (IP2:48); it increases trust in a data-sharing system (IP4:25); and in general, blockchain allows to create decentralized networks that function without the interference of central authorities.

State Secretary Plakolm highlighted three major aspects to be important within the digital services provided by the Austrian government – which are transparency, security, and safety. Blockchain technology encompasses all three components; however, it is not applied for Austria’s digital services, such as for ID-Austria (IP3:39). However, the State Secretary for Digitalization argued that blockchain offers many advantages, particularly in terms of transparency and security; however, the developers and initiators have decided to use other tools and technologies for the digital identity service ID-Austria (IP3:39). In response to the question of whether more research is needed on blockchain in order to be implemented in the future, the State Secretary emphasized the importance of staying vigilant and up-to-date because of the rapid changes and dynamic developments in recent years. “My principle is to never stand still”, and highlighted the need for improvements and adjustments if necessary (IP3:41). State Secretary Plakolm further argued that it is important to be open for technology in all areas and that we should always keep our eyes and ears open in all directions to avoid going down a one-way street, ending up in a “Sackgasse” (IP3:45).

6.11 Outlook

Regarding the question of **“Current Trends or Future Developments”** the experts described different interests and outlooks. For the CEO, after the waves of Bitcoin, Smart Contracts, DAO, and DeFI, digital identity is what he believes to be the next big thing (IP2:5). For the State Secretary for Digitalization of Austria, digital identity seems to be an important topic, as the digital identity service ID-Austria is being promoted and several improvements and developments in this regard are already in the works (IP3).

The Product Growth Manager mentioned “Ocean Enterprise” which seeks to “create it's stable, robust, regulated foundational technology that is fully open source for all the companies in the world to come together and uh and really improve their industry.” (IP1:72) The expert, thereby, promoted this upcoming product, and referred to the automotive industry and described the issue of different automobile companies which do not want to share their data with others due to competition concerns, but underscores the importance of sharing data within their industry as it would improve their industry by revealing “insights” and “knowledge” (IP1:72). The expert further mentioned the health industry, which could benefit from sharing data open source. Additionally, “if you're thinking about health, imagine hospitals and research institutes coming together with their data, with their efforts with solutions that provide privacy to each one of them to really fast track life, cancer research and all this stuff. You'd require much less funding because people don't need to buy tons of data all the time. Um And you just fast track the process of finding the cure of cancer the cure of HIV, and everything else. So, what we're hoping and what I'm really excited for is really all these companies and governments coming together for the greater good as opposed to everyone trying to enhance profitability” (IP1:72)

The Product Growth Manager’s future **“Imaginary 2050”** is quite skeptical. The expert is concerned because of AI’s hype, bringing “hyper profitability, hyper growth, and hyper everything to the table” which made him believe that “we're going to be seeing ourselves a world that is very detached to what we know now” (IP1:80). However, the expert imagined that in the year 2050 there will be collectives, or “probably social media of people gathering to share their data and other stuff” (IP1:82). The expert added that he is not sure which products there will be, but the “awareness of data will be huge” (ibid.). Furthermore, because “AI is getting so centralized already two years after the launch of Open AI, that (…)

people are understanding their concern. And so, I think we very much see consortium of organizations coming together um with um with data ownership technologies to facilitate both the capitalist world and also the, you know, more individual interest." (IP1:82)

In contrast to the Product Growth Manager, the State Secretary's imaginary about 2050 and Austria's future is more optimistic. State Secretary Plakolm expressed hope when envisioning Austria to be on top of the data-driven economy in 2050, driven by the efforts and initiatives of the Austrian government that push AI developments with the right policies and laws forward. This approach allows a successful harnessing of the technology's potential and opportunities. Additionally, humans have to remain at the center of any technological development, which the AI Act perfectly demonstrates (IP3:56). Technology in general, as history has shown, has been used in either good or bad ways, which is simply a part of human nature, according to the CEO (IP2:114). The expert concluded that technology per se is not going to change the human nature, because "those concepts are not connected" (ibid.).

7 Discussion

The goal of this empirical research was to understand how different actors within the digital economy envision the future of data ownership, the role of emerging technologies, such as blockchain, and what this means for societies. The raw data collected from the four interviews, presented in Chapter 6, are subsequently linked to the existing literature. This ultimately allows us to answer the research questions and develop new theories. The research questions provide guidelines for this chapter. Initially, the main research question is introduced and discussed, focusing on the different actors' imaginaries about the future of data ownership and the role of blockchain. Following the initial part, this chapter introduces and discusses the three sub-questions. The final section aims to link Marx's views on capitalism, private property, estrangement, and other concepts to contemporary issues in digital capitalism, data, and centralized data extraction.

7.1 Answering the Main Research Question

What are the future imaginaries of different actors within the digital economy regarding data ownership and the role of emerging technologies, such as blockchain, in digital societies?

7.1.1 Data Ownership Imaginaries

The interview results indicate that there are no rules about data ownership within an entire "unregulated space" (IP2:44), and the question of "who owns the data" is perceived as an ambiguous situation (IP1:14). According to the results, the concept of data ownership lacks a unified definition among the experts (IP1:16; IP2:7; IP3:8; IP4:12,14). All experts articulated partially divergent understandings and highlighted various issues related to the topic. This may cause confusion among stakeholders regarding the overall understanding of

DO, and they demand clarity for enhanced discussion and future development. Asswad & Gómez (2021) also highlight this lack and the absence of a unified definition in their work. The authors describe the frequent confusion about DO, which is the confusion between ownership and usage privileges (4). Furthermore, they argue that the term DO is associated with many domains, including data governance, data management, data sharing, data security, data privacy, data integrity, data sovereignty, data stewardship, data transparency, and data traceability (Asswad & Gómez 2021: 2). This highlights the wide spectrum of aspects associated with DO and the need to discuss and compare different perspectives, ideas, and concepts carefully, as their understandings and meanings might differ among actors. Consequently, if societies aim to build effective, new, robust systems that enable individual data ownership, more clarity is required. A crucial step for Europe would be to integrate data ownership into the GDPR with a unified definition of what DO means and encompasses. Including data ownership with a clear definition in the GDPR can facilitate awareness at a much greater level beyond academia and Web 3.0.

Recent developments in big tech firms, including Microsoft (Microsoft.com, accessed 10th September), governments such as Austria and Estonia (E-Estonia, accessed 18th July 2024; oesterreich.gv.at, accessed 8th September), and institutions such as the World Bank (IP2:7), have indicated increasing attention to DO and DI (Asswad & Gómez 2021: 2). According to the results collected from the interviews with State Secretary Plakolm (IP3) and the CEO (IP2), we see increasing attention as governments, institutions and other big tech companies are promoting the concepts of DO and DI.

From a governmental perspective, State Secretary Plakolm (IP3) refers to Austria's national initiative, ID-Austria, while envisioning the concept of data ownership. In the State Secretary's vision, data ownership means having control of the dataset, including its usage, storage, application, and processing, as well as the power to decide how and for what purpose the data should be used and processed (IP3:8). The ID-Austria initiative promotes data sovereignty while exemplifying a clear top-down approach. Data sovereignty is also one of the arguments for decentralized identity use cases within Web 3.0 and SSI narratives; however, in contrast to Austria's initiative, it is envisioned as a decentralized and bottom-up approach (Allen 2016; Reed et al. 2020). This marks an intriguing starting point for a discussion: if we compare the two visions of a government promoting data ownership and data sovereignty on the one hand, while Web 3.0 narratives also promote data ownership and data sovereignty, then we could ask whether these two approaches represent a clash or whether a hybrid version of both would make sense. On the one hand, ID-Austria – a service provided by a proactive centralized authority that strives to guarantee transparency, safety, and security and overall provides an infrastructure, framework, governance, and regulation. However, this might raise questions within blockchain narratives concerning individual autonomy and freedom. On the other hand, there is a decentralized approach that promotes individual freedom and empowerment. However, this raises questions about governance and accountability. Therefore, would it make sense to merge these contrasting approaches to harness the advantages of both?

One country that decided to follow a sort of hybrid approach is Estonia. The Estonian government provides regulation, a governance framework, and the infrastructure while leveraging blockchain technology and its characteristics. Citizens can therefore be sure about their data being safe and secure, and to trust the Estonian government (Asswad & Gómez 2021: 11).

Another example of a hybrid data ownership infrastructure was described in the interview with the CEO. The expert expressed his surprise when explaining that his company was about to close a deal – concerning DO and DI systems, in which blockchain technology represents a core part – with one of the most corrupt governments in the country (IP2). This is indeed quite surprising, since the initial vision of the early crypto-anarchist community revolved around the idea of eliminating intermediaries and central actors who today envision blockchain's potential for blockchain-supported governance at an institutional level to "avoid power centralization problems on the Internet, tackle corruption, and increase governmental transparency." (Semenzin et al. 2022: 2; see Tapscott & Tapscott 2016). Therefore, the tensions between blockchain's potential praised within the Web 3.0 space and real-world application by governments raise critical questions: Does such a hybrid solution truly address issues around DO and DI, or is it being misused by a system that originally was designed to challenge? What are the trade-offs in such a hybrid system?

Overall, this example connects to what the CEO envisions, namely that governments are becoming more interested in these topics as they increasingly consider "the ownership of data is in the person" (IP2:7). Moreover, even though traditional data monetization firms of Web 2.0 are reluctant in acknowledging this "new reality," these companies are also going to adapt to this new reality in the coming next 3-5 years, the expert envisions (ibid.). An example of this shift in the commercial sector is a product promoted by Microsoft called Microsoft Entra Verified ID (learn.microsoft.com, accessed 6th September 2024). According to Microsoft, the reason for product development is the increasing number of cases of identity theft and data breaches, which necessitates self-governed decentralized identities that put "individuals in control of their own digital identities, providing a secure and private way to manage identity-related data without relying on centralized authorities or intermediaries" (learn.microsfot.com, accessed 6th September). The description of Microsoft's decentralized identity project resembles that of the CEO of the ID firm (IP2:55). However, whether blockchain or zero-knowledge-proof technology is part of Mircrosoft's solution can only be assumed based on the terms (DID, decentralization, cryptography, trust system, or wallet) and the descriptions used (learn.microsfot.com, accessed 6th September). These arguments, statements, words, and descriptions allow us to critically ask: Does Microsoft genuinely want to address these topics or does the firm just want to catch "the next wave of DID, DI, DO solutions" (IP2:5) by taking advantage of the usage of buzzwords typically associated with the Web 3.0 community in order to build their own products for their own benefit?

Skeptics might state that this could be just another business model of big tech firms and service providers that allows the accumulation of more data and profit, representing another stage of ever-reinventing capitalism (Schumpeter 1943).

If this business model, which puts the individual user at the center, facilitating both complete control over their identity and data sovereignty, eventually replaces the traditional Web 2.0 model – aiming for controlled intermediation, extensive data extraction and monetization, and the control of digital interaction – we can investigate whether this shift mirrors the concept of *creative destruction* (see Chapter 2).

These examples, in which governments and corporations enter the digital identity and data ownership domain, raise the question of why such central authorities promote a topic that represents a typical narrative within the SSI movement and the evolving Web 3.0 space, in which intermediaries and other centralized, powerful entities are envisioned to have less control over interaction, data, and overall, people. Do blockchain's decentralized nature, immutability, robustness, or transparency spark their interest, or are there additional factors to consider? To date, only time will tell whether these projects will evolve into another capitalistic version of complete control over citizens, users, and their data, or whether they serve as a solution for addressing issues in DO and data management (Microsoft.com; learn.microsoft.com).

The Austrian government follows several approaches that fundamentally differ from those of countries such as China. The State Secretary emphasized that such systems that facilitate “transparent citizens” are perceived as highly controversial (IP3:12). Notably, although State Secretary Plakolm advocates for transparency, safety, and security and considers these to be essential elements for building robust systems in which people can trust, the Austrian government has decided not to utilize blockchain technology for their ID citizen service.

Given that robust and effective digital identity systems, such as ID-Austria’s, which are based on the principles of transparency, safety, and security – characteristics that align with those of blockchain (noting that safety primarily pertains to the Bitcoin blockchain) – function without relying on blockchain technology, then why should society use this technology for DO and DI purposes?

7.1.2 Blockchain Technology Imaginaries

First, one of the key findings of this research is that the experts envision a future in which technology – primarily blockchain – contributes to addressing some of the issues presented in Chapter 3, but only as a part of a broader set of tools and approaches (IP1:18-20; IP2:41,52,95; IP4:16,33). This encompasses zero-knowledge-proof, hashing, cryptography, and other technologies built on top of a blockchain, such as smart contracts. Therefore, it can be argued that blockchain alone will not resolve contemporary challenges but can play a role along with other tools to address specific issues. This relates to what was described in Chapter 3. The development of blockchain technology, as it stands today, was made possible by integrating a diverse set of other technologies, including public key encryption, hash proof, and digital time stamping (Nakamoto 2009). Thus, blockchain’s effectiveness depends on a combination of various tools, resulting in a solution tailored for a specific problem. This mirrors what the experts envision: building robust DO and DI systems requires more than just blockchain; it requires a set of tools.

Furthermore, according to the CEO (IP2), Web 3.0 – with blockchain at the center of this “iteration of the Internet” (IP4:20) – is not going to replace all Web 2.0 applications and services with a decentralized version of it; instead, the CEO further imagines the co-existence of different applications and versions.

Decentralization is a fundamental characteristic of blockchain technology. Decentralization, according to the CEO fixes "at least partially the concentration of information and the control of the excessive control of information (…) so it's going to undermine a part of the power that big players have today." (IP2:82) The CEO's vision mirrors what Harari stated: "If we want to prevent the concentration of wealth and power in the hands of a small elite, the key is to regulate the ownership of data." (2019: 93) One way to achieve this is by building a common, native identity layer that allows to create DIDs and facilitates new forms of both data and identity management. This enables users to manage and control their own identities, thereby eliminating the need for other centralized authorities. Furthermore, the experts envision that introducing DIDs promotes a new system, a new iteration of the Web (Web 3.0) characterized by a decentralized, more democratic network of individual users who are in control of their identities and data. Furthermore, if fully decentralized, blockchain provides an extra layer of stability (IP1:48) within the system, facilitates incentive mechanisms (IP2:48), and in combination with ZK-proof technology, it creates privacy and allows selective disclosure of information (IP2:52). Blockchain is envisioned as an infrastructure that consists of a decentralized database, peer-to-peer system, and cryptography combined with an incentive mechanism (IP4:20). The technology facilitates the creation of a reward-sharing system in which participants can receive tokens or other forms of rewards for their contributions and actions, as explained by the Senior Researcher (IP4:16,18,20,37). Therefore, when properly implemented, blockchain can not only facilitate the democratization of information access, control, and sharing, but also promote greater equity by eliminating fee-charging intermediaries.

According to the literature and perspectives of some experts, the imaginaries of smart contracts primarily revolve around a specific idea, which is the elimination of the need for some intermediaries and transactional processes. Their automated and self-executing nature, along with their robustness due to the absence of human interference (IP1:62), and their immutability, while resting on the overall characteristics of blockchain, smart contracts are envisioned to play a role in specific processes and future use cases. Moreover, according to the results, the future of smart contracts seems promising as they facilitate automation, efficiency improvements, and transparent cost-saving transactions.

Although smart contracts carry a diverse set of promising characteristics, the experts also highlighted their limitations. The key findings here indicate that, at this moment of writing, some visions of eliminating intermediaries, such as lawyers, and replacing entire systems with trustless systems may sound promising for some but appear to be too far off and in need of more critical consideration. It is important to note that the emergence of blockchain-based trustless systems does not eliminate the notion of trust. Instead, the notion of trust shifts from trust in humans, institutions, governments, or other intermediaries to trust in technology and smart contracts. This opens another topic for discussion: people within such trustless systems need to establish trust in the technology before they can accept and adopt it. Moreover, the vision of replacing particular interactions with a few lines of code, which previously required trusted controlled intermediation, raises the following questions: How can these codes be trusted? How can people with mediocre or less understanding in coding or computer science trust the technology? How can one be sure that the coders can be trusted and that the code itself aligns with human needs and societal values?

In today's digital age, spending more time on the Internet becomes a necessity. This requires enhanced levels of trust to ensure transactional processes, stable interactions, and secure information-sharing. All four experts agreed on the importance of trust in today's digital worlds. State Secretary Plakolm noted that even the best services and most efficient administrative channels are worthless when people do not trust these services or the ways in which data is processed (IP3:10). To achieve this, the State Secretary emphasized that transparency, security, and safety must always be guaranteed, representing the State Secretary's primary premise for digital services (IP3:18).

To build a system similar to the physical world, in which a person simply identifies their identity with a passport validated by someone authorized (IP2), two aspects are fundamental: technology and governance (IP2:18-28). However, this can be expanded with the Product Growth Manager's vision: for effective data ownership products, it also requires a cultural shift (IP1:18,20), including education and knowledge. From a governmental perspective, State Secretary Plakolm emphasized the importance of trust, transparency, safety, and knowledge for building robust systems that handle citizens' data (IP3:26). In addition to providing knowledge and education, it is important to address concerns and fears through initiatives such as workshops, as State Secretary Plakolm further explained (IP3:37). Providing knowledge and education about technology and services goes hand in hand with facilitating inclusiveness and addressing concerns and fears, which can potentially increase the levels of trust, thereby facilitating acceptance and adoption. A similar stage process was described by the Product Growth Manager, emphasizing that at first technology brings discomfort, but after people use it, they understand it, which then brings about cultural shift (IP1:18-20). Therefore, based on the results, we can argue that the development of a robust identity layer for data ownership applications requires a multifaceted approach, encompassing technological advancements, governance frameworks, time, education, knowledge, and a cultural shift. A narrative advocating for a decentralized network architecture, which engenders users' trust through its technological design rather than reliance on intermediaries, may facilitate this development and the emergence of effective data ownership use cases, resulting in the empowerment of users through individual data sovereignty and ownership, enabling them to harness the potential of decentralization in the evolving iteration of the Web.

7.2 Answering the Sub-Questions

SQ1: How might the utilization of blockchain affect the distribution of power over data?

Blockchain technology, in an addition to other tools, influences power distribution over data, primarily due to its core characteristic of decentralization. The results indicate that decentralization partially reduces the concentration and control of information (IP2:82) and thus undermines the power of "big players" in the digital economy. In combination with other tools, such as decentralized identifiers (DIDs) (IP2) and smart contracts (IP1), blockchain technology enables the creation of a self-regulated infrastructure. This infrastructure enables owners of decentralized identities to manage and control their identity and data. This promotes the concept of data sovereignty and the idea of power over data returning to the people (e.g. Lee 2019; René & Mapes 2019; Tapscott & Tapscott 2016; Voshmgir 2020).

However, it is important to note that although blockchain facilitates the democratization of data ownership through decentralized infrastructure and identities, it also carries inherent power dynamics (Varys et al. 2022), particularly in combination with smart contracts. For example, developers can wield power over other participants of the network because of their superior knowledge, technical skills, and understanding. By coding specific IF-THEN statements that may not be apparent for regular users, such smart contracts and services could potentially serve only the developers' interests. This raises concerns about a shift in power dynamics, moving from institutions to individuals with technical and specialized knowledge (technocracy) (Varys et al. 2022). Therefore, careful and critical consideration is indispensable, as new power imbalances might emerge before the decentralized infrastructure is fully implemented.

A shift of power over data to the people also includes another implication, which is the shift in responsibility. Traditionally, institutions such as banks manage and safeguard people's assets and depots. This is, according to one expert (IP1:60), because people do not fully trust themselves; they entrust these institutions rather than themselves. In contrast, users of decentralized digital identities do not rely on intermediaries but must manage and control their DIDs and access keys on their own. This introduces risks of potential loss of data, DIDs, or even entire identities. At the same time, a shift in responsibility also offers people the opportunity to increase their levels of self-trust and autonomy.

SQ2: What does blockchain technology offer or imply for digital societies in the pursuit of a more equitable digital economy?

Blockchain-based decentralized systems can facilitate the democratization of information access and sharing. Decentralized digital identities or self-sovereign identities, do not rely on intermediaries, such as platforms, and allow for individual control over data. In combination with zero-knowledge-proof mechanisms and cryptography, privacy can be ensured, allowing users to be in full control of the disclosure of their data, which ultimately fosters a more democratic digital ecosystem.

Furthermore, one important aspect highlighted in the interviews was the opportunity to build reward systems enabled by blockchain technology's characteristics. The results indicate that a system that allows users to receive rewards in the form of tokens for particular actions and contributions is envisioned (IP4:16,18,20,37). Due to the absence of intermediaries that charge fees for their services, users directly benefit from the reward-sharing system, based on their actions and contributions. When implemented properly, such a system can help to address specific issues. The Senior Researcher described an example where participants in a specific recycling project are incentivized to collect plastic bottles and receive tokens based on their contributions represented as data. Purpose-driven ecosystems (see Voshmgir 2020: 108) as such enable users to directly benefit from their activities by receiving network tokens (e.g. Steemit), without relying on intermediaries or paying fees for their services (Taghdiri 2019), except network fees. Users can directly see and grasp the implications of their actions as they are rewarded based on them. Whatever the reward is, it encourages people to become active and behave in a certain way.

This vision also raises concerns about potential exploitations because users may try to manipulate such a system in a certain way to receive more rewards, highlighting the need for some sort of governance. However, at the same time, this opens new opportunities for discourse concerning new forms of income. For instance, a reward-sharing system that concerns climate change could be established, allowing participation from everywhere in the world. The decentralized architecture encourages people to behave in a climate-friendly manner by offering (digital) rewards. Appropriately implemented, this could effectively merge the physical and digital worlds and facilitate inclusiveness of marginalized groups and less developed countries.

Moreover, in other industries, as presented in Chapter 3, artists who usually rely on various intermediaries to promote and share their music could leverage a decentralized architecture and technological stack (smart contracts). This not only enables them to directly interact with their community and foster reciprocal relationships; it also allows them to benefit more from their own work, as intermediaries no longer cut off percentages of their earnings, facilitating new business models.

Blockchain can thus play a vital role in the pursuit of a more equitable digital economy. Blockchain can facilitate new business models and reward-sharing systems in which users are encouraged and empowered by directly benefiting from their contributions. Consequently, by eliminating the need for intermediation, power dynamics can be mitigated while benefiting from self-earned rewards.

SQ3: In what ways does blockchain technology enable the creation and operation of decentralized trustless systems?

There are various debates and visions about blockchain facilitating trustless systems. Consequently, it is essential to discuss blockchain and smart contract applications in conjunction with the notion of trust.

The results indicate that blockchain can utilize its decentralized infrastructure to record and time-stamp transactions, which are validated by the network of participants, run by the people (IP4:12) and without a central authority involved. Advanced cryptographic mechanisms ensure data integrity and secure transactions while reducing the need to trust intermediaries who typically manage these processes. Instead of traditional intermediaries, smart contracts are envisioned to enforce specific rules and automate some transactional processes without human interference. However, the visions found in some literature on blockchain, concerning the creation of trustless systems, are debatable and need critical consideration.

The concept of a blockchain-based trustless system necessitates an infrastructure that enables a trustless system. Therefore, although trust in intermediaries could become redundant in some cases, the notion of trust does not fully vanish; rather, it shifts from trusting intermediaries to trusting blockchain technology and its architecture, which is not individually controllable. Blockchain, along with smart contracts, can facilitate the development of new digital infrastructures that reduce the need to trust intermediaries for particular IF-THEN agreements and transactional processes. However, it does not eliminate trust but rather creates new forms of trust (Alston et al. 2021: 2), namely trust in technology. In other words, in traditional intermediation service systems, intermediaries or central authorities ensure the functioning of the infrastructure and guarantee that people can trust the services. In contrast, in a decentralized system, it is the technology that people have to trust. Moreover, trust is not something that can simply be inscribed into the system. Trust, as debated by early and contemporary social theorists (Simmel (1900), Hobbes (1985), Parsons (1970), Giddens (1990), Luhmann (1979)), is a vital societal need but complex issue; it is determined by a complex and dense web of social interactions, as explored in Chapter 3. Trust, based on the elaboration in Section 3.2.2, plays a fundamental role in facilitating cooperation, interaction, cohesion, and social order. Societies' increasing complexity over time necessitated the establishment of institutions that act as intermediaries and ensure trustful interactions among actors. These institutions verify, for instance, certificates, passports, and other credentials, which in turn can be used by individuals to identify themselves when required. As discussed with the CEO, this highlights the need for trust registries (IP2:18-28).

These results indicate that not everything can be ascribed to a smart contract. The human aspect still plays a vital role, and trust, as a human belief, cannot simply be written into code (IP2:18-28,95). The necessary role of trust registries underscores the importance of the human part in the equation, which makes some visions of making trust in humans redundant by replacing it with trust in code (O`Dwyer 2015) seem controversial.

Blockchain alone is neither going to recreate trust in the digital world nor will it eliminate what is being envisioned as corrupt factors of contemporary societies: human nature and trust in humans (O`Dwyer 2015). For effective decentralized networks, it demands other tools and means, and more importantly, the human part. Blockchain neither eliminates the notion of trust nor the need for human trust. Moreover, blockchain is not a complete substitute for the traditional trust mechanisms. Instead, blockchain can facilitate a new architecture of trust (Werbach 2018) but which combines technological and human elements. In sum, trust is never going to be purely technological and always requires the human part of the equation (IP2:95).

A broader theoretical societal question would be: What could it mean for future societies if technological advancements – in combination with AI – somehow managed to ultimately allow the creation of systems that are entirely managed and controlled by smart contracts? Additionally, if smart contracts represent the new modern forms of intermediation that enable transactions, interactions, the verification of credentials, or any other mediating service, what would this mean for societies and social interactions in general if no government or mighty power were in place but technology ruling and acting as a sovereign?

7.3 Marx in the Digital Age – Connecting Marx with Data and Digital Capitalism

In this discussion, we delve into Marx's views on class struggle and estrangement and link them to the contemporary era of digital capitalism:

The bourgeoise – who own the means of production and the products while exploiting the laborers – can be compared with the modern capitalists, operating under digital capitalism, who own and control platforms and all the information within; the proletarians, on the other hand – who are used as a commodity by capitalists (who aim to increase their capital) – can be compared with the users whose behaviors are monitored, analyzed, and sold as products for profit. Thus, before delving deeper into this, it is essential to ask whether it is right to call user-created data an activity of labor from a Marxist perspective.

When we connect Marx's considerations about labor to the topic of data, users' activity on the platform can be considered a productive activity as it produces a valuable commodity: data. Eventually, the data is sold by the capitalists for profit. This process ultimately enables the capitalist to capture excess value as surplus value. Hence, based on this elaboration, user-created data can be reasonably argued to be a result of a form of labor akin to production. Defining user activity as a form of labor allows us to delve deeper.

As explored in Chapter 2, the laborer constantly produces products that appear as alien objects because of the objectification of labor, which leads to estrangement and alienation (Marx 1844/1932; Marx 1887). Estrangement can be linked with the following interview results: people do not know what their data precisely means (IP1:12), what its value might be (IP1:36), and do not really care about data in general or its consequences (IP2:12,41; IP4:12). In both cases, whether in Marx's analysis or as discussed within the context of the current digital age, laborers (users) tend to feel disconnected from the products they create because these products (data) are owned and controlled by others (capitalists) (Marx 1844/1932: 33). Additionally, in Marx's view, the product (data) can be considered a summary of the labor activity which is spending time on the platform producing it.

Moreover, similar to what Marx (1844/1932: 30) argued, the production (of data) itself is active alienation. This assumption can be drawn from Marx's arguments combined with experts' statements about users spending time on the platform, producing data, not knowing what the data precisely means, and not caring about it or its consequences (IP1:36; IP2:114; IP4:12). Therefore, it can be assumed that users' activity of producing data – the production itself – is already a process of active alienation. Moreover, users objectify their activity (labor) in the form of a product (data) and tend to place more value on the outcome – which is the hope to get something back of value, such as free services and entertainment (IP1:8) – than on the data they produce.

In addition, at present, since the traditional Internet lacks a native identity layer (René & Mapes 2019: 87), which could allow the regulation of the ownership of data in the digital realm, and since "we are operating in an unregulated space" (IP2:44), it is the platform owner who ultimately owns the data, but never the user (IP2:41). The objectification of labor, combined with a lack of ownership, facilitates alienation and amplifies asymmetries and inequalities in power and control. However, when it comes to the visions concerning the question of "Who should eventually own the data," three experts referred to the potential and characteristics of blockchain technology, which they believe could partially play a role in resolving these issues including the topics of ownership (e.g. McConaghy et al. 2017), building the missing identity layer (McConaghy et al. 2017; Voshmgir 2020), and mitigating unequal power dynamics in data related-processes (IP1:18,20; IP2:103; IP4:16,18,20).

Another discussion that could enrich the one about linking Marx's views on capitalism with modern digital capitalism concerns the topic of "wages." This includes the guiding question of whether traditional compensation in the form of wages – received by workers for selling their labor power – can be compared to the "compensation" users receive in the form of free apps and entertainment (as a form of "wages") in exchange for the provision of time, privacy, and attention (in terms of labor), or whether users' activity should be considered as a novel extensive form of exploited, unpaid labor. As answering this would, unfortunately, extend this thesis' purpose and scope, this represents an interesting topic for future sociological discussions.

8 Conclusion

This thesis explored how different actors within the digital economy envision the future of data ownership and the role of emerging technologies, particularly blockchain technology. Given blockchain's current infant status in research and development, as well as the limited information available about the implementation and effective application of blockchain for data ownership purposes, a gap in the literature was identified, and the researcher decided to follow a qualitative research approach. This allowed the researcher to understand what experts envision about the concerning topics (Strauss & Corbin 1990: 11). Expert interviews were chosen as the method of choice and were demonstrated to be suitable for this research. The interviews allowed for an in-depth exploration of individual imaginaries regarding the future of data ownership and blockchain's role. The researcher was able to gather different visions, generate new data, formulate theories about the subject matter, answer the research questions, and contribute to the gap in the literature. Adopting Marx's theory to the digital age proposes additional ways of understanding class struggles along with their dynamics in today's data-driven society. The lack of literature on blockchain technology application for data ownership allowed the researcher to delve into the various implications of decentralized infrastructures for societies and unravel sociotechnical imaginaries along with the implications on existing power dynamics in this regard.

Therefore, the research results indicate that the applied methods effectively contributed to the answering of the guiding research question: What are the future imaginaries of different actors within the digital economy regarding data ownership and the role of emerging technologies, such as blockchain, in digital societies?

Initial Aim

This thesis demonstrates that the initial aim of exploring blockchain and providing clarity regarding particular topics and challenges, including private property (Tapscott & Tapscott 2017), digital identities (Careja and Tapus 2023), power dynamics (Srnicek 2017), shifting asymmetries (Tapscott & Tapscott 2016), data ownership (Zyskind et al. 2015), and the utilization of blockchain for social good (Dávila 2023) has been successful. Furthermore, this research has successfully provided insights into the means and tools needed for challenging capitalistic data management operations and mitigating asymmetries in information access and ownership through the establishment of robust, democratic, (decentralized) information-sharing systems. These explorations contribute to the existing literature a more comprehensive understanding of blockchain and smart contract applications for data ownership.

Data Ownership Imaginary

The research results indicate that both data ownership and blockchain technology have no unified definition, which is why the researcher suggests a careful, critical reflection and clear definition of what debating actors precisely mean and understand in this regard. One possible approach in the EU for providing clarity and a common definition would be the integration into the GDPR.

Although data ownership has not yet been sufficiently addressed in the GDPR, it has gained increasing attention recently. The results indicate that a wave of digital identity is evolving, which will have a great impact on industries and the economy within the next five years. This wave promotes the idea of "Ownership of information belongs to the people" and the overall concept of "My information is mine."

Recent developments demonstrate the general increase in attention and awareness regarding the topic of data ownership, including Austria's forerunner initiative ID-Austria (oeasterreich.gv.at, accessed 8th September 2024), the governmental service of Estonia (e-estonia.com, accessed 1st August 2024), Microsoft's Entra Verified ID (learn.microsoft.com 6th September 2024), and the general movement of self-sovereign-identity and Web 3.0.

ID-Austria represents an example of a central authority promoting the concept of data sovereignty, in which the user is at the center. This enables users to control various personal certificates and identifiers for better administrative services, ensuring cost savings and efficiency improvements. The primary premise of transparency, safety, security, and trustworthiness marks a fundamental contribution to the robustness and effectiveness of the ID service-system. Furthermore, fundamental rights, the common good of users, privacy, freedom of expression, and other democratic principles must be secured and ensured. The 2.7 million digital ID's already in existence in Austria demonstrate the well-accepted citizen service with the government's goal of increasing the number and digitizing every ID.

Blockchain Technology Imaginary

A fundamental research result indicates that blockchain technology can contribute to the creation of effective DO use cases. With its core characteristics revolving around immutability, security, and decentralized infrastructure, blockchain serves as part of a bigger toolset for building robust and effective DO solutions. This key finding indicates that blockchain technology will not solve the issue of DO alone. Thus, in a multifaceted approach encompassing zero-knowledge-proof, DIDs, and smart contracts, it can play a vital role. However, effective implementation and application require more than a technological aspect.

The results indicate that the governance aspect is also envisioned as crucial for building robust systems that allow the identification of one's persona simply and conveniently with a digital passport. This underscores the need for human operators, as the registration and verification of a certain document or DID can only be validated by trust registries. Therefore, successfully adopted and effective decentralized DO use cases necessitate additional aspects besides technology and governance, including proper education, knowledge and skills, time, a fundamental cultural shift, and humans.

One of the most envisioned blockchain use cases is associated with smart contracts. The results indicate that smart contracts represent a promising solution for particular intermediation and transactional processes. Their robustness, transparency, and automation, are their core advantages. Moreover, the potential to eliminate intermediaries can result in improved efficiency and cost savings.

However, as explored in this study, not all aspects of contractual relationships can be fully automated. This is because many institutional intermediation services require trust, and trust is a complex societal phenomenon and a human belief, which is why it cannot simply be written into code.

Importantly, smart contracts also carry risks associated with exploitation or manipulation because of programmers' potential bad intentions or poorly written codes. Therefore, for effective utilization, it is essential to ensure that smart contracts' design and IF-THEN statements align with societal needs, values, and norms. Moreover, smart contracts also raise concerns regarding the trustworthiness of the coders, which demands transparency in protocol development as well as education among people to better mitigate the risks of undesirable outcomes. As a result, the design and implementation of smart contracts require careful consideration, as well as acknowledgment of the complexities of human interactions and social structures.

Furthermore, according to the results, Web 3.0 – with blockchain at the center of this "iteration of the Internet" – is not going to replace all Web 2.0 applications and services with a decentralized version; instead, a coexistence of different applications and versions is envisioned.

In combination with other tools, such as decentralized identifiers (DIDs) and smart contracts, blockchain technology enables the creation of a self-regulated infrastructure. If fully decentralized, it provides an extra layer of stability, partially reduces the concentration and control of information, and consequently undermines some of the power of big players in the digital economy. In combination with zero-knowledge-proof technology, it creates privacy and allows the selective disclosure of information.

Building a common, native identity layer allows the creation of DIDs and the establishment of new forms of data and identity management, promoting the concept of data sovereignty and the idea of returning the power over data back to the people (Lee 2019; René & Mapes 2019; Tapscott & Tapscott 2017; Voshmgir 2020).

Societal Implications

From a deeper sociological perspective, the research results indicate that blockchain has the potential to address some of the issues presented, including tackling private property issues; facilitating the democratization of data; mitigating power relations by eliminating particular intermediaries and their services; flattening asymmetries in information access and sharing; enabling decentralized digital identities that are empowered through the full control of both their decentralized identifiers (DIDs) and data; and facilitating the creation of a new architecture of trust. Importantly, since trust is a complex societal construct based on social relationships and other human aspects, serving as a glue that holds society together, it cannot be simply written into code and be replaced by technology. Trust is never solely technological.

Building blockchain-based trustless systems does not imply that the levels of trust are no longer involved or needed. Instead, trust shifts from institutions, intermediaries, and other central authorities to trust in technology. Trust in technology requires both knowledge and technical skills. If insufficiently educated people enter the realm, the risks arise of them being exploited or manipulated by the coders and architects of decentralized networks. This can facilitate the separation of regular users and those who possess superior knowledge and skills (technocracy), rather than facilitating inclusiveness.

Robust and functioning systems allow to build trust in technology over time, leading to greater acceptance and adoption. Therefore, it will be crucial in the coming years to build such a robust system, in which people can trust and build confidence, in order to implement and utilize the potential of smart contracts better than they are used today.

Decentralized systems based on blockchain technology carry the possibility of organizing and coordinating interactions in a less hierarchical manner, with shifting power dynamics and more control for people. Thus, when properly implemented, blockchain not only facilitates the democratization of information access, control, and ownership but also promotes greater equity by eliminating fee-charging intermediaries, facilitating reward-sharing systems and incentive mechanisms, enabling new forms of income, and potentially shifting class relations.

Future Research

The research further indicates that a hybrid system that combines governmental services with blockchain-based decentralized architecture presents an intriguing avenue for future research. Researchers may engage with the question of potential trade-offs, addressing challenges in both centralized and decentralized systems, and should focus on exploring ways to maximize the advantages of both and developing robust systems that encompass empowerment and appropriate regulatory oversight. Countries such as Estonia have already explored the advantages of both approaches in their national e-governance strategy (E-Estonia, accessed 18th July 2024). Such examples could thereby serve as valuable case studies and offer insights into the practical implementation of decentralized digital identity systems at the national level.

Examining the phenomenon of estrangement is another intriguing sociological issue for future research. As Marx (1844/1932) pointed out, the objectification of labor in combination with the lack of ownership facilitates alienation and further amplifies asymmetries and inequalities in power and control. Future research may investigate whether the *Quantification of the Social* (Mau 2019) contributes to a better understanding of data and its usage – through e.g., fitness trackers – and ultimately to greater connection to data; moreover, could this further reduce objectification, diminish alienation, and ultimately mitigate asymmetries in power and control?

Limitations

It is beyond the scope of this study to address the question of the definition of data ownership. Therefore, it may be advisable for scholars to actively engage in this issue and further push for a universal definition and clarity.

The limitations of this study are also acknowledged by the relatively small sample of experts. A larger sample would allow us to gather more imaginaries regarding this topic and unravel the different understandings and visions of different industries and branches.

As the development around blockchain applications for data ownership is increasing and raising attention, more real-world implementations and case studies emerge. This development suggests that researchers should expand this study to other industries and fields of society, including the medical sector or institutional e-health services.

However, one limitation of this research is that it could not determine whether the decentralized nature of blockchain will ultimately bring forth more democratic societies.

One additional recommendation for future research is to dive into the worlds of decentralized systems by exploring and examining decentralized communities, providing an opportunity for investigation through the lens of digital sociology.

Concluding words

Both data ownership and blockchain technology lack a unified definition, which can lead to confusion in debates. However, recent developments demonstrate awareness at various levels and extents, which may encourage further discussion and necessitate clarity.

The concept of imaginaries plays a crucial role not only in contributing to a more comprehensive understanding of emerging technologies and their implications but also in underscoring the importance of examining the visions, motivations, and (un)desired outcomes, particularly of those that drive innovation and technological development or with great influential power.

The struggle between advocates of democratic data ownership infrastructures and those profiting from the information centralization and monetization persists and requires careful observation.

Technology itself does not determine our direction; it is up to us how we use it and what we make out of these tools. We can either create greater surveillance and power mechanisms or we can utilize technology for societal benefit, building democratic infrastructures that finally allow us to own what we produce – our data.

9 References

ASKARANY, D.. (2016): Attributes of innovation and management accounting changes. Contemporary Management Research. 12(4). 455-466. https://doi.org/10.7903/cmr.1144.

ASOKAN, D.R., Huq, F.A., Smith, C.M., & Stevenson, M.. (2022): Socially responsible operations in the Industry 4.0 era: post-COVID-19 technology adoption and perspectives on future research. International Journal of Operations & Production Management. Vol. 42 No. 13. pp. 185-217. https://doi.org/10.1108/IJOPM-01-2022-0069.

ASSWAD, J, & Marx Gómez J.. (2021): Data Ownership: A Survey. Information. 12(11):465. https://doi.org/10.3390/info12110465.

ALEXOPOULUS, C., Charalabidis, Y., Loutsaris, M.A., Lachana, Z..(2021): How blockchain technology changes government. International Journal of Public Administration in the Digital Age. https://doi.org/10.4018/IJPADA.20210101.oa10

ALLEN, C.. (2016): The path to self-sovereign identity. https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/ (last retrieved 18th August 2024).

ALSTON, E., Law, W., Murtazashvili, I., & Weiss, M. B. H.. (2021): Blockchain Networks as Constitutional and Competitive Polycentric Orders. Journal of Institutional Economics. 1– 17. https://doi.org/10.2139/ ssrn.3887701.

ANDROULAKI, E., Manevich, Y., Muralidharan, S., Murthy, C.; Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., et al.. (2018): Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference—EuroSys ’18. Porto. Portugal. 23–26 April 2018. ACM Press: New York. NY. USA. pp. 1–15.

ATKINSON, Robert D., Doug Brake, Daniel Castro, Colin Cunliff, Joe Kennedy, Michael McLaughlin, Alan McQuinn, & Joshua New. (2019): A Policymaker’s Guide to the “Techlash” —What It Is and Why It’s a Threat to Growth and Progress. Information Technology & Innovation Foundation.

AZARIA, A.; Ekblaw, A., Vieira, T., & Lippman, A.. (2016): MedRec: Using Blockchain for Medical Data Access and Permission Management. In: Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD). Vienna. Austria. 22–24 August 2016. IEEE: Piscataway. NJ. USA. 2016. pp. 25–30.

BACK, Adam. (2002): Hashcash - A Denial of Service Counter-Measure.

BAHGA, A., & Madisetti, V. K.. (2017): Blockchain Applications: A Hands-On Approach. Berlin: VPT.

BERNERS-LEE, T.. (2000): Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor. New York: Harper Collins Books.

BIRCH, Kean, & Kelly Bronson. (2022): Big Tech, Science as Culture. 31:1. 1-14.

BROOKER, K. (2018, July 1): “I was devastated”: Tim Berners-Lee, the man who created the world wide web, has some regrets. Vanity Fair. https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets (last retrieved 14th September 2024).

BYUN, C.. (2014): The Economics of the Popular Music Industry: Modelling from Microeconomic Theory and Industrial Organization 95.

CACHIN, C.. (2016): Architecture of the Hyperledger Blockchain Fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Academic Press: Cambridge. MA. USA.

CAREJA, Alexandru-Cristian Careja, & Nicolae Tapus. (2023): Digital Identity Using Blockchain Technology. Procedia Computer Science, Volume 221. Pages 1074-1082. ISSN 1877-0509. https://doi.org/10.1016/j.procs.2023.08.090.

CHAUM, David. (1981): Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84-88. URL: https://doi.org/10.1145/358549.358563.

CHERGAROVA, Vasilka, Vinicius Arcanjo, Mel Tomeo, Jeronimo Bezerra, Luis Marin Vera, & Anthony Uloa. (2022): Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency. In: Issues in Information Systems. Vol. 23.

CLARKE, Roger. (1994): Human Identification in Information Systems: Management Challenges and Public Policy Issues. Information Technology & People 7. no. 4. 6-37.

COHEN, Julie E.. (2019): Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University.

DAI, J., & M. A. Vasarhelyi. (2017): Toward Blockchain-Based Accounting and Assurance. Journal of Information Systems 31 (3): 5–21. doi:10.2308/isys-51804.

DÁVILA, Joshua. (2023): Blockchain Radicals: How Capitalism Ruined Crypto and How to Fix It. Watkins Media Limited.

DE FILIPPI, P., MANNAN, M., & REIJERS, W.. (2020): Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62(June), 101284.

DE FILIPPI, P. & Wright, A.. (2018): Blockchain and the law: The Rule of Code. New York: Harvard University Press.

DEGUCHI, A. et al. (2020): What Is Society 5.0?. In: Society 5.0. Springer. Singapore. https://doi.org/10.1007/978-981-15-2989-4_1.

DIAZ, A.. (2008): „Through the Google Goggles. Sociopolitical Bias in Search Engine Design.” In: A. Spink and M. Zimmer (eds.) Web Search. Multidisciplinary perspectives. Heidelberg: Springer: 11-34.

DIETRICH, Fabian & Louw, Louis & Palm, Daniel. (2023): A Systematic Literature Review Of Blockchain-Based Traceability Solutions. 10.15488/13509.

DIFFIE, W. & M.E. (1976): Hellman. New directions in cryptography. IEEE Trans. on Information Theory 22(6):644–654.

DUAN, Keru, Gu Pang, & Yong Lin. (2023): Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management. Journal of Digital Economy. Volume 2.

DURKHEIM, Émile. (1893): De la Division du travail social: étude sur l'organisation dessociétés supérieures. Paris: Alcan.

DURKHEIM, Émile. (2014): The division of labor in society (S. Lukes, Ed.; W. D. Halls. Trans.; Free Press trade paperback edition). Free Press.

E-ESTONIA. e-estonia.com (last retrieved 18th July 2024).

ELIAS, Norbert. (1982): State Formation and Civilization (volume 2 of The Civilizing Process). Oxford: Blackwell.

FLANDERS, Wally. (2023 July 24): 1 VP Al Gore @ ITU Telecom Conference in Buenos Aires A Network of Networks CSPAN 3:24:94. [Video]. YouTube. https://www.youtube.com/watch?v=bS2PkQ_pWgc (last retrieved 26th August 2024).

FUSO, Francesco, Lunesu, Maria Ilaria & Pani, Filippo & Pinna, Andrea. (2018): Crypto-voting, a Blockchain based e-Voting System. 223-227. 10.5220/0006962102230227.

GEORGESON, David A.. (2018): Cryptocurrencies as an Alternative to Fiat Monetary Systems. Applied Economics Theses. 35. http://digitalcommons.buffalostate.edu/economics_theses/35.

GIDDENS, Anthony. (1971): Capitalism and Modern Social Theory: An Analysis of the Writings of Marx. Durkheim and Max Weber. Cambridge. Cambridge University Press. HM19 G53.

GIDDENS, Anthony. (1990): The Consequences of Modernity. Oxford. Polity Press.

GORD, Michael. (2016): Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality. Bitcoin Magazine. 26. https://bitcoinmagazine.com/technical/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751.

GLASER, Barney, & Strauss, Anselm. (1967): The Discovery of Grounded Theory. Strategies for Qualitative Research. Chicago: Aldine.

GLÄSER, Jochen, & Grit Laudes. (2006): Experteninterviews und qualitative Inhaltsanalyse als Instrument rekonstruierender Untersuchungen. 2. durch- gesehene Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

HABER, S., & Stornetta, W.S.. (1991): How to time-stamp a digital document. J. Cryptology 3, 99–111. https://doi.org/10.1007/BF00196791.

HARARI, Y.. (2019): 21 lessons for the 21st century. Vintage.

HART, D.. (2002): Ownership as an Issue in Data and Information Sharing: A Philosophically Based View. Australas.

HEAP, Imogen. (2017): Blockchain Could Help Musicians Make Money Again. Harvard Business Review. June 5. 2017. available at https://hbr.org/2017/06/blockchain- could-help-musicians-make-money-again, [https://perma.cc/D9XF-HPJK].

JANEČEK, V.. (2018): Ownership of Personal Data in the Internet of Things. Comput. Law Secur. Rev.. 34. 1039–1052.

JANSSEN, Marijn, Vishanth Weerakkody, Elvira Ismagilova, Uthayasankar Sivarajah, & Zahir Irani. (2020): A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. International Journal of Information Management. Volume 50.

JASANOFF, Sheila. (2015): "Future Imperfect: Science, Technology and the Imaginations of Modernity." In: Dreamscapes of Modernity: Sociological Imaginaries and the Fabrications of Power. edited by Sheila Jasanoff and Sang-Hyun Kim. 1–33. Chicago: University of Chicago Press.

JASANOFF, S, & Kim, S-H.. (2015): Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power. Chicago. IL. U.S.: University of Chicago Press.

KARAFILOSKI, E. & Mishev, A.. (2017): Blockchain Solutions for Big Data Challenges: A Literature Review. In Proceedings of the IEEE EUROCON 2017-17th International Conference on Smart Technologies. Ohrid. Macedonia, 6–8 July 2017. pp. 763–768.

LARIOS-HERNÁNDEZ, G. J.. (2017): Blockchain entrepreneurship opportunity in the practices of the unbanked. Business Horizons. 60(6). 865—874.

LACITY, M.. (2018): A Manager's Guide to Blockchain for Business: From Knowing What to Knowing How. Warwickshire. UK: SB Publishing.

LEE, Jei Young. (2019): A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Business Horizons. Volume 62. Issue 6. Pages 773-784. ISSN 0007-6813. https://doi.org/10.1016/j.bushor.2019.08.003.

LIANG, X., Zhao, J., Shetty, S., Liu, J., & Li, D.. (2017): Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. In: Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal. QC. Canada. 8–13 October 2017. IEEE: Piscataway. NJ. USA. 2017. pp. 1–5.

LIEBKIND, Joe. (2017): Are Smart Contracts the Best of Blockchain? Investopedia. https://www.investopedia.com/news/are-smart-contracts-best-block chain/.

LIU, Y., Z. Zhao, G. Guo, X. Wang, Z. Tan & S. Wang. (2017): An Identity Management System Based on Blockchain. 15th Annual Conference on Privacy, Security and Trust (PST). Calgary. AB. Canada. 2017. pp. 44-4409. doi: 10.1109/PST.2017.00016.

LUHMANN, Niklas. (1979): Trust and Power. Chichester. Wiley.

LYON, David. (2007): Surveillance Studies: An Overview. Cambridge: Polity Press.

MAGER, Astrid. (2010): Mediated health: Sociotechnical practices of communicating medical knowledge via the web and their epistemic implications [Doctoral dissertation. University of Vienna]. University of Vienna Repository.

MANSKI, S.. (2017): Building the Blockchain World: Technological Commonwealth or Just More of the Same? Strategic Change 26 (5): 511–522. doi:10.1002/jsc.2017.26.issue-5.

MARX, Karl. (1887): Capital: A critique of political economy (Vol. 1. S. Moore & E. Aveling, Trans.; F. Engels. Ed.). Progress Publishers. (Original work published 1867).

MARX, Karl. (1844/1932): Economic and philosophic manuscripts of 1844 (M. Milligan, Trans.). Progress Publishers. (Original work written 1844. first published 1932).

MARX, Karl, & Engels, Friedrich. (1848/1969): Manifesto of the Communist Party. In Selected Works (Vol. 1, pp. 98-137). Progress Publishers. (Original work published 1848).

MARX, Karl, & Friedrich Engels. (1848/1998): The Communist Manifesto. Oxford: Oxford University Press.

MARX, Karl. (1959): Economic and philosophic manuscripts of 1844. (M. Milligan, Trans.). Progress Publishers. (Original work published 1932).

MARX, Karl. (1994): Selected Writings. Trans. and Ed. Lawrence Simon. Indiana: Hackett Publishing Company, 1994.

MAU, S.. (2019): The Metric Society (1st ed.). Wiley.

MAYRING, Philipp. (2000): Qualitative Content Analysis [28 paragraphs]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1(2). Art. 20.

MAYRING, Philipp. (2010): Qualitative Inhaltsanalyse Beltz Verlagsgruppe, 69 469 Weinheim, ISBN: 9783407291424.

MAYRING, Philipp. (2014): Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt, 2014.URN: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-395173.

McCONAGHY, M., McMullen, G., Parry, G., McConaghy, T., & Holtzman, D.. (2017): Visibility and Digital Art: Blockchain as an Ownership Layer on the Internet. Strategic Change: Briefings in Entrepreneurial Finance. SI on Blockchain Applications. 26(5). 461-470.

McNEIL, M. C., MacKenzie, A. B., Tutton, R. J. C., Haran, J., & Arribas-Ayllon, M.. (2017): Conceptualizing imaginaries of science, technology, and society. In: U. Felt, R. Fouche, C. A. Miller, & L. Smith-doerr (Eds.). The Handbook of Science and Technology Studies (4th ed.. pp. 435-464). Article 10 MIT Press. Cambridge, Mass..

MOUGAYAR, W.. (2016): The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley, New Jersey.

MINERAUD, J.; Mazhelis, O.; Su, X.; & Tarkoma, S.. (2016): A Gap Analysis of Internet-of-Things Platforms. Comput. Commun. 89–90. 5–16.

MISZTAL, B.A.. (1992): The Notion of Trust in Social Theory. Policy and Society. 5(1). 6-15.

MOHANTA, B., Panda, S. & Jena, D.. (2018): An Overview of Smart Contract and Use cases in Blockchain Technology. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Vorab-Onlinepublikation. https://doi.org/10.1109/ICCCNT.2018.8494045.

MORABITO, Vincenzo. (2017): Business Innovation Through Blockchain. 10.1007/978-3-319-48478-5.

MORTAZAVI, Sohale Andrus. (2021): Cryptocurrency Is a Giant Ponzi Scheme. In: Jacobin. Economy, Science and Technology. https://jacobin.com/2022/01/cryptocurrency-scam-blockchain-bitcoin-economy-decentralization.

NAKAMOTO, S.. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

OSBORNE, Richard & Dave Laing. (2021): Music by Numbers: The Use and Abuse of Statistics in the Music Industries. Intellect Books.

O´DWYER, R.. (2015): The Revolution will (not) be Decentralized: Blockchains. Commons Transition.

OCEAN PROTOCOL. (2017): Ocean Protocol. 3rd November. https://www.youtube.com/watch?v=FEeicvNSyk4 (last retrieved 9th July 2024).

OCHS, C., Büttner, B., & Lamla, J.. (2021): Trading Social Visibility for Economic Amenability: Data-based Value Translation on a "Health and Fitness Platform." Science, Technology, & Human Values, 46(3), 480–506. https://doi.org/10.1177/0162243920928138.

ÖNDER, I., & Treiblmaier, H.. (2018): Blockchain and tourism: three research propositions. Ann. Tour. Res. 72:5. doi: 10.1016/j.annals.2018.03.005.

PARSONS, T.. (1970): Research with Human Subjects and the Professional Complex. In: Freund, P. (ed), Experimentations with Human Subjects. New York.

PEREZ, Yessi Bello, & Imogen Heap. (2018): Decentralising the Music Industry with Blockchain, Mycelia For Music, http://myceliaformusic.org/2016/05/14/imogen-heap-decentralising-the-music-industry-with-blockchain/. [https://perma.cc/LF2T-GYBK] (last visited 10th July, 2024).

PETERS, G.W. & Panayi, E.. (2015): Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Social Science Research Network.

PFADENHAUER, M.. (2009): At eye level: The expert interview—A talk between expert and quasi- expert. In Interviewing experts (pp. 81–97). Springer.

PISA, Michael & Matt Juden. (2017): "Blockchain and Economic Development: Hype vs. Reality." CGD Policy Paper. Washington, DC: Center for Global Development. https://www.cgdev.org/publication/ blockchain-and-economic-development-hype-vs-reality.

PRATHI, Gopi. (2022): Blockchain in Media and Entertainment.

QUACH, S., Thaichon, P., & Martin, K.D. et al.. (2022): Digital technologies: tensions in privacy and data. J. of the Acad. Mark. Sci. 50. 1299–1323. https://doi.org/10.1007/s11747-022-00845-y.

RAGNEDDA, M. & G. Destefanis (Eds.). (2020): Blockchain and web 3.0: Social, economic, and technological challenges routledge. https://doi.org/10.4324/9780429029530-8.

REED, D., Preukschat, A., & Allen, C. (2020): Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning Publications.

REIJERS, W., Brolcháin, F. O., & Haynes, P.. (2016): Governance in Blockchain Technologies & Social Contract Theories. Ledger Journal. 1(1). 134–151. https://doi.org/10.5915/LEDGER.2016.62.

ROGERS, E.. (2003): The Diffusion of Innovations. Fifth Edition. The Free Press. New York. (247).

ROUSSEAU, J.-J.. (1762): The Social Contract and Discourses. London. Everyman.

ROZAS, D., Tenorio-Fornés, A., & Hassan, S.. (2021): Analysis of the Potentials of blockchain for the governance of Global Digital Commons. Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2021.577680.

SAARIKKO, T., Westergren, U.H., & Blomquist, T.. (2017): The Internet of Things: Are You Ready for What's Coming? Bus. Horizons 2017. 60. 667–676.

SANDSTROM, Gregory. (2017): Who Would Live in a Blockchain Society? The Rise of Cryptographically-Enabled Ledger Communities. Sociol Epistemology Review and Reply Collective 6. No.5.

SEMENZIN, Silvia & Rozas, David & Hassan, Samer. (2022): Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. Policy and Society. 41. 10.1093/polsoc/puac014.

SEMENZIN, S.. (2023): 'Blockchain for good': Exploring the notion of social good inside the blockchain scene. Big Data & Society, 10(2). https://doi.org/10.1177/20539517231205479.

SCHLATT, V., Schweizer, A., Urbach, N., & Fridgen, G.. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

SCHUMPETER, J. A.. (1943): Capitalism, socialism and democracy. Routledge.

SCHILLER, Dan.. (2000): Digital Capitalism: Networking the Global Market System. MIT Press Books,.The MIT Press. edition 1, volume 1.

SIMMEL, Georg. (1900): The Philosophy of Money.

SIMMEL, Georg. (1908): Untersuchungen über die Formen der Vergesellschaftung, Duncker & Humblot, Berlin 1908.

SIMMEL, Georg. (1910): How is Society Possible? American Journal of Sociology. 16(3). 372–391. http://www.jstor.org/stable/2763090.

SMITH, A, & STIRLING, A.. (2018): Innovation, Sustainability and Democracy: An Analysis of Grassroots Contributions. Journal of Self-Governance and Management Economics. 6(1). 64-97.

SRNICEK, Nick. (2017): Platform Capitalism. Malden, MA: Polity Press.

SRNICEK, N. & Williams A.. (2015): Inventing the future: postcapitalism and a world without work. Verso Books.

STAAB, P.. (2021): Digitaler Kapitalismus. (3. Auflage). Suhrkamp Verlag.

STATISTA. (2024): Ethereum (ETH) - statistics & facts. https://www.statista.com/topics/8807/ethereum-eth/ (last retrieved 25th September 2024).

STRAUSS, A., & CORBIN, J.. (1990): Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park. CA: Sage.

STRÜCKER, Jens & Simon Albrecht & Stefan Reichert. (2019): "Blockchain in the Energy Sector," Springer Books. In: Horst Treiblmaier & Roman Beck (ed.). Business Transformation through Blockchain, chapter 2. pages 23-51. Springer.

SULLIVAN, Clare. (2018): Digital identity – From emergent legal concept to new reality. Computer Law & Security Review. Volume 34. Issue 4. Pages 723-731. ISSN 0267-3649. https://doi.org/10.1016/j.clsr.2018.05.015.

SWAN, M.. (2015): Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.. Sebastopol.

TAGHDIRI, A. (2019): How Blockchain Technology Can Revolutionize the Music Industry. Harvard Journal of Sports and Entertainment Law.

TAPSCOTT D, & TAPSCOTT A.. (2016): Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. New York. NY. US: Penguin.

TAPSCOTT, Don & TAPSCOTT, Alex. (2017): Realising the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. Geneva: World Economic Forum.

TENG, J. T. C., Grover, V., & Güttler, W.. (2002): Information technology innovations: general diffusion patterns and its relationships to innovation characteristics. IEEE Transactions on Engineering Management. 49(1). 13-27. https://doi.org/10.1109/17.985744.

TREIBLMAIER, Horst. (2018): The impact of the Blockchain on the supply chain: a theory-based research framework and a call for action. Supply Chain Manage. 23. 545–559. doi: 10.1108/SCM-01-201 8-0029.

TREIBLMAIER, Horst, & Zeinzinger, T.. (2018): "Understanding the Blockchain through a gamified experience: a case study from Austria." 25th European Conference on Information Systems (Portsmouth: UK).

TREIBLMAIER, Horst, & Beck, R.. (2019a): Business Transformation Through Blockchain—Volume I. Cham: Palgrave Macmillan.

TREIBLMAIER, Horst, & Beck, R.. (2019b): Business Transformation Through Blockchain – Volume II. Cham: Palgrave Macmillan.

TREIBLMEIER, Horst. (2019): Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. Front. Blockchain 2:3.

TREIBLMAIER, Horst, & Umlauff, U.. (2019): Blockchain and the future of work: a self-determination theory approach. In: Blockchain Economics: Implications of Distributed Ledger Technology. eds M. Swan, J. Potts, S. Takagi, P. Tasca, & F. Witte (New Jersey. NJ). 105–124. doi: 10.1142/978178634639 1_0006.

VAN ASBROECK, B., Debussche, J., & César, J.. (2017): Building the European Data Economy: Data Ownership. White Paper. Bird & Bird: London, UK.

VAN DER CRUIJSEN, Carin, de Haan, Jacob & Rooij, Maarten. (2023): The Impact of High Inflation on Trust in National Politics and Central Banks (January 17, 2023). De Nederlandsche Bank Working Paper No. 762. Available at SSRN: https://ssrn.com/abstract=4330151 or http://dx.doi.org/10.2139/ssrn.4330151.

VARYS, Barry & Duane, Ja-Nae & Marabelli, Marco. (2022): Power Dynamics in the Evolution of Blockchain.

VEITH, H.. (2023): DIPLOMARBEIT Umsetzung von Blockchain-Anwendungen im Energiesektor, am Beispiel von Energiegemeinschaften. In Fakultät Für Architektur Und Raumplanung [Thesis. Diplomarbeit]. Technische Universität Wien. https://repositum.tuwien.at/bitstream/20.500.12708/176695/1/Veith%20Helena%20-%202023%20-%20Umsetzung%20von%20Blockchain-Anwendungen%20im%20Energiesektor%20am.pdf.

VOSHMGIR, Shermin. (2020): Token Economy: How the Web3 reinvents the Internet.

WAN, S.. (2021): CryptoSlate. Internet vs. crypto adoption chart predicts 1 billion users by2027. from https://cryptoslate.com/internet-vs-crypto-adoption-chart-predicts-1-billion-users-by-2027. (last retrieved August 2nd 2024).

WARK, McKenzie. (2004): A Hacker Manifesto. Cambridge. MA: Harvard University Press.

WEBER, Max. (1904–1905): The Protestant ethic and the spirit of capitalism.

WEBER, Max. (1978): Economy and Society: An Outline of Interpretive Sociology. Edited by G. Roth and C. Wittich. Berkeley et al.. University of California Press.

WEBER, Max. (2001): The Protestant ethic and the spirit of capitalism (T. Parsons, Trans.; A. Giddens. Intro.). Routledge Classics. (Original work published 1904–1905).

WERBACH, K.. (2018): The blockchain and the new architecture of trust. The MIT Press. https:// doi.org/ 10.7551/mit- press/11449.001.0001 (retrieved January 25th 2023).

WOODSIDE, Joseph M., Augustine, Fred K. Jr., & Giberson, Will. (2017): Blockchain Technology Adoption Status and Strategies. Journal of International Technology and Information Management: Vol. 26: Iss. 2. Article 4. DOI: https://doi.org/10.58729/1941-6679.1300).

WRIGHT, Aaron & De Filippi, Primavera. (2015): Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal. 10.2139/ssrn.2580664.

YING, Peng, Chen, X., & Wang, X.. (2022): Enhancing supply chain flows through blockchain: a comprehensive literature review. International Journal of Production Research. 61(13). 4503–4524. https://doi.org/10.1080/00207543.2022.2157064.

YLI-HUUMO, J., Ko, D., Choi, S., Park, S., & Smolander, K.. (2016): Where is current research on blockchain technology? A systematic review. PLoSONE 11:0 163477. doi: 10.1371/journal.pone.0163477.

ZNANIECKI, F.. (1965): Social Relations and Social Roles: The Unfinished Systematic Sociology. San Francisco: Chandler.

ZUBOFF, S., & Schwandt, K.. (2019): The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books.

ZYSKIND, G., & Nathan, O. et al.. (2015): Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW). 2015 IEEE. IEEE. pp.180–184.

Internet References:

https://www.biblegateway.com/blog/2016/07/the-wired-soul-an-interview-with-tricia-mccary-rhodes/ (last retrieved August 1st 2024)

https://coinpaper.com/2977/how-many-blockchains-are-there-unveiling-the-ecosystem-s-diversity (last retrieved June 26th 2024)

https://cointelegraph.com/news/crypto-on-track-1-billion-users-end-2025-analyst (last retrieved June 10th 2024)

https://crypto.com/company-news/global-cryptocurrency-owners-grow-to-580-million-through-2023 (last retrieved June 18th)

https://www.economist.com/united-states/2024/04/17/americas-trust-in-its-institutions-has-collapsed (last retrieved May 24th 2024)

https://e-estonia.com/ (last retrieved 1st August 2024)

https://www.edelman.com/sites/g/files/aatuss191/files/2019-04/2019_Edelman_Trust_Barometer_Technology_Report.pdf (last retrieved July 7th 2024)

https://ethereum.org/en/developers/docs/smart-contracts/) (last retrieved June 14th 2024)

https://etherscan.io/chart/active-address (last retrieved 28th June 2024).

https://www.eurofound.europa.eu/en/blog/2022/trust-national-institutions-falling-data-behind-decline (last retrieved June 14th 2024)

https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx (last retrieved June 3rd 2024)

https://www.identity.com/preventing-data-breaches-with-decentralized-identity/ (last retrieved May 20th 2024) https://www.identity.com/what-is-identity-theft/ (last retrieved May 20th 2024)

https://www.ig.com/en-ch/trading-strategies/what-is-blockchain-technology--200710 (last retrieved August 26th 2024)

https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview (last retrieved September 6th 2024)

https://markmetry.medium.com/blockchain-technology-is-the-most-significant-invention-since-the-internet-and-electricity-f2d44a631ef6 (last retrieved May 20th 2024)

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/straight-talk-about-big-data (last retrieved July 5th 2024)

https://www.microsoft.com/en-us/security/blog/2022/03/10/why-decentralization-is-the-future-of-digital-identities/ (last retrieved September 6th 2024)

https://www.nasdaq.com/articles/crypto-to-have-1-billion-users-in-10-years-says-coinbase-ceo (last retrieved July 10th 2024)

https://www.oesterreich.gv.at/id-austria.html (last retrieved September 8th 2024)

https://oceanprotocol.com/ (last retrieved July 9th 2024)

https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html (last retrieved August 1st 2024)

https://thex.press/digital-identity-verification-evolution/ (last retrieved August 15th 2024)

https://www.triple-a.io/cryptocurrency-ownership-data (last retrieved July 10th 2024)

https://www.youtube.com/watch?v=FEeicvNSyk4 (last retrieved July 9th 2024)