Adoption of cryptocurrencies by millennials in Vienna: Is there a future for Decentralized Finance (DeFi)?

Master Thesis submitted in fulfillment of the Degree

Master of Science

in Management

Submitted to Dr. Horst Treiblmaier

Benjamin Šafarič

1823006

Vienna, 17.6.2021

AFFIDAVIT

I hereby affirm that this Master's Thesis represents my own written work and that I have used no sources and aids other than those indicated. All passages quoted from publications or paraphrased from these sources are properly cited and attributed.

The thesis was not submitted in the same or in a substantially similar version, not even partially, to another examination board and was not published elsewhere.

17.6.2021

Date

ABSTRACT

Cryptocurrencies are a relatively new topic in finance accompanied by many unknowns of Blockchain technology. This paper aims to analyze the adoption of cryptocurrencies from the aspect of millennials and financial institutions. This is increasingly important because of the transition from Web 2.0 to 3.0 and the disruptive potential of decentralized finance (DeFi) which represents a challenge for major stakeholders in the modern economy. For many years, financial experts have been talking about stocks, bonds, and other traditional assets but a new asset class, particularly interesting for web-savvy millennials, might change this narrative. Cryptocurrencies not only challenged traditional assets but disrupted the legacy financial industry and opened new questions, such as how to classify, define and regulate them. Cryptocurrencies and digital assets led to the emergence of decentralized finance (DeFi), and the question of whether it could be the future of finance. Industry experts and academics are questioning whether decentralized financial models (DeFi) will disrupt traditional finance. This master's thesis aims to analyze in more detail Blockchain technology and the future of DeFi as well as whether and to what extent millennials in Vienna have adopted cryptocurrencies.

Keywords: Web 3.0, Blockchain technology, DeFi, Cryptocurrencies, Millennials.

ACKNOWLEDGEMENTS (OPTIONAL)

A list of institutions and people who may have contributed to your thesis, which you think deserve a mention under this heading.

TABLE OF CONTENTS

Affidavit I

Abstract II

Acknowledgements (optional) III

List of Figures VII

List of Abbreviations IX

1 Introduction 10
1.1 Research questions 11
1.1.1 First research question 11
1.1.2 Second research question 12
1.1.3 Third research question 12
1.2 Thesis structure 13

2 Theoretical part – literature review 15
2.1 Blockchain in general 15
2.2 Blockchain 17
2.2.1 Advantages and disadvantages of Blockchain technology 18
2.3 Blockchain in banking and finance 22
2.4 Blockchain in other sectors 24
2.5 Consensus mechanism 27
2.5.1 Proof of work 27
2.5.2 Proof of stake 29

3 Cryptocurrencies 31
3.1 The definition and history of money 31
3.2 Concept and legal framework of cryptocurrencies 34
3.3 The concept of Bitcoin 35
3.4 Ethereum 38
3.5 Decentralized finance - DeFi 44
3.6 The impact of cryptocurrencies on developing countries 48
3.7 Problems caused by the emergence of cryptocurrencies and illegal activity 49

4 Millennials 51
4.1 The concept of millennials 51

5 Research part 53
5.1 Purpose statement 53

5.2 Research approach 53
5.3 Research objectives 53
5.4 Research methodology 54
5.4.1 Survey 54
5.4.2 Interview 56

6 RESULTS AND DISCUSSIONS 58
6.1 Questionnaire 58
6.2 Hypothesis analysis 75
6.3 Interview results 85
6.3.1 First expert interview 85
6.3.2 Second expert interview 87

7 Conclusion 89
7.1 First research question 89
7.2 Second research question 90
7.3 Third research question 91
7.4 General conclusion 92

8 Literature 94

9 Appendices 105
9.1 Appendix A: Questionnaire 105
9.2 Appendix B: Interviews 110
9.2.1 First expert interview 110
9.2.2 Second expert interview 112
9.3 Appendix C: SPSS output 114

LIST OF TABLES

TABLE 1. POSITIVE AND NEGATIVE EFFECTS OF BLOCKCHAIN TECHNOLOGY 19
TABLE 2. EVALUATING ETHEREUM L2 SCALING SOLUTIONS: A COMPARISON FRAMEWORK 43

LIST OF FIGURES

FIGURE 1. BLOCKCHAIN DESIGN 17
FIGURE 2. ENCRYPTION PROCESS 18
FIGURE 3. BITCOIN BLOCKCHAIN – WHAT IS PROOF OF WORK? 28
FIGURE 4. HOW LONG IT WILL TAKE FOR BITCOIN TO BE BROKEN BY QUANTUM COMPUTING 29
FIGURE 5. BITCOIN AND ETHEREUM PROTOCOL LAYERS & TECH STACK, FRAMING BITCOIN 40
FIGURE 6. MOST POPULAR INVESTMENT CATEGORIES 44
FIGURE 7. DEFI DIGEST AND COMMON ISSUES 45
FIGURE 8. TOTAL VALUE LOCKED IN DEFI 46
FIGURE 9. SURVEY QUESTION 1. "GENDER" 58
FIGURE 10. SURVEY QUESTION 2. "AGE" 58
FIGURE 11. SURVEY QUESTION 4. "FAMILIARITY WITH BLOCKCHAIN TECHNOLOGY"-LIKERT SCALE 59
FIGURE 12. SURVEY QUESTION 5. "PERFORMANCE EXPECTANCY"- LIKERT SCALE 59
FIGURE 15. SURVEY QUESTION 8. „FACILITATING CONDITIONS" – MULTIPLE-CHOICE 61
FIGURE 16. SURVEY QUESTION 9. „HEDONIC MOTIVATION" – MULTIPLE-CHOICE 62
FIGURE 17. SURVEY QUESTION 10. „PRICE VALUE" – MULTIPLE-CHOICE 63
FIGURE 18. SURVEY QUESTION 11. „HABIT" – MULTIPLE-CHOICE 63
FIGURE 19. SURVEY QUESTION 12. „THINKING ABOUT THE NEXT 2 YEARS WOULD YOU?" – MULTIPLE-CHOICE 64
FIGURE 20. SURVEY QUESTION 13. „CRYPTOCURRENCIES CAN EASILY BE CONVERTED INTO CASH" 65
FIGURE 21. SURVEY QUESTION 14. „IT'S A GOOD TIME TO BUY CRYPTOCURRENCIES" 66
FIGURE 22. SURVEY QUESTION 15. „IF THE ECB ISSUES ITS OWN CRYPTOCURRENCY WOULD YOU?" 67
FIGURE 23. SURVEY QUESTION 16. „WHICH OF THE FOLLOWING ACTIVITIES WOULD YOU ACCEPT?" 67
FIGURE 24. SURVEY QUESTION 17. „WOULD CRYPTOCURRENCIES IN "PAPER FORM" INCREASE TRUST AND ADOPTION ?" 68
FIGURE 25. SURVEY QUESTION 18. „DO YOU TRUST FINANCIAL INSTITUTIONS?" 69
FIGURE 26. SURVEY QUESTION 19. „ARE YOU FAMILIAR WITH THE CONCEPT OF DECENTRALIZED FINANCE?" 69
FIGURE 27. SURVEY QUESTION 20. „IF CRYPTOCURRENCIES (AND DECENTRALIZED FINANCE) WOULD REPLACE BANKS (AND TRUST-BASED FINANCIAL INSTITUTIONS), WHAT WOULD BE THE EFFECT?„ 70
FIGURE 28. SURVEY QUESTION 21. „DO YOU THINK THAT YOUR FINANCIAL EDUCATION IS IN THE BEST INTEREST OF YOUR GOVERNMENT OR BANK? 71
FIGURE 37. SURVEY QUESTION 22. „SHOULD THE GOVERNMENT RESTRICT THE USE OF CRYPTOCURRENCIES?" 71
FIGURE 30. SURVEY QUESTION 23. „WOULD CYBER-CRIME INCREASE WITH THE USE OF CRYPTOCURRENCIES?„ 72
FIGURE 31. SURVEY QUESTION 24. "BLOCKCHAIN AND CRYPTOCURRENCIES AS A SCHOOL SUBJECT?" 73
FIGURE 41. SURVEY QUESTION 25. "WHAT IS THE VALUE OF CRYPTOCURRENCIES (SUCH AS BITCOIN) 73
FIGURE 43. SURVEY QUESTION 26. "WHAT DISTURBS YOU THE MOST ABOUT CRYPTOCURRENCIES?" 74
FIGURE 44. MILLENNIALS WHO ARE FAMILIAR WITH BLOCKCHAIN TECHNOLOGY THINK CRYPTOCURRENCIES CAN EASILY BE CONVERTED INTO CASH 75
FIGURE 45. MILLENNIALS WHO ARE FAMILIAR WITH BLOCKCHAIN TECHNOLOGY WOULD ACCEPT TO RECEIVE A SALARY IN CRYPTOCURRENCY 76
FIGURE 46. MILLENNIALS WHO BELIEVE THAT CRYPTOCURRENCIES CAN INCREASE THEIR INCOME WOULD BUY MORE CRYPTOCURRENCIES IN THE NEXT 2 YEARS 77
FIGURE 47. MILLENNIALS WHO ARE FAMILIAR WITH DEFI BELIEVE THAT THE GOVERNMENT SHOULD RESTRICT THE USE OF CRYPTOCURRENCIES 78

FIGURE 53. MILENNIALLS WHO BELIEVE THAT FINANCIAL EDUCATION IS IN THE BEST INTEREST OF THEIR GOVERNMENT OR BANK WOULD ADOPT CRYPTOCURRENCIES ISSUED BY THE ECB 79
FIGURE 48. MILLENNIALS WHO TRUST IN FINANCIAL INSTITUTIONS THINK THAT CRYPTOCURRENCIES ARE DIGITAL GOLD 80
FIGURE 49. MILLENNIALS WHO BELIEVE THAT THEIR FINANCIAL EDUCATION IS IN THE BEST INTEREST OF THE BANK OR GOVERNMENT THINK THAT IT IS NECESSARY TO INCLUDE "BASICS OF CRYPTOCURRENCIES AND THE USE OF BLOCKCHAIN TECHNOLOGY IN FINANCE" AS A COMPULSORY SUBJECT IN SCHOOL OR UNIVERSITY 81
FIGURE 50. MILLENNIALS WHO TRUST IN FINANCIAL INSTITUTIONS BELIEVE THAT THE GOVERNMENT SHOULD RESTRICT THE USE OF CRYPTOCURRENCIES 82
FIGURE 51. MILLENNIALS WHO CANNOT IMAGINE A LIFE WITHOUT A BANK THINK THAT CYBERCRIME WOULD INCREASE WITH THE USE OF CRYPTOCURRENCIES 83
FIGURE 52. MILLENNIALS WHO ARE INFLUENCED BY NEGATIVE NEWS THINK THAT CRYPTOCURRENCIES ARE MONEY FOR CRIMINAL AND TERRORISTS 84

LIST OF ABBREVIATIONS

AMM – automated market making

ASIC – application-specific integrated circuit, a computer used for *mining* (Proof of Work)

CBDC – central bank digital currency

CeFi – centralized finance

CPU – central processing unit

dapp – decentralized application

DeFi – decentralized finance

dex – decentralized exchange

DLT – distributed ledger technology

ECB – European central bank

flash loan – an uncollateralized loan that is repaid within the same block

GPU – graphics processing unit, graphic processor,

KYC/AML – know your customer/anti-money laundering

L2 – layer 2 scaling

liquidity mining – way of providing liquidity based on automated market making

liquidity pool – a collection of funds locked in a smart contract

oracle – device, entity, or service that provides off-chain data to the Blockchain.

PoS – Proof of Stake

PoW – Proof of Work

SNARK – succinct non-interactive arguments of knowledge

UI/UX – user interface, user experience

yield farming – providing liquidity and receiving bonus tokens

1 INTRODUCTION

The importance of money that does not rely on institutions and a central point of failure has been discussed throughout history. Cryptocurrencies are digital currencies that first gained traction as an experiment among the cypherpunk community, and although they have faced resistance from regulators and governments, their adoption has been increasing in the past decade. How much cryptocurrencies have flourished in the last few years is visible by the market capitalization of the cryptocurrency market. Undoubtedly, the younger generations are more open to accepting technological innovations. While Millennials are an example that adoption comes easier with digital literacy, older generations are seeking alternatives for asset diversification in a financial system full of pitfalls and uncertainty.

The role of Blockchain technology in the financial sector is rapidly increasing although many still haven't discovered it. Beneficial industry use cases can be seen in other industries as well, such as improving the efficiency of supply chains for example. In addition to many advantages, there are several negative aspects which must be taken into consideration which is justified given the early nature of every disruptive technology. Blockchain in financial sense is often associated with cryptocurrencies, especially in the media. Spectacular headlines mostly about the financing of terrorism and negative environmental impacts because of high energy consumption often make unjust claims without mentioning the tradeoff between decentralization, scalability, and security. Precisely for that reason, it is in the interest of governments, regulators, and industry decision makers to define and adequately place the use of Blockchain and cryptocurrencies in suitable legal frameworks for a sustainable future.

The latest trends in the financial industry are cryptocurrencies and digital assets, out of which the concept of Decentralized finance emerged. Although the infrastructure of automated borrowing and lending has been possible in the legacy banking system, it's reliance on centralized points of authority is prone to failure and ultimately loss of funds due to market inefficiencies. Decentralized finance has the potential to disrupt the financial system on the "ground zero" layer of the financial system, which is based on a trustless, disintermediated, and open infrastructure. This financial technological infrastructure has not only the potential to be more efficient and less bureaucratic, but it has also opened new possibilities which can go beyond the understanding of finance as we know it today. Its secure and quantitative nature makes it suitable for integration with all emerging technologies such as Artificial intelligence, Internet of Things and more. Since the decentralization of finance is a new concept, the real impacts and future is unknow. Clarification is in perspective and global leadership has identified its disruptive potential. The aim of this master's thesis is to provide an insight from the millennials perspective when it comes to adoption of cryptocurrencies and Decentralized Finance.

1.1 Research questions

The research topics to be presented through this work relate to the emergence of cryptocurrencies and the way cryptocurrencies are adopted by its users. This research is directed towards analyzing millennials (i.e., people born from 1980 to 2000). Another topic covered in this research is the analysis of the sentiment towards Decentralized Finance, its adoption potential for the mainstream today, and whether it can be perceived as an alternative concept to the existing financial infrastructure. Since legal frameworks play a crucial role in this context, emerging regulations regarding cryptocurrencies and digital assets will be discussed and taken into consideration. Regulation has a high impact on the developments of any new concept. This is because the authorities can either support or resist endeavours which are not proven to be safe, secure and aligned with certain goals. Security and transparency when transacting is a crucial and systemically relevant for the whole society, which is why they are currently under supervision, controlled and monitored by systemically relevant authorities to prevent chaos, anarchy and the financing of activities which are forbidden by law, rules, or customs. Accordingly, the third research question will be formulated in the regulatory context taking into consideration the adoption of cryptocurrencies specifically for illicit behaviour and the role of regulators. A special emphasis will be given on countries that have already made significant progress in passing laws regulating digital assets using trustless technologies.

1.1.1 First research question

To what extent are cryptocurrencies adopted by millennials?

First, a thorough review of the available literature is presented. To gain more meaningful insights into the research question, a questionnaire in the form of a survey will be conducted using 150 randomly selected participants. Using this approach, it is possible to conclude whether millennials attempt to use cryptocurrencies in their daily lives, what their opinion is about cryptocurrencies in general, their trust, and whether the financial picture in the world could change over the next years once cryptocurrencies achieve mainstream adoption.

Hypothesis 1: Millennials who are familiar with Blockchain technology think cryptocurrencies can easily be converted into cash.

Hypothesis 2: Millennials who are familiar with Blockchain technology would accept to receive a salary in cryptocurrency.

Hypothesis 3: Millennials who believe that cryptocurrencies can increase their income would buy more cryptocurrencies in the next 2 years.

1.1.2 Second research question

Is there a future for DeFi?

With the appropriate use of research methods, analysis of existing literature, as well as interviews with professionals from the industry, the second research question will be answered. The research question focuses primarily on the advantages and disadvantages of decentralized finance and the potential future impacts.

Hypothesis 4: Millennials who are familiar with DeFi believe that the government should restrict the use of cryptocurrencies.

Hypothesis 5: Millennials who believe that financial education is in the best interest of their government or bank would adopt cryptocurrencies issued by the ECB.

Hypothesis 6: Millennials who trust in financial institutions think that cryptocurrencies are digital gold.

Hypothesis 7: Millennials who believe that their financial education is in the best interest of the bank or government think that it is necessary to include “Basics of cryptocurrencies and the use of blockchain technology in finance” as a compulsory subject in school or university.

1.1.3 Third research question

Can the adoption of cryptocurrencies increase illicit activities?

Although fiat currencies have been used in the past for financing illicit activities, the question arises whether cryptocurrencies represent a more modern way of financing illegal activities. By answering the third research question, the impact of cryptocurrency usage on financing illicit activities will be taken into perspective.

Hypothesis 8: Millennials who trust in financial institutions believe that the government should restrict the use of cryptocurrencies.

Hypothesis 9 : Millennials who cannot imagine a life without a bank think that cybercrime would increase with the use of cryptocurrencies.

Hypothesis 10: Millennials who are influenced by negative news think that cryptocurrencies are money for criminals and terrorists.

1.2 Thesis structure

The master thesis *„Adoption of cryptocurrencies by millennials in Vienna: Is there a future for Decentralized Finance (DeFi)?"* consists of two parts. The first part represents the review of the literature and the theoretical implications of cryptocurrencies. Firstly, an analysis of Blockchain technology is being presented in the narrower financial context, focusing on cryptocurrencies and digital assets. Defining cryptocurrencies has been a long process for institutions such as the World Bank, International Monetary Fund, Bank for International Settlements, European Central Bank, European Banking Authority, European Securities and Markets Authority, Financial Action Task Force and other decision-makers. In addition to defining the concept, the advantages of Blockchain technology will be presented, as well as identify possible challenges that are an indispensable part of any disruptive technology, which is in this case distributed ledger technology (DLT) popularly known as *Blockchain technology*. After that, an overview of the concept of achieving consensus in the network will be presented and the way the network achieves consensus, primarily the popular mining-based *Proof of Work* and staking-based *Proof of Stake*. Consecutively, the research aims to present the recent shifts from using Proof of Work (PoW) towards Proof of Stake (PoS).

After analyzing Blockchain more in detail, research will present that Blockchain is merely a technological tool that can be used for good or bad purposes. The concept of decentralized monetary systems has been a significant contributor to the ease of conducting illicit business activities, inspired by the darknet. An example of that was Silkroad, a marketplace on the darknet, where participants exchanged goods and services using bitcoin as a payment alternative.

The next step is defining and determining the concept of cryptocurrencies, where a special emphasis will be placed on the regulatory aspects of cryptocurrencies. By using Switzerland and Liechtenstein as an example, the research will analyze current trends towards the regulation of increasingly omnipresent digital assets. Certainly, *bitcoin* marked the past decade as a controversial topic unleashing a weave of alternative cryptocurrencies (altcoins), where many of them are tokens created with malicious intent. The research provides an analysis of the concept behind the technology and its creator to clearly distinguish the advantages and disadvantages of bitcoin. The next topic will then shed light on Ethereum, the first alternative cryptocurrency to gain widespread adoption due to its additional functionalities and revolutionary features (Turing completeness which enabled the use of automated transactions). Ethereum strived not only to make transactions faster but to provide a platform for building *smart contracts* and decentralized applications called *dapps*. If Bitcoin opened the door towards rethinking the concept of money as a store of value, then Ethereum challenged the way we think about financial institutions by automating procedures in a trustless system.

Consecutively, due to its nature of working without intermediaries, the idea of decentralized finance started to emerge (built on Ethereum, Polkadot, Cardano) disrupting the business model

of banking, finance, and insurance. The functionalities and use cases of DeFi such as decentralized exchanges (*dexes*), automated borrowing and lending (*flash loans*), yield farming (*liquidity providing*) gained interest in the public. DeFi raised discussions about the necessity of centralized intermediaries, such as financial and governmental institutions. Although, vulnerabilities such as *smart contract exploits*, *oracle manipulation*, *flash loan arbitrages,* and other sophisticated methods for gaining asymmetrical benefits for individuals in the market make it difficult for the mainstream to adopt.

Nevertheless, the fact that centralized power has been historically often abused in favor of individuals and not in the true interest of the whole society (*principal-agent problem*), DeFi can only be part of the solution if it's used responsibly and for the benefit of the whole society.

Another converging topic besides DeFi is the adoption of cryptocurrencies by a specific category of society. Namely, millennials are perceived as an utterly liberal part of the population, especially when it comes to the adoption of emerging technologies and are knowledgeable in the digital ecosystem.

The second part of the research is practical. It is based on a mixed-method approach, combining an anonymous survey and three expert interviews. The survey is structured into multiple sets of question topics. The first group of questions is about the person (age, gender, level of education). The second set of questions refers to the questions concerning Blockchain technology and cryptocurrencies. In this part, the respondent's subjective general assessment of the topic will be taken into consideration. The third set of questions tackles the adoption and the openness towards using cryptocurrencies for the long term. Finally, the last set of questions is a subjective comparison between DeFi and centralized finance (CeFi), which will give us an insight into potential public adoption of DeFi. The survey will be conducted on roughly 150 randomly selected respondents in Vienna, emphasizing on millennials. In terms of expert interviews, all three will be conducted with professionals from Crypto Valley Switzerland, a global hub for professionals and academics. Combining a survey with the general population and opinions from industry experts will aim to provide a clearer understanding of the adoption of cryptocurrencies with all its positive and negative implications and the future trend and developments of Decentralized Finance.

2 THEORETICAL PART – LITERATURE REVIEW

The literature that is primarily considered for the purpose of creating an overview of Blockchain technology and cryptocurrencies includes *Blockchain blueprint for a new economy (2015)* from Swan describing the stages of its potential developments. Furthermore, Antonopoulos' *Mastering Bitcoin (2014) & Mastering Ethereum (2018),* Tapscott's *Blockchain Revolution – How the Technology behind Bitcoin and other Cryptocurrencies is changing the world (2018),* Burniske & Tatar's *Cryptoassets (2017),* Wang's *Crypto Economy (2018),* Casey's *the impact of Blockchain Technology on Finance – a Catalyst for Change (2018),* have provided a more in-depth perspective into the research topic. The authors also play a significant role in defining and determining the notion of DeFi. Additionally, academic research from respected professors (including but not limited to) Dr. Horst Treiblmaier (Modul University Vienna), Dr. Philipp Sandner (Frankfurt School of Business), Dr. Aleksander Berentsen (University of Basel), Dr. Fabian Schär (University of Basel) has been taken as an academic backbone. Furthermore, from the technological perspective, basic research from the *Web3 Foundation, Ethereum Foundation, Cardano Foundation* has been included. Information about cryptocurrencies and the institutional adoption are derived primarily from *Seba Swiss, Bitcoin Suisse, Kraken, Coinbase, Celsius, and Binance.* Sources from analytic companies such as *Glassnode, Messari, Cointelegraph research, Coingecko research,* and smart contract auditing companies *Certik, Consensys, Chainalysis* provided a deeper look into the market overview. Ongoing research from the *Frankfurt school of business Blockchain Center, Blockchain at Berkley, LSE Blockchain Hub, MIT Blockchain, EY Blockchain, Deloitte Blockchain Institute* has not been neglected. Particularly important for understanding the economic context are works from *Hayek, Keynes, Schwab, Taleb*. Although the research is relying on legal connotations stemming from the *Liechtenstein Blockchain Act* and *Switzerland Blockchain law,* it does not neglect developments in other countries, be it positive or negative for the industry. Lastly, insights from International Token Standardization Association (ITSA) have been considered.

2.1 Blockchain in general

Half a decade after Bitcoin became the first widely used cryptocurrency, Blockchain gained attention from the industry and the research community (Anderson et al, 2015). Although the technology has progressed it is difficult to predict how Blockchain technology will evolve in the future. Its history is relatively short, and the world is just starting to recognize its potential. In times of uncertainty, it is becoming more and more discussed that Blockchain could be one of the most important innovations since the emergence of the Internet (McKinsey, 2015). The system design is serverless and trustless without intermediaries (Samuel, 2018).

Blockchain is a distributed database that controls the process of logging information, transactions and enables tracking of assets within the network (Gupta, 2018). According to Treiblmaier

(2019), Blockchain is a "digital, decentralized ledger in which transactions are logged and added in chronological order to create permanent and tamper-proof records". This database is in the form of a chain of verified transactions distributed on the network which is cryptographically protected and stored in a decentralized way on the network. (Morris, 2016). The connections which contain information about digital transactions are stored in a chain-like structure (Berentsen & Schär, 2017). Once finalized, a transaction cannot be altered or changed retroactively once it is added as a block to the chain. The concept of immutability is unique because it makes it prone to centralized points of failure. In theory, no intermediary, server or regulator can impose or alter rules to the network. A Blockchain network comes in theory with transparent predefined rules. All transactions are public, transparent and the history of transactions are tamper proof. Unlike a classic online database, Blockchain enables communication with several computers called nodes which act as validators. As soon as consensus is achieved the transaction gets finalized through validation making it settled and irreversible.

Nowadays, banks and governments are experimenting with Blockchain technology to improve their internal processes such as keeping information safe and carrying out transactions (Tapscott, 2018). With the rising adoption of Blockchain technology, the traditional financial system could soon see benefits of integrating Decentralized Finance (DeFi) to automate processes, lower costs, increase security, and improve transparency. The common misconception is that a Blockchain infrastructure *wastes* energy for achieving consensus, while resource expenditure is an *investment* into keeping the network secure. Security gets achieved through validators that get incentivized for being trustworthy in the network while acting in their best interest in anticipation of a block reward as well as transaction fees. This ensures the authenticity and validity of information on the network. Malicious actors would need invest more resources than trustworthy actors on a continuous basis to be able to perform an attack such as double spending. The Blockchain ledger is public and any person can check whether a transaction has been finalized while granting a certain amount of privacy with the use of public addresses instead of personal data.

2.2 Blockchain

Blockchain is an immutable ledger of transactions. The data is stored on *nodes* on the Blockchain network. *Private* Blockchains are mainly used in industry-specific settings, whereas *public* Blockchains are open for all stakeholders. *Hybrid* Blockchains combine properties of public and private Blockchains. They can be *permissioned* or *permissionless*, based on the predefined rules of the network. While the latter is the standard, some permissioned Blockchain alternatives are being used for industry specific use cases (such as in supply chain management systems for example). Blockchain keeps transactions, events, or any form of data recorded in a chain-like structure eliminating the risk of changing, altering, or tampering the history. Since blocks are added to the Blockchain linearly and chronologically, the difficulty of changing or altering blocks is increasing with the length of the chain (Swan, 2015). The block creation process can be seen in Figure 1.

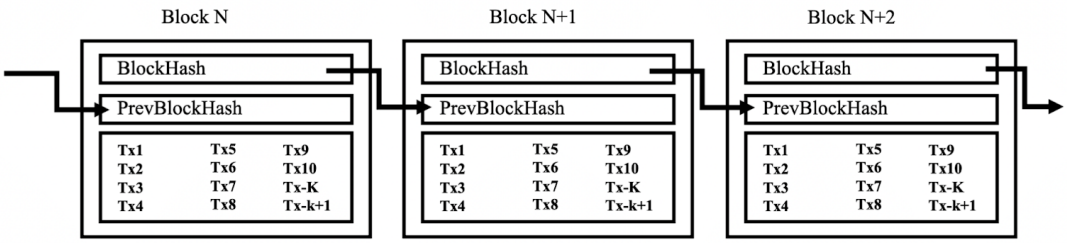


Figure 1. Blockchain design, source: Rosa et al. (2020)

Every Blockchain node stores a copy of the entire Blockchain database or ledger called a *full node*, which is connected to the Blockchain network to ensure trustworthiness. Malicious actors in the network cannot change the history or add malicious blocks, making it to resource intensive for the consensus mechanism to fail. As long as the majority is responsible for validating transactions on a trustworthy way, a malicious agent cannot double-spend or alter transactions. The reward incentives behind validating transactions enables everybody to act in their interest by simultaneously acting as trustworthy participants in the network. Blockchain technology has complete information about the addresses and the state of the Blockchain from the first block up to the most recent (Swan, 2015). Put simply, Blockchain is a distributed ledger that allows the community to record (securely encrypted) data on multiple computers in a decentralized way. In Bitcoin's case, transactions are recorded in the form of inputs and outputs using *UTXO's* (unspent transaction outputs). Ethereum is more advanced in this sense due to Turing completeness which enables more sophisticated transactions using smart contracts and *address* based accounts. That's a limitation of Bitcoin because it was designed to be simple, robust and solely built for the purpose of making manual transactions. Ethereum enables not only sending and receiving a cryptocurrency, but its smart contract feature enables the creation and transfer of

any generic (fungible, ERC20) or unique (non-fungible, ERC721) token (Piscini et al., 2017). Entries are permanent, transparent, and can be searched publicly (using an explorer such as etherscan), allowing community members to review pending and completed transactions. The detailed process of signing and verifying a transaction can be seen in Figure 2.

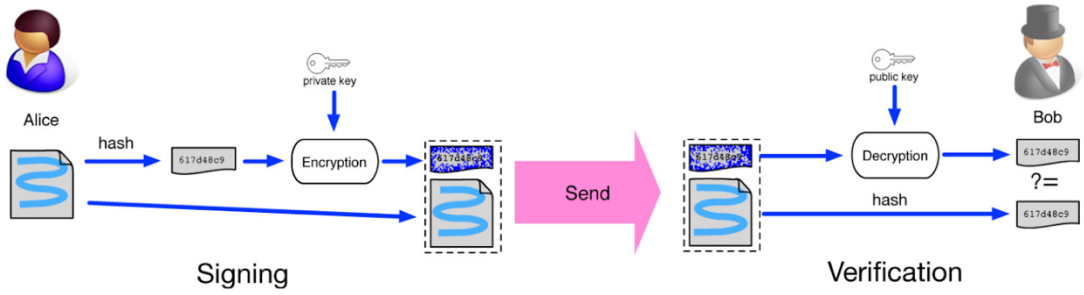


Figure 2. Encryption process, source: Rosa et al. 2020

One of the important characteristics of Blockchain is that it enables the disintermediation and decentralization between all parties globally. Blockchain technology finds application both in financial and non-financial industries (Crosby et al., 2016). A Blockchain network works like an autonomous system that provides the necessary infrastructure for handling cryptocurrencies, financial contracts, tokenized property in a global borderless system. Besides its applications in an economic context, Blockchain can also be used as a system for recording, tracking, and monitoring with the help of sensors. For trustworthy logging, data inputs with the use of *oracles* must provide trustworthy data. The primary role of the Blockchain is to be an accounting and global transaction system that can include all forms of property owned by all parties around the world (Swan, 2015). In addition to establishing trust in the protocol, Blockchain enables the exchange of information with others on a safe and efficient way (Piscini, Hyman & Henry, 2017). A decentralized autonomous database can ensure borderless validity and authenticity for information crucial to society without the use of centralized points of failure (Crosby et al., 2016).

2.2.1 Advantages and disadvantages of Blockchain technology

According to 24 expert interviews conducted by Treiblmaier in 2018, the majority believe Blockchain could have a long-term and sustainable effect on the economy (Treiblmaier, 2019). The core element is the transformation of the World Wide Web from the *internet of information* towards the *internet of value*, known as the transition from Web 2.0 to 3.0 (Sandner, 2019).

Treiblmaier (2019) points out that Blockchain is a nascent technology that can have long-lasting positive and negative impacts on the economy, society and work in the near future.

Economically, Blockchain can be a driver for added value in terms of innovation, productivity, and increased transparency. At the same time, it can cannibalize certain business models, especially in the financial sector (Treiblmaier, 2019).

Society can benefit from greater financial inclusion of underprivileged parts of the world where banking services are inaccessible due to corruption, lack of infrastructure, or other conditions (Treiblmaier, 2019). Although adoption of the technology could bring benefits, it could also increase the gap between the digitally literate and illiterate (Treiblmaier, 2019). With the rise of digitalization, many fear the lack of *privacy* (Treiblmaier, 2019). Enhanced monitoring and tracking capabilities with the use of Blockchain technology could posses a threat to freedom of citizens (Treiblmaier, 2019).

Another genuine concern is the increasing *digital gap* (Treiblmaier, 2019). Laggers of technological adoption could fall behind and be at a disadvantage in the future due to higher automatization (Tapscott, 2018). The opportunities lie in optimizing part-processes as well as providing end-to-end solutions (Treiblmaier, 2019).

Productivity and efficiency at work could improve but could also be a potential reason for layoffs in the future (Treiblmaier & Umlauff, 2019).

The above-mentioned positive and negative impacts of Blockchain technology on economy, society and work are depicted in Table 1.

Effects	Economy	Society	Work
Positive	Innovation	Financial inclusion	Increase of efficiency
	Productivity	Property rights	Reduction of routine activities
	Value transfer	Less bureaucracy	New incentive forms
	Transparency	Democratization	Employee participation
Negative	Unclear use cases	Privacy loss	Increased control
	Legal uncertainty	Digital gap	Autonomy loss
	Cannibalization	Financial risk	Qualification gap
	Waste of resources	Unclear effects	Layoffs

Table 1. Positive and negative effects of Blockchain technology, source: Sandner, P., Welpe, I., & Tumasjan, A. (2019). Der Blockchain Faktor. BoD - Books on demand

Decentralization is the main characteristic of public Blockchains meaning that it doesn't rely on a single point of failure, such as an institution or a server. Decentralization means that the system can successfully operate because participants themselves assure that the network is in

consensus without having to rely on a centralized organ. Each system has a database that is prone to breaching and hacking, so it must ensure that data is well protected with each processed transaction (Bahga & Madisetti, 2016). Consensus mechanisms fulfil that role and ensure network security. Transactions on the network are recorded, logged and the data is available and accessible for everyone on the internet. The most important feature of Blockchain is that recorded data cannot be changed, deleted or altered. This provides users the necessary trustworthiness and ensures authenticity, transparency, immutability, and security (Bahga & Madisetti, 2016). Those values

In a *trustless system,* participants rely on verification rather than trusted intermediaries. Thus, it is not necessary to have a trusted third-party in a transaction of goods, services, information, or data. It makes it difficult for market participants to inflict damage to other participants if the system is based on verification rather than trust (Stiglitz, 2017). This is true for all stakeholders in a trustless network. Since the system is constantly being updated and, spending the same amount twice is not possible because of timestamps. The double spending problem has been an issue in centralized system because they are not synchronised with each other in real-time. Many institutions fall victim to flaws in systems and a malicious actor can take advantage of such a system. It makes it easier for malicious participants to spend the same amount twice because of asymmetry of information (Stiglitz, 2017). The authenticity feature is a crucial constituent for achieving trust and equilibrium in markets (Stiglitz, 2017). In the future, trust could increase without the need of central points of failure. This could enable a wide variety of network services, ranging from transactions, smart contracts, decentralized applications, to decentralized autonomous organizations.

Immutability is an advantage because it means that once a transaction is verified, it is final and cannot be altered, changed, deleted or reverted. Blockchain users have full control over all transactions by themselves (Songara & Chouhan, 2017). However, it is important to note that immutability also means that once a transaction is finalized and verified, it cannot be reverted, even if it is done with malicious, illegal, or otherwise harmful intent.

The high *security* of Blockchain technology is achieved by individual participants in the network. Every person entering the Blockchain gets a unique ID (*public key*) associated with the wallet, protected by a mnemonic backup seed phrase (*private key*). This encrypted data enables users to interact without revealing sensitive information. Another reason for Blockchain's security is a reliable chain of cryptographic hashes. When a new block is created, it is necessary to calculate a new hash value for the new block. The new hash includes the hash of the previous block, ensuring that malicious blocks cannot alter the chain. The hash consists of a type, the value of the previous hash, time of the block creation, user's ID number, mining level, and the Merkle root where information about previous transactions and hashes is stored. Each user (or node) on the network automatically generates this hash. In this case, it is impossible to change any information about hash values and that is what security is reflected in (Data Flair, 2018).

Blockchains are *fast* in finalizing actions. A transaction in centralized systems is usually processed only partly and usually involves escrow accounts in international transactions, meaning that transactions are finalized within days (Song et al., 2016). Blockchain's finality is faster than in traditional finance, and in Bitcoin's case the transaction is finalized within roughly 10 minutes. However, finality means that unwanted transactions can never be reverted, even if proven to be illegal. Although Blockchain systems seem to be a universal solution they always face a trade-off between decentralization, scalability and security.

Blockchains are *transparent* because all network participants can access the ledger from a browser and view the history of transactions publicly.

When it comes to disadvantages, the most media covered topic is *power consumption*. This is due to the consensus mechanism called *Proof of Work*. To protect the network from attacks, miners must utilize computer processing power (hash power) to verify transactions and add new blocks to the chain. To get rewarded from the network (block reward) and to get rewarded from the users (transaction fees) nodes are using energy. This energy consumption is an investment in the security and robustness of the network, making it extremely expensive for malicious actors to attempt attacks. Due to a pre-programmed event called *halving*, block rewards are halved each time a certain amount of bitcoin have been mined (210.000, occurring roughly every 4 years). After a total of 21 million bitcoin will be mined (presumably in the next few years), there will be no more additional block rewards. This doesn't mean that miners will *work for free* but rather that the system (the network) will not issue block rewards and miners will receive only transaction fees paid by users (the sender). Signature verification is one of the biggest challenges of Blockchain, and because each transaction must be signed by a cryptographic schema it is amounting to high energy consumption (Golosova & Romanovs, 2018). Ethereum is transitioning to a more sustainable consensus protocol, where less energy is used, and more decentralization is granted. The majority of the projects which are operational or still in development opt for Proof of Stake (or a variation thereof, such as leased PoS, delegated PoS, Proof of Authority, and so on). According to Tasca & Tessone (2020) "Blockchain systems incur operational and maintenance costs that are generally absorbed by the participants in the network".

Research from Bitcoin Suisse shows that Bitcoin's energy is not wasted because it powers the most secure and global network, and that the environmental footprint is often overestimated. Renewable electricity sources make up 73% of the energy expenditure for mining which is double the global average (Huber, 2021). Furthermore, up to 30TWh of hydro energy is wasted because demand is lower than potential supply and lack of storage possibilities.

Another disadvantage are *forks.* There are two types of forks, namely soft forks and hard forks (Light, 2017). Soft forks can be viewed as an *update* to the existing Blockchain system, whereas hard forks form a new chain, making the *old* Blockchain obsolete and outdated. If the block, previously considered valid, violates the new soft fork rules, it will not be considered after the

soft fork is complete. For example, if a soft fork limits the size of a block to 500 kB, but before that, it was 1 MB, the blocks that are larger than 500 kB will not be valid in the new chain after the upgrade (Light, 2017). A hard fork is the opposite term of a soft fork and refers to the loss of set and rules from blocks in an earlier protocol. This procedure is the same as the soft fork procedure, but the value and result are the opposite. For example, a hard fork increases the block size to 2 MB from 1 MB. If the block has passed all the rules of the hard fork, the block will be accepted, even if the block was not in the chain before (Light, 2017). A hard fork creates a new token contract. This means that two independent tokens co-exist, making it sometimes difficult for newcomers to distinguish between two versions. The International Token Standardization Association (ITSA) is tackling this issue with a proper framework for classification and identification mechanisms to protect users from mistakenly making transactions on *the old* chain. The solution which ITSA developed is based on a successful and proven method, similar to Uniform Resource Locators (URLs) on the world wide web.

Scalability is the main issue of all Blockchains. Stemming from the fact that Blockchains are databases, which means that they have to be stored in the form of data. As more and more transactions are approved, and blocks are added to the database, the full copy of the blockchain increases in size day by day. Scalability is one of the trade-offs mentioned in *the Scalability trilemma* besides decentralization and security. For example, Bitcoin's Blockchain has exceeded 100GB of storage, and new blocks are added in roughly 10 minutes intervals. Some Blockchains are focused on higher throughput when it comes to the speed of transactions but that usually comes at the cost of decreased decentralization or a compromise in security. Layer 2 solutions such as Lightning Network for Bitcoin or *rollups* solve this problem.

2.3 Blockchain in banking and finance

The banking and finance industry has traditionally provided trust, security, and stability for individuals and institutions. Since the internet emerged, digital payments started to get traction at the beginning of the 21st century. When applying Blockchain in this industry, few industry experts could expect record-keeping without an accountant, investing without a broker, charity without a trustee, loans without a bank, escrow without an agent, insurance without an underwriter and money without a central bank. However, this could soon be reality. As for example, Bitcoin is a trustless intermediary-free exchange of data with the use of Blockchain technology which provides an alternative trust mechanism between parties involved in a particular transaction (Nakamoto, 2008). Although economists such as Milton Friedman discussed the likelihood of an *E-cash system* in 1999, it wasn't clear that a pseudonym with the name of Satoshi Nakamoto would invent a revolutionary "*Peer-to-peer electronic cashless system"* combining computer science, cryptography, and economics. The idea that a currency is backed by nothing but a mathematical algorithm at its core was highly experimental (Nakamoto, 2008). According to Drescher (2017) "With respect to peer-to-peer systems, this means that people will join and

continue to contribute to a system if they trust it and if the results of interacting with the system on an ongoing basis confirm and reinforce their trust."

Today, Blockchain can be used for making transactions, ranging from real-time digital payments, micropayments, remittances, and creation of digitally stored ownership records (Holotiu, Pisani & Moormann, 2017). Although it might seem simple today, a system based on cryptography and mathematics introduced a secure and trustless accounting system, enabling participants to agree on the approval of a particular transaction (Holotiu, Pisani & Moormann, 2017). Keeping the network secure and avoiding those funds are spent twice (double spending problem) is one of the issues that banks have solved in a centralized manner. Although currencies nowadays are stable, many currencies have failed due to war, hyperinflation, or systemic collapse in the past. While the traditional role of financial institutions is in mitigating the risk and providing clarity behind transactions, the emergence of Blockchain technology is challenging this narrative. After only a decade, *bitcoin* as the first decentralized digital currency within a decentralized monetary network *Bitcoin* has the potential to become a global reserve currency, operated exclusively with the use of a mathematical algorithm (Robleh et al., 2014). The idea behind Bitcoin is not to provide only a currency and programmable money but an alternative platform detached from the traditional financial system. Due to the pre-programmed fixed supply of tokens, it is designed to become deflationary over time, making it suitable as a safe haven in economically uncertain times due to its scarcity. According to Yang, Brown & Treleaven (2017) "In the banking and financial services domain, Blockchain technology can simplify business processes while creating safe, trustworthy records of agreements and transactions."

Banking institutions were created to provide an infrastructure for global trade. The Blockchain is a new infrastructure that can achieve the same result, but on a more global and permissionless scale, safely and at the same time transparently. Blockchain gives the power of financial communication to the individual. It makes trade more efficient by removing manual and paper processes and introduces simplified and automated processes. The only drawback is that the transactions are not KYC/AML compliant by default. Blockchain can also be a great tool for cooperation because it is decentralized, and no entity can own it entirely. By establishing a decentralized payment channel, banking institutions can use new technologies to enable faster payments and reduce fees for processing them. By offering more certainty and lower transaction costs, banks could co-exist with Bitcoin, and use Blockchain to their advantage by innovating and bringing new products to the market. Distributed ledger technology, such as Blockchain, could allow bank transactions to be settled directly and tracked by banks better than existing protocols such as SWIFT. Moving money around the world is logistically challenging for many banks because of a set of international regulations and different interpretations of transaction finality. A simple bank transfer must bypass a complicated system of intermediaries (Guo & Liang, 2016).

Buying and selling assets such as goods, stock, or debt is based on tracking who owns the goods that are subject to the transaction. Financial markets achieve this with a complex network of

stock exchanges, brokers, clearinghouses, and payment providers (Attaran & Gunasekaran, 2019). All these different parties are built around an outdated system of paper ownership. This system is not only slow but also full of errors and prone to fraud. Blockchain can revolutionize entire financial markets by creating a decentralized digital asset database. The distributed ledger enables the transfer of property rights through cryptographic tokens that may represent such assets outside the chain.

Banks are currently not able to make any financial transactions without authentication. However, the verification process consists of many different steps that are often user-unfriendly and time inefficient. With Blockchain technology, consumers and companies can benefit from accelerated verification processes. This is because Blockchain enables the safe reuse of authentication for other services. Thanks to Blockchain, users can choose how they want to identify and who they want to share their identity with. What is needed is that they must register their identities on the Blockchain only once. Naturally, keeping this kind of information on the Blockchain also provides more authenticity in the long term (Attaran & Gunasekaran, 2019).

Guo & Liang (2016) compared traditional banking businesses, internet finance businesses (FinTech 1.0), and Blockchain-based finance businesses (FinTech 2.0) in terms of customer experience, efficiency, cost, and safety. Overall, in a Fintech 2.0 ecosystem cost savings, safety, operational efficiency, and (personalized) customer experience is higher than in traditional banking business (Guo & Liang, 2016).

Nonetheless, Blockchain can also find applications outside of the field of finance. In traditional supply chains, parties are known and have mutual trust but because of bureaucracy and data protection, it leaves a lot of room for improvement. However, companies today do not want to have an open approach when it comes to disclosing ownership details, such as demand, capacity, orders, prices, and margins because they want to protect their business and competitive advantages. This means that most Blockchains in the supply chain must ensure enough transparency while providing room for some restrictions on certain segments of data (Felea & Albastroiu, 2013). In many cases, real-time supply chains already have billions of transactions and data. Such systems are not perfect, and many supply chains have data problems that are differently formatted, difficult to access, or difficult to visualize or analyze in the context of large data. Nevertheless, well-managed central databases can be achieved today, combined with supply chain visualization and analytical capabilities.

2.4 Blockchain in other sectors

Blockchain technology is widely used in various sectors. In addition to the financial sector, the role of Blockchain technology is already reflected in the media industry, art, law and many more to come (Bashir, 2017).

Blockchain technology can be used for many non-financial applications. The earliest use cases include supply chain, elections, voting, and logging of sensitive data. Blockchain is useful for providing transparency and authenticity, for example proving proof that a particular event happened at a certain time. Blockchain is also suitable for situations where it is necessary to know the history of property ownership, without trusting legal documents or lawyers. It eliminates the counterparty risk because the ownership proof is beyond national legislation and borders. It could provide more transparency to supply chains, for example by providing evidence to the network about the real origin of an ingredient or a product. It can bring more justice by shedding light on manufacturing processes. For example, it can tackle the problem of black and child labour and force manufacturers due to lack of supervision and control. The process of controlling the middlemen in production can be costly, and Blockchain can serve as a tool for providing more transparency, making production of goods more sustainable. Intellectual property is another use case where Blockchain technology can be applied. Although progress has been automated throughout recent years, music and video artists have to actively protect their data and monitor copies by themselves, proving to be costly in the long term. Blockchain could also improve administrative work and prevent the risk of counterfeiting with false signatures or deceiving certification. Blockchain technology shows its advantages especially in the field of authenticating patents and licenses.

Namely, two characteristics of Blockchain technology make it particularly relevant to the patent system: *hashing* and *proof of existence*. The first characteristic is hashing which is described as a process through which a document is transformed into a fixed-length code, similar to a digital fingerprint (European Parliament, 2017). The second characteristic, proof of existence, involves recording the hash on the Blockchain. It creates a record that provides the reader with information that a particular hash existed at a specific time. A record can be verified by anyone, but no one can interpret the contents of the hash without additional information. However, the owners of the original document can prove that the document existed at the time the transaction was made by repeating the hash procedure on an identical copy of their original document. Although centralized proof of existence services are already available and used in patent offices, Blockchain could further automate and make the transfer of managing ownership more efficient. Furthermore, existing patent controlling systems are slow and expensive due to human labor, which can be optimized with the use of Blockchain technology (European Parliament, 2017).

Elections today are still conducted offline with the use of paper voting for many reasons. But the case of a small town named Zug in Switzerland is a real-life example that direct democracy can work with the use of Blockchain. Many experts agree on the fact that electronic voting for national elections would revolutionize the development of system security. According to Park et al., (2020) “The recent interest in online and Blockchain voting proposals appears related to a growing political enthusiasm for improving and modernizing election systems — and for

increasing their security from malicious interference." However, there are many other types of regional and organizational choices that could be simpler using Blockchain technology, as they enable more people to be involved in making important decisions, adopting long-term strategies, employing people for a wide range of positions, etc. Blockchain is a record logging and verification tool that makes transparency a priority and distributes truth among all users. An electronic Blockchain-enabled voting system would allow voters to perform tasks such as logging, counting, and managing problems while ensuring that the original is stored as a value and cannot be copied and altered, which is often the case today. It makes accessing the voting log easy and less labor intensive. Transferring and altering is impossible because the hash codes would not match the original records, and voters would see that the record is different from the original. An illegitimate vote cannot be added because other voters might see that it is incompatible with the rules (perhaps because it is already included or not associated with a valid record). Such use cases can also be utilized for the votes of shareholders in companies, which has been the case in Estonia (European Parliament, 2017). Nguyen (2016) states that Blockchain is expected to have an essential role in the global economy.

According to Casino et al. (2019), Blockchain will impact the public and private sector, as well as society as a whole. The change will start from the financial sector and slowly progress to non-financial ones (Crosby et al., 2016).

The *public sector* can benefit from increased accountability, safety, and automation, making government services more efficient (Casino et al., 2019). This is especially crucial in the context of *Smart cities* where Blockchain could serve as a secure communication platform. (Casino et al., 2019). According to Swan (2015) Blockchain governance will benefit from the aspect of authenticity, validity. Applications include registration or legal documents, attestation, identification, marriage contracts, taxes, voting, intellectual property management (Swan, 2015).

The *financial sector* applications include auditing, asset management, wealth management, and insurance. In the near future, it is possible to see a shift in payment processing, prediction markets, improvements in managing securities, commodities, derivatives, and synthetic assets (Haferkorn and Quintana Diaz, 2015).

Healthcare is another industry that can benefit from increased automation, authenticity, transparency in terms of general healthcare management, patient record keeping, medical data sharing, drug tracking, clinical trial, and precision medicine (Casino et al., 2019).

Supply chain management is expected to benefit from more flexible value chains with improved transparency, accountability. This is due to better tracking of goods, monitoring of processes, predicting supply and demand, easier document management in logistics, and more (Casino et al., 2019). Consumers can have better insights into verified information about where their food is coming from, increasing food safety and quality from a buyer's perspective.

The *education* sector could tackle issues of vulnerability, security, and privacy when it comes to certificates, accreditations, qualifications, and degrees.

Treiblmaier (2019) discusses that the true potential of Blockchain lies in the interoperability between the Internet of Things, Big data, Artificial intelligence (Treiblmaier, 2019).

2.5 Consensus mechanism

Consensus mechanisms are protocols designed to ensure that all participants in the Blockchain adhere to pre-set rules. These mechanisms ensure that transactions arise from a legitimate source. A good consensus algorithm is a prerequisite for efficiency, security, and convenience (Zheng et al, 2017). Blockchain is a decentralized technology, and no centralized authority can change the rules of the protocol. Therefore, the network requires participants to verify and authenticate any activities that occur on the Blockchain. The whole process is based on the aforementioned activities of network participants and makes Blockchain technology confidential, secure, and reliable for digital transactions. Several consensus mechanisms have been introduced in theory and practice, whereby security, scalability, and decentralization are in a constant trade-off triangle. The most popular mechanisms are currently Proof of Work and Proof of Stake (Baliaga, 2017).

2.5.1 Proof of work

Proof of work is a form of cryptographic evidence of zero-knowledge proofs in which one party proves to others that a certain amount of computer effort has been spent for some purpose. Verifiers can subsequently confirm this cost with minimal effort on their side. Proof of work is based on solving mathematical equations consisting of complex encryption algorithms. To achieve security, *secure hashing algorithms* are used. Today, SHA256 is the most commonly used hashing algorithm. It was initially used for encryption in Bitcoin, but other crypto projects have been adopting it ever since (Tar, 2018).

Each transaction is broadcasted to a mining pool and verified by nodes in the network through decryption (Bonneau et al., 2015). Each node collects transactions on the block and the block is associated with a difficult mathematical problem, representing the encrypted transaction. Solving this complex algorithm is called *mining*. The miner who solves the problem first secures the right to add the block to the longest chain of blocks to receive a reward from the network. Once the transaction has been confirmed, the miner broadcasts the newly mined block to each node in the network. The longest chain of blocks is the consensus of all transactions, ultimately recording all transaction in a chronological order with time-stamps (Bonneau et al, 2015).

Miners are a major pillar of securing consensus because the process of verification and logging transactions can only be done by miners within the network. Proof of work requires significant computing power in order to mine. The mining process is a random trial-and-error method and

hashing power plays a significant role. For the *target hash* to be recognized, it must contain a lower number than the hash block (Lisk, 2019). Proof of work consensus assumes that half of the network nodes are always honest miners. Namely, getting more than half of the hashing power makes this consensus mechanism vulnerable for a 51% attack. The Proof of Work hashing process can be seen in Figure 3.

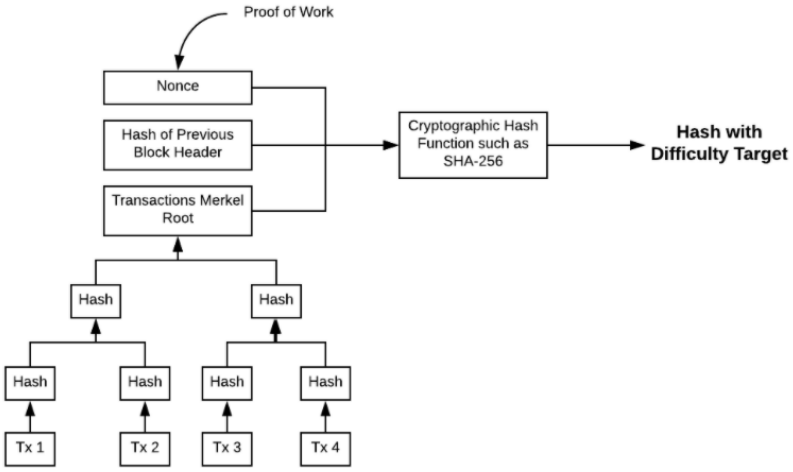


Figure 3. Bitcoin Blockchain – What is Proof of Work?, accessible at: https://vitalflux.com/bitcoin-Blockchain-proof-work/.

One of the biggest drawbacks of this mechanism is power consumption and the energy cost associated with it. This is because of the race between miners for the highest hash power. In the beginning, it was possible to compete with regular computers but as the race continued, mining-specific computers such as ASICs started to gain traction in the mining community.

Recent research from Bitcoin Suisse has shown that the energy consumption of Bitcoin is as big as Sweden (131 TWh/year) or Belgium (78 TWh/year) (Huber, 2021). However, this energy is derived 73% from renewable sources which is quadruple as much as the industry standard today (Huber, 2021).

Another deficiency of this mechanism is that the process is slow compared to Proof of Stake, making it hardly scalable enough for day-to-day transactions without layer 2 solutions such as the Lightning Network. And because several mining pools aggregated into mining pools dominate large amounts of mining power, the power of mining pools can impose a significant risk to decentralization. Recent attacks have proven that the Proof of Work mechanism can be sensitive to 51% attacks (Sayeed & Gisbert, 2019). Although, according to an open source calculator crypto51.app, an attempt of attacking the Bitcoin Blockchain would require $26b in hardware costs and $18m daily costs for electricity, making it a solid financial barrier for such an attack.

However, due to technological advancements specific computers called *quantum computers* have emerged that utilize *Shor's algorithm* for factoring. Those are currently used for research and laboratory purposes, and many believe they impose a threat for cryptocurrencies and every service that uses the industry-standard hashing method (asymmetric elliptical curve encryption) and Rivest–Shamir–Adleman (RSA) public-private key encryption (Furrer et al., 2020).

Quantum computers cannot perform any task other than factoring and deriving the private key based on the public key and are not computers that can be used for general purposes. Nevertheless, experts believe that new quantum-resistant techniques (post-quantum cryptography) will emerge that can make Blockchain technology quantum-resistant and secure in the future (Bernstein, 2009). Research done by Marchenkova in late 2019 shows that the highest relative likelihood of Bitcoin vulnerability to quantum computing will be between 2030 and 2050. The potential vulnerability to quantum computing is depicted in Figure 4.

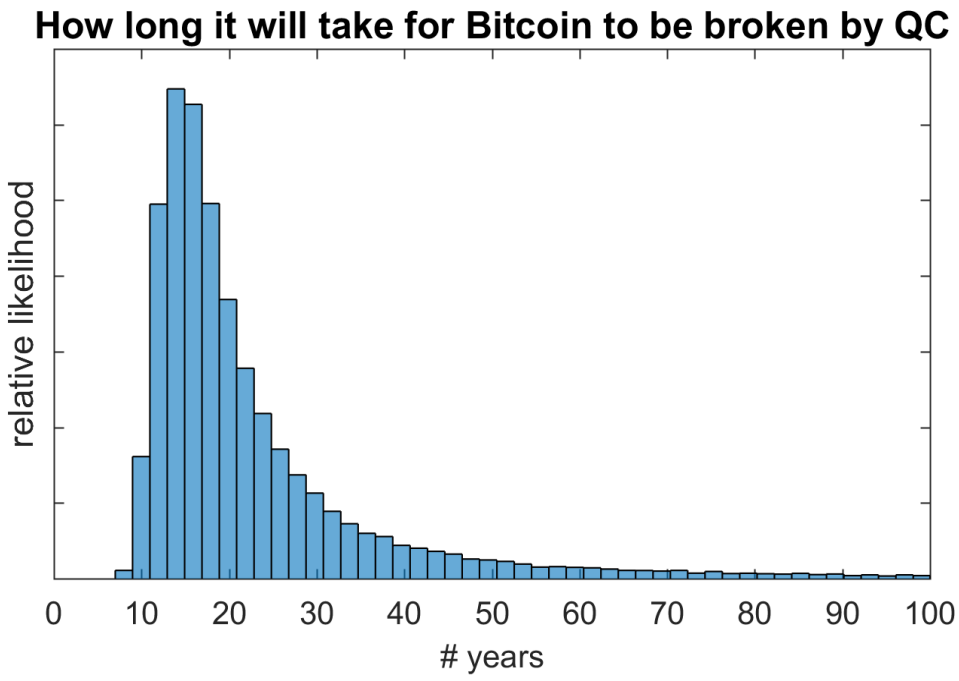


Figure 4. How long it will take for Bitcoin to be broken by quantum computing, Marchenkova (2019), accessible at: https://www.amarchenkova.com/2019/09/13/quantum-computer-bitcoin/

2.5.2 Proof of stake

The growth of Blockchain ecosystems and the adoption of Blockchain technology in different domains and applications have created a competitive environment in which newer protocols

and algorithms are quickly introduced and implemented without formal analysis and verification processes. The lack of binding research with practice implies that many of the widely used protocols and algorithms have yet to undergo formal analysis that checks the system's security properties and fundamental accuracy. This process is extremely important, especially for consensus algorithms that find how to resolve conflicting requirements in the absence of central entities which could define consistency, performance, scalability, and liveliness of the system (Thin et al, 2018).

Proof of stake is a consensus mechanism that approves blocks based on the "stake" of participants in the network. The disadvantage of this consensus mechanism is that validators who possess a large number of coins have more power than other participants (Sayeed & Gisbert, 2019). Peercoin was the first cryptocurrency to use this consensus in 2012. The advantage of proof of stake is that it does not require expensive mining hardware and it does not consume as much energy. Unlike the Proof of Work mechanism in which anyone can become a miner, not everyone can become a validator in this mechanism. Namely, currency ownership is the prerequisite for being a validator and participate in the process of confirming transactions (Seang & Torre, 2018).

In comparison with Proof of Work where mining capacity depends on computational power, validating in Proof of Stake requires locking coins for validation purposes for a cetrain amount of time. Validators do not receive a block reward, instead, they solely collect transaction fees as a reward (unlike in PoW, where the miners get both rewards).

The energy efficiency of Proof of Stake is beneficial for the environment which comes from the fact that trustworthy validators get the chance of validating transactions in advance. In case the validator is offline, passive, or acts maliciously in another way an event called *slashing* is enforced. This is a form of punishment from the network that is not possible in Proof of Work where a malicious or passive miner is simply disregarded. Another advancement of Proof of Stake is the fact that it's more decentralzied and open for participants without the knowledge of setting up the equipment. Stakers can simply stake their tokens with a wallet integrated in the browser, not requiring uptime, energy, effort or maintenance of equipment.

Since validators only receive transaction fees, the scenario in which validators create blank blocks can be avoided because they are encouraged to perform the maximum number of transactions to maximize their gains. The problem occurs when the centralization of this mechanism occurs. Proof of stake includes the selection of validators (the higher the stake, the more likely the user is to be selected as the creator of the next block), then additional balance mechanisms are needed to reduce the risk that rich validators will become even richer, and the validator with smaller stakes will not be viewed as *trustworthy enough* from the network. However, the big advantage of Proof of stake is the lower possibility of a successful 51% attack because of the capital requirements needed to obtain 51% of the cryptocurrency token supply.

3 CRYPTOCURRENCIES

3.1 The definition and history of money

Money is an economic unit that serves as a medium of non-verbal communication and means of exchange in every modern economy. The primary function is measuring economic value. The secondary characteristic is storing of value as well as payment standard. The tertiary layer reflects its function of the basis of credit, liquidity to wealth, distribution of income, and maximization of utility.

In the beginning, money has been issued as an IOU token (to keep track in a *creditor-debitor* relationship). Keeping such *IOU ledgers* was untransparent because it relied on honesty, reliability, and trust between the contracting parties. After trade between communities evolved, the need for a more standardized unit of value measurement emerged. The second phase in money creation was minting coins from precious metals (usually with a ruler's watermark). Metal coins were hard to counterfeit, durable, portable, and divisible. However, bigger quantities of metal money were often cumbersome and dangerous for transport, and difficult to store safely. In addition to that, precious metals (such as gold) could be mixed with non-precious metals (such as tin), which demanded a degree of expertise in identifying the real *face value* of a metal coin in a transaction, not only based on weight. Early Chinese rulers came to the idea to issue IOU paper certificates for long-distance trading while the metal coins were kept safe and secure. Those certificates of precious metals represented debt in the form of a certificate that could be swapped with other certificates. As global trade grew, the idea of paper certificates grew, making it easy and convenient for holders to exchange them with the guarantee of receiving the underlying asset. The problem of having various precious metals was alleviated with the emergence of gold, and civilizations were moving from a micro to a macro-based economic system. Certificates became currencies pegged to gold. The gold standard continued for centuries but the need for flexible exchange rates was needed.

The gold standard was widely used in the 19th and 20th centuries. Institutions such as the Federal Reserve Bank (FED), International Monetary Fund (IMF) were established and ideas about boosting the economies after wars and economic downturns demanded monetary stimulation of the money supply. Economies using monetary expansion mechanisms (*quantitative easing*) were able to recover faster, and the concept from issuing additional debt (based on a certain percentage of gold reserves), shifted to the concept based entirely on debt. In the 20th century, the U.S. Dollar as the global reserve currency based on the Bretton Woods system of monetary management, ensuring stability between major independent war-torn economies. By 1970, the U.S. gold reserves deteriorated from 55% to 22%. Because of the growing public debt incurred by the war in Vietnam, trade deficits and monetary inflation demanded action. President Nixon signed a short-term executive order in the hopes of achieving long-term economic stability without the

approval of the IMF or the State Department. This is known as *the Nixon shock*, a temporary measure ending international convertibility of the U.S. Dollar to gold. This temporary measure has been legalized, and the idea of quantitative easing and economic stimulus has been discussed.

The global economy and macroeconomically relevant states have been following *The principles of the General Theory* by John M. Keynes (Keynesian economics). The Keynesian school is based on the idea that government intervention can stabilize the economy. The opposing school was inspired by *the road to Serfdom* by Friedrich A. von Hayek, a Nobel prize winner, and defendant of classical liberalism. The Austrian school of economics is based on individualism and the thought that social phenomena are results from the motivations and actions of individuals. Thus, they believe that money should be free of governmental control.

According to a study published on DollarDaze.org, 775 fiat currencies have not survived the test of time. Twenty percent failed through hyperinflation, 21% were destroyed by war, 12% destroyed by independence, 24% were monetarily reformed, and 23% are still in circulation. The study shows that the life expectancy for fiat currencies on average has been 27 years based on history. Founded in 1694, the British pound Sterling is the oldest fiat currency today. However, from the perspective of value, the British pound is worth less than 0.5% of its original value (based on silver) today. Consecutively, the currency has lost 99.5% of its value due to inflation.

In the beginning, cryptocurrencies were often equated with the term *cryptoassets* (Gurguc & Knottenbelt, 2019). Cryptocurrencies are digitally represented assets designed to work as a medium of exchange using cryptography. Token ownership records are recorded in a ledger database which is typically distributed throughout a network of participants, making it decentralized (Dourado & Brito, 2014). Such a distributed database enables the network to be in consensus about *the truth of the majority*, making the system reliable against problems that usually occur within traditional centralized financial models, as spending the same funds more than once (double-spending problem). Many cryptocurrencies are decentralized networks that are based on Blockchain technology. One of the main characteristics of cryptocurrencies is that they are generally not issued by any central authority and are immune to manipulation by a central bank or government. According to Narayanan et al., (2016) “Cryptocurrencies too must have security measures that prevent people from tampering with the state of the system and from equivocating”.

Although the idea of digital currencies emerged earlier, bitcoin was the first widely adopted digital asset. Bitcoin was a project following a one-page whitepaper from an anonymous using the pseudonym *Satoshi Nakamoto* in January 2009. From then until today, many alternative coins have used the infrastructure under which bitcoin was built upon. Since the distributed ledger network Bitcoin has a pre-programmed fixed supply of 21 million tokens to be ever in circulation, many believe the asset is deflationary by design. The design code (script) is publicly accessible

and although the copy of the code can be modified and built upon, it is not possible to change the properties of the Bitcoin network. Although the idea of a digital currency is simple, the execution is difficult because of a known problem that Bitcoin claims to have solved, the Byzantine Generals Problem.

In decentralized networks, the problem is trust between parties. How can parties which inherently don't know each other achieve trust is where researchers and developers discovered that Bitcoin is more than an attempt of a digital currency. In only a decade, it proved to be one of the most robust examples of distributed ledger technology. Transactions on the Bitcoin Blockchain are recorded and accessible for public inspection. However, the public ledger doesn't reveal sensitive information, making it quasi-anonymous.

The transactions are being validated by computers (usually *mining rigs*) called nodes. They maintain the accuracy and consensus of the ledger by holding a full copy of the ledger which is constantly updated. Nodes verify wallet-to-wallet transactions in a process called *mining*, by solving complex mathematical algorithms. The first node that successfully verifies a transaction receives the transaction fee paid by the sender and a reward from the network. Verified transactions are stacked together in blocks in a chain-like manner. Bitcoin uses the Proof of Work consensus mechanism, but in the past decade, many other forms of consensus mechanisms have arrived.

The value of a cryptocurrency is determined liberally, namely on the free market which is driven purely by supply and demand. Although bitcoin and other cryptocurrencies can be sent from one wallet to another directly in a peer-to-peer fashion, they are usually traded on one of the centralized cryptocurrency exchanges. The price is determined with the help of an order book, which is also common on the stock exchange. Since many exchanges have had their security systems breached (or *hacked*), decentralized exchanges (or DEXes) are starting to emerge with a unique system that doesn't need a centralized market maker, by ensuring liquidity through AMM (Automated Market Making).

And although cryptocurrencies are not backed by an asset such as gold or a promise from the government, there is a debate whether there is any *intrinsic value* behind cryptocurrencies. Most cryptocurrencies are backed by nothing in the real world, and thus many financial experts believe it is a speculative asset. The main idea behind Bitcoin is to have a monetary system independent from central banks, governments, corporations, or any centralized entity. This idea was inspired by economic downturns called *crashes* and limited options for the average person to hedge against such events apart from physical gold (Gartz & Iinderbrandt, 2017). But since there is nobody physically guarding the network, barriers for potential attacks are theoretically non-existent, which is why cryptography plays a crucial role in keeping the network and its participants secure. This is achieved through public-private key cryptography (Houben, 2015).

Cryptocurrencies remove intermediaries, so each transaction is settled quickly and directly between two users with access to a computer device. Transactions are safer than standard banking systems and can be done regardless of the user's location. The decentralized nature of the open code protocol ensures that network control remains in the hands of users. Transactions depend on network participants, and the user's funds cannot be retrieved if they have been lost or sent to a wrong address, since there is no third party such as a banking institution that could revert a transaction.

3.2 Concept and legal framework of cryptocurrencies

The peak of the digital revolution began in the last decade of the 20th century, and it is most visible through making digital communication devices more accessible for the masses, and the placement of the Internet in the private sphere (Cunjak & Mataković, 2018). The European Central Bank (ECB) has classified cryptocurrencies as a subset of virtual currencies (European Parliament, 2017). Initially, in 2012, the ECB defined cryptocurrencies as a form of digital money, usually issued and controlled by its founders (European Parliament, 2017). With the emergence of Blockchain technology and cryptocurrencies, the situation today is somewhat different than before. Namely, states are increasingly reaching for the regulation of this matter to limit the use of cryptocurrencies for illicit and illegal purposes, in any way. The report from the World Economic Forum from 2018, published by the Financial Times, had a simple title: "Blockchain can no longer be ignored" (Arnold, 2018). The World Economic Forum pointed out that it is crucial to regulate to prevent the use of cryptocurrencies through the Dark Web and enable proper use through normal financial flows (Herian, 2019).

For years, financial institutions and governments of most countries have issued warnings about the dangers that exist in connection with investing in cryptocurrencies. Such warnings, usually issued by central banks and state treasuries, are mainly intended to educate citizens about the differences between fiat currencies and cryptocurrencies, which are not issued by an organ that has constitutional authority about declaring intrinsic value to a currency (The Law Library of Congress, 2018). In 2018, much research was conducted on this topic, which included governments around the world. Namely, most countries were against cryptocurrencies, but at that time some countries considered that cryptocurrencies were not a threat and that their role would be seen primarily in finance in the future, and these were primarily Spain, Belarus, the Cayman Islands, Iceland, and Luxembourg (The Law Library of Congress, 2018). Switzerland and Liechtenstein are the countries that were the first to regulate cryptocurrencies. Some jurisdictions are trying to go even further and develop their own cryptocurrency system. This category includes a diverse list of countries, such as the Marshall Islands, Venezuela, Central Bank of the Eastern Caribbean (ECCB) member states, and Lithuania (The Law Library of Congress, 2018).

Over the years, the issue of regulation has changed greatly. Namely, in 2020, the monetary authorities of China completed the design of the CBDC (Central Bank Digital Currencies) which

demanded global operational standards for real-world operation. Furthermore, the mentioned framework was applied by countries such as the Bahamas, Japan, France, Great Britain, Australia, Switzerland, while Brazil announced the launch of the CBDC before 2023 (Seba Bank, 2021).

In 2021, the Basel Committee on Banking Supervision (BCBS) pointed out several novelties related to cryptocurrencies and cryptoassets based on the discussion paper *On designing prudent treatment of cryptocurrencies* published in December 2019. There it explained that banks face certain risks when dealing with cryptocurrencies that outweigh traditional liquidity, credit markets, operational risks, money laundering, and terrorist financing (Seba Bank, 2021).

3.3 The concept of Bitcoin

Bitcoin is the first decentralized, permissionless, and public Blockchain network. It uses bitcoin as the native currency for peer-to-peer transactions within the protocol (Antonopoulos, 2014). Its unique characteristic is that it is the first worldwide digital currency issued without a central bank to gain mass adoption. Essentially, bitcoin is data that is transferred between digital wallets in form of transactions. Its uniqueness lies in the fact that (end-to-end) transactions are executed without intermediaries. It was never before the case that a payment can be made without a trusted centralized body being involved in the issuance, administration, or maintenance of a currency system (Forman et al., 2019). The network protocol *Bitcoin*, using the cryptocurrency *bitcoin* (*btc)* was created by Satoshi Nakamoto (pseudonym) as an open-source project in 2009 (Forman et al., 2019). Bitcoin is of particular interest to economists as a virtual reserve currency that has the potential to disrupt existing payment systems, and perhaps monetary systems (Böhme et al., 2015).

The idea of Bitcoin emerged first within the cypherpunk community and was inspired by economic crises, monetary instability, and corruption of a highly centralized financial system (McLean & Nocera, 2011). The whitepaper *Bitcoin: A Peer-to-Peer Electronic Cash System* was released in 2008, in the year when Lehman Brothers, the fourth-largest bank in the USA, officially filed for bankruptcy, leaving many in poverty (Wiggins, Piontek & Metrick 2014). Shortly after the collapse of the systemically relevant bank and the largest bankruptcy in the United States, a global crisis emerged beyond the *housing bubble burst* that resulted in an aggregated economic damage measured approximately at $10t (Wiggins, Piontek & Metrick 2014). The causes of the crisis led from missing regulation, lack of financial supervision, to corruption. Apart from the multi-factorial complexity of financial crises in the past, the importance of Bitcoin as an emerging idea was to provide an alternative in a financial crisis such as the 2008 crisis (White, 2009). The financial system came under public pressure because of the subprime mortgages and dubious synthetic financial derivatives (collateralized debt obligations) consisting of housing mortgages, backed by NINJA loans (no income, no job, no assets). These complex financial instruments named CDO's were assigned the highest security rating (AAA) by prestigious auditors and

rating agencies (Randall & Mills, 2008). The state (and its citizens) had to bear the consequences of financial sanitation, in the form of bank bailouts to save what was left of the financial system (Congressional Budget Office, 2020). The public questioned the fairness and justice of such a financial system, where the majority has to bear for the costs whereas financial executives were awarded bonuses (Ferraro, 2009). This phenomenon of a monopoly (power, and knowledge is not new, but the effects can lead to a market failure scenario based on the asymmetry of information because of moral hazard (principal-agent problem) and adverse selection. In theory, principals are incentivized to act primarily in their interest to the detriment of others. The theory of Information asymmetry by Stiglitz et al addresses trust as a constituent element of a traditional economic system (Stiglitz, 2017). Trust is imminent in any centralized system because democratic decision-making can impair the quality and velocity of decision-making, that's why our history has been based on authority and trust in leadership. The idea of how to minimize centralized points of failure is a constituent part of why decentralization is a property of Bitcoin, which is supposed to be trustless, decentralized, permissionless by default. Bitcoin is believed to be an alternative to a central bank in an existing monetary system, based solely on pre-programmed rules. Blockchain technology promises to bring immutability, transparency, and trust.

The idea of Bitcoin was to solve this problem in a way that individuals have full autonomy and responsibility in a parallel monetary system based on the rules of such a protocol, beyond the reach of state intervention. Traditionally, financial intermediaries such as banks were responsible for keeping the balances of clients in a centralized way. They were the providers of basic financial infrastructure and trust was the main constituent to prevent fraud and the possibility of making multiple transactions with the same funds (double spending problem).

Although many forms of e-cash were known, the *Proof of Work* consensus algorithm revolutionized and eliminated the need for trust. This system introduces *miners* as validators to work in their interest by maintaining a public copy of the public and decentralized ledger. Miners were contributing to the security and robustness of the system by verifying transactions and received, firstly, a reward for each successfully verified transaction (block reward) and secondly, the transaction fee paid by the sender (transaction fee). This concept of maintaining system robustness through a consensus mechanism is based on the zero-knowledge proof method that was invented in 1993 by Dwork and Naor as a proposed solution to *DDoS* attacks (distributed denial of service, or *spam* in layman terms) where the goal is to crash the server due to overload. It gained popularity and practical applicability precisely because of its use in the Bitcoin protocol, which makes such an attack too *expensive* due to high resource consumption while performing such an attack.

Bitcoin uses a security method called PoW to maximize security. It is a method that is based on information that is difficult to create and provides other participants easy verification and verification of transactions. Cryptocurrencies are stored on decentralized wallets (public key) on the

network for which the private key represents a unique string of letters and numbers acting as a back-up password.

The process called mining is a key security feature of the Bitcoin network. The idea is for Bitcoin miners to solve cryptographic puzzles and accumulate transactions in a block, and add the last block to the previous one, forming a block-chain. They then perform a cryptographic hashing operation based on trial and error until a hash value is produced as output. For Bitcoin, the hash function is a function called SHA-256, which uses the National Security Agency's (NSA) security level encryption standard using ECDSA (Elliptic Curve Digital Signature Algorithm). To provide additional security, Bitcoin uses the SHA-256 function twice, a process known as double SHA-256 (Stiglitz, 2017).

The Bitcoin Blockchain is constantly updated and the record history is stored throughout nodes that act as guardians of data throughout the globe. This ledger of transactions is storing information about how much bitcoin each user has in his wallet. The wallet contains information about the amount of bitcoin the user owns, history of all of his transactions, the user's secret private key, and his public address (Bartlet, 2016).

Since all transactions are tracked, counterfeiting is impossible. Although ownership of bitcoin can be transferred, it cannot be changed or duplicated. The pseudonymity provided when making a transaction is one of the key reasons for the success of Bitcoin today. When digitally paying with bitcoin, it is not necessary to provide any personal data, making KYC/AML rules non applicable on the network layer. Every user has absolute control over their funds, meaning that only a person with a private key can access and determine the destiny of the bitcoin at that address. Banks or any other organizations are not needed to store sensitive data and asset records because every bitcoin transaction is recorded by computers throughout the network. All transactions are finalized faster than by traditional banking procedures, without unnecessary intermediaries, with less infrastructure needed to make payments across state borders. Bitcoin provides its users with security without identification, making it difficult for unauthorized access, intervention or succession. The advantages can also be viewed as its biggest disadvantages because it makes taxation and supervision of users extremely difficult when needed for public security.

The guarantee of the value of bitcoin is designed on the model of flammable metals, which are limited in nature, primarily gold. For that reason, Satoshi determined in the bitcoin code that there is a maximum of 21 million tokens ever in existance and that if the Bitcoin protocol remains the same, the last bitcoin is predicted to be mined in 2040. According to some forecasts, as early as 2035, 99% of the programmed Bitcoin network supply will be in circulation (20,800,000 BTC, while in 2140 the interest in further mining in today's sense of the word (Proof of work mechanism) will disappear because huge resources would be needed to mine every additional bitcoin (Hayes, 2020). Although bitcoin has a reputation for instability, large fluctuations, and illegal activities, to which many add the collapse of the traditional concept of monetary systems, most

still agree that its emergence is one of the most disruptive ideas since the emergence of the Internet (Vigna & Casey, 2016). The millennial era is known for the rapid development of technology where innovative technologies could be integrated into various scientific and technical disciplines (Min, Jeanne & Suk Hi, 2018). Stakeholders could join forces in a "fusion of technologies that blurs the boundaries between the physical, digital and biological spheres" (Schwab, 2016). This fusion of technologies goes beyond mere combination. Fusion is more than just complementary technology because it creates new markets and new opportunities for the growth of each participant in a given innovation (Min, Jeanne & Suk Hi, 2018). According to Schwab (2016), Blockchain has a profound innovative potential. In his opinion, Blockchain technology is likely to give rise to countless other technologies, starting with the financial sector and progressing to many other sectors. Schwab (2016) mentiones that Blockchain is a constituent of the upcoming fourth industrial revolution and its impact will be mainly in tracking registrars for birth certificates, title deeds, marriage permits, company registrations and global proof of ownership.

3.4 Ethereum

Ethereum is a decentralized, public, permissionless, Turing-complete Blockchain platform introduced in 2013 (Buterin, 2013). The creator of the Ethereum platform is Vitalik Buterin, who first introduced his idea as an improvement to Bitcoin. Backed by notable technology leaders, the idea emerged as an independent project in 2015. Ethereum is a protocol based on Blockchain technology which is similar to Bitcoin, but with several notable differences. Ethereum at the moment is likewise using the *Proof of Work* consensus mechanism introduced by Bitcoin, but initial steps have been made towards the transition to *Proof of Stake*. The main differentiating factor is the Turing completeness property of the Ethereum Blockchain which offers more flexibility. Developers can use the existing Ethereum ecosystem with its self-executing pre-programmed rules as a framework for building their cryptographic tokens, launch new projects, and develop *on top* of the Ethereum Blockchain (Zmaznev, 2017). This became popular in 2017 and led to an Initial Coin Offering (ICO) craze, as a new way to fundraise and launch new projects (Lambert, Liebau & Roosenboom, 2020). The Bitcoin community didn’t embrace Ethereum as an alternative because of its token creation flexibility, which led many to believe it was a launchpad for scam projects when it was first introduced. The Bitcoin community criticized Ethereum for not being deflationary in nature with a fixed pre-programmed supply of the platform native currency eth, which opens the possibility of diluting existing token holders through inflating the token supply. Ethereum's vision was to serve as a building block for creating new projects rather than a *digital central bank* and a store of value. Ethereum is supposed to be a more *modern* Blockchain in this sense because of the possibility of creating Smart contracts (self-executing if-this-then-that actions), decentralized applications (dapps), and decentralized autonomous organizations (DAO). According to Swan (2015), Ethereum can be viewed as a successful step towards a more improved Blockchain ecosystem, calling it the *Bitcoin 2.0* (Swan, 2015).

Ethereum Virtual Machine (EVM) is a run-time environment that plays a crucial role in the Ethereum ecosystem. Similar to Bitcoin Core, EVM provides a framework for executing code with algorithmic complexity (Wood, 2017). For developers, EVM enables the creation of applications written in a programming language that is compatible with the EVM itself (Zmaznev, 2017). This software solution is compatible with several programming languages, which allows developers to launch their own dapps on a unique platform instead of creating several separate Blockchains which are not compatible with each other.

An early decentralized autonomous organization under the name *the DAO* developed a smart contract on Ethereum in 2016 and raised $150m to finance the project (Vigna, 2016). The DAO was exploited in June 2016 when an unknown hacker took advantage of the network's flaws and stole 11.5 million ethereum tokens (worth roughly 20b € in February 2021) (Popper, 2016). The aforementioned event sparked a debate in the crypto community about whether Ethereum should perform a hard fork to compensate for the seized funds (Peck, 2016). This was followed by a division of the network into two Blockchains: Ethereum and Ethereum Classic. The first is actually a new Blockchain network, while the latter is the old version. Ethereum classic is a Blockchain operating today, though many 51% and double-spending attacks are happening more and more often (Leising, 2017).

Blockchain systems can be divided into two groups, public or private. A public Blockchain is a Blockchain without any restrictions on network participation. Private systems are usually used for optimizing internal business processes where only predefined users can gain network access or must register to share predefined information with the system owner. Examples of such distributed ledger systems are Hyperledger or R3 Corda (BitFury Group, 2015).

Ethereum is a public Blockchain based on the Proof of Work consensus where smart contracts are written in Solidity (Franke, Schletz & Salomo, 2020). According to Bambara and Allen (2018), a smart contract is a computerized algorithm that essentially executes the terms of the contracts. For activities to take place publicly and without permission, Blockchains such as Ethereum require a consensus protocol that is resistant and robust to errors and failures. In Proof of Work, all the miners are competing against each other to create the next block. This process requires resources in the form of hashing power, which leads to energy consumption (Digiconomist, 2020). To solve this problem, various concepts have developed over time. Proof of Stake consensus is considered as the best alternative compared to PoW today. However, it is important to note that there is always a trade-off between decentralization, security, and scalability. Unlike PoW, PoS does not use computing power (mining) to verify new transactions but rather *locks* funds in the user's wallet (staking) with which transactions are validated. Ethereum Foundation has taken steps to move to Ethereum 2.0 with the aim of implementing PoS with Istanbul hard fork as an initial step in January 2020 (Dexter, 2018).

Since Ethereum is a live network with a lot of users, this transition is not easy and the migration of Ethereum to Ethereum 2.0 is a process that is going to take years, preventing stakers from unlocking their stake for the period of transition. Through implemented technological upgrades, Ethereum has become a more advanced cryptocurrency with higher and faster transactions and achieved the first major adoption milestone as an alternative currency (altcoin) compared to Bitcoin (Zmaznev, 2017). Although the Ethereum network is facing congestion and high gas fees making it unsuitable for day-to-day transactions, it is far more scalable than its Gold-on-Chain big brother Bitcoin.

Scalability is the reason for high transaction fees on *Ethereum mainnet*. There are currently two approaches to solving this problem. On the one hand, Ethereum is implementing improvements of the *mainnet* (from Ethereum 1.0 to Ethereum 2.0, meaning the transition from PoW to PoS) to achieve its long-term scalability goals. On the other hand, *layer 2 (L2)* solutions are being developed rapidly, enabling the settlement of transactions outside of the Ethereum protocol. Layer 2 scaling solutions are common for the Bitcoin protocol as well (Lightning network). In the next figure is a comparison between Bitcoin and Ethereum and an overview of transaction, application, and aggregation layers.

Scalability is the reason for high transaction fees on *Ethereum mainnet*. There are currently two approaches to solving this problem. On the one hand, Ethereum is implementing improvements of the *mainnet* (from Ethereum 1.0 to Ethereum 2.0, meaning the transition from PoW to PoS) to achieve its long-term scalability goals. On the other hand, *layer 2 (L2)* solutions are being developed rapidly, enabling the settlement of transactions outside of the Ethereum protocol. Layer 2 scaling solutions are common for the Bitcoin protocol as well (Lightning network). Figure 5 shows an overview of transaction, application, and aggregation layers

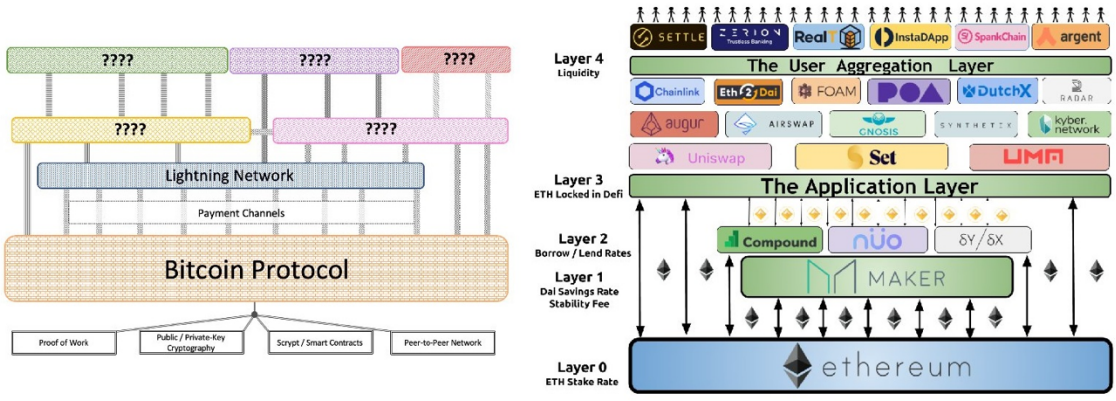


Figure 5. Bitcoin and Ethereum protocol layers & tech stack, Framing bitcoin (2020) accessible at https://framingbitcoin.com/bitcoin-vs-ethereum-protocol-tech-stack-overview/

As visible in Figure 5, Smart contracts are the main differentiating factor between Ethereum and Bitcoin. Smart contracts can perform any predefined actions on the Ethereum Virtual Machine

(EVM). The above-mentioned gives Ethereum flexibility. Just like Bitcoin, block creation occurs when transactions are bundled and submitted in a chain-like fashion. Unlike Bitcoin, Ethereum follows a different pattern for selecting blocks that are added to a valid Blockchain. Ethereum follows a protocol called GHOST (Crypto Compare, 2015). Ghost protocol contributes to a reduction in lost computer power and increases incentives for slower nodes. Thus, enabling faster confirmation of transactions. While blocks are usually created in Bitcoin every 10 minutes, Ethereum can do it within minutes. (Peyrott, 2017).

There are various industries where smart contracts can be applied in the future. Some of these applications are (Alharby & van Moorsel, 2017):

- Internet of Things, Smart property: An interconnected world is full of nodes that share data over the Internet. The impact of Blockchain-based smart contracts is allowing those nodes to share or access different digital properties reliably and without a centralized point of failure (Christidis & Devetsikitois, 2016).
- Music Rights Management and E-commerce: potential use is to facilitate and trade between parties without a reliable third party. This would result in a reduction in trading costs. Smart contracts can only forward a payment to the seller when the customer is satisfied with the product or service they receive. There are other possible applications such as e-voting, mortgage payments, digital rights management, car insurance, distributed file storage, identity management, and supply chain.

Decentralized applications are another innovation brought by Ethereum. They are described as peer-to-peer applications. Their unique characteristic is that no server or entity controls them, making them censorship-free (Metcalfe, 2020). The prototypical modern software application includes at least one user interface (UI) (Metcalfe, 2020). From a big picture perspective, Ethereum is a Blockchain enabling automated transactions based on pre-approved sets of rules in the form of Smart contracts, which run on the back end. A dapp is a front-end solution that encompasses the smart contract(s) so that the end-user can interact with it in a more user-friendly way, by connecting his wallet (usually as an extension in the browser) directly to the web application (dapp).

The benefits of using Blockchain dapps are reflected in the following (Metcalfe, 2020):

1. The user can see what happens before performing the function or sending any data.

2. Once a user signs, approves and the transaction is verified, it cannot be withdrawn, planted, or deleted. In itself, these properties are extremely useful. This is the same as protocol-level decentralization.

3. Management can be decentralized so that dapp users can interact with websites directly with the use of their browser-integrated wallets.

When it comes to disadvantages, *Scalability* is the main point that plagues Ethereum and other Blockchains. Several remedies come at a cost of decentralization and security such as rollups, sidechains, etc. The most discussed are currently *zk-rollups* and *optimistic rollups*.

An example of the latter is *Optimism* which offers an easy way to migrate existing *dapps* without compromising on security and scaling by a factor of 100x. Privacy is given by default, but it comes with the compromise of security. As a result, *nasty tails* can result in loss of funds due to theft with attack vectors (Adler, 2019).

ZK-Rollups are a more advanced and sophisticated method of achieving Zero-Knowledge Proof. It uses a method called *SNARK* (succinct non-interactive arguments of knowledge), meaning that transactions are pre-verified by the *rollup* contract. According to Sasson et al., (2014) allows one party to prove to another possession of certain information without revealing that information. The old Merkle root redirects to the new one and is thus not susceptible to manipulation by operators (Reitwießner, 2016).

Ethereum's current throughput is about 25 transactions per second, making it better than Bitcoin, which can only do seven transactions per second. Although, in practice, the transactions are still too expensive for mainstream usage. This low transaction throughput happens because of the amount of time it takes to validate and put a transaction within the block. Raiden was to be the first L2 scaling solution for the Ethereum network, but other solutions such as Plasma, Matic/Polygon are quickly gaining adoption (Buterin, 2016).

Matter Labs has presented aspects taking into consideration security, performance, usability and other factors in a table serving as a framework for evaluating (dis)advantages of scalability solutions. Table 2 compares state channels, sidechains, plasma, optimistic rollups, zkRollups and validium serving as an insight into the scalability concerns in the industry today.

	State channels	Sidechains[0]	Plasma	Optimistic rollups	Validium	zkRollup
Security						
Liveness assumption (e.g. watch-towers)	Yes	Bonded	Yes	Bonded	No	No
The mass exit assumption	No	No	Yes	No	No	No
Quorum of validators can freeze funds	No	Yes	No	No	Yes	No
Quorum of validators can confiscate funds	No	Yes	No	No	Yes [1]	No
Vulnerability to hot-wallet key exploits	High	High	Moderate	Moderate	High	Immune
Vulnerability to crypto-economic attacks	Moderate	High	Moderate	Moderate	Moderate	Immune
Cryptographic primitives	Standard	Standard	Standard	Standard	New	New
Performance / economics						
Max throughput on ETH 1.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	2k TPS [3]	20k+ TPS	2k TPS
Max throughput on ETH 2.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	20k+ TPS	20k+ TPS	20k+ TPS
Capital-efficient	No	Yes	Yes	Yes	Yes	Yes
Separate onchain tx to open new account	Yes	No	No	No	No	No [5]
Cost of tx	Very low	Low	Very low	Low	Low	Low
Usability						
Withdrawal time	1 confirm.	1 confirm.	1 week [4] (?)	1 week [4] (?)	1..10 min [7]	1..10 min [7]
Time to subjective finality	Instant	N/A (trusted)	1 confirm.	1 confirm.	1..10 min	1..10 min
Client-side verification of subjective finality	Yes	N/A (trusted)	No	No	Yes	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded	Bonded
Other aspects						
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes	Yes	Yes
Native privacy options	Limited	No	No	No	Full	Full

[0] Some researchers do not consider them to be part of L2 space at all, see https://twitter.com/gakonst/status/1146793685545304064

[1] Depends on the implementation of the upgrade mechanism, but usually applies.

[2] Complex limitations apply.

[3] To keep compatibility with EVM throughput must be capped at 300 TPS

[4] This parameter is configurable, but most researchers consider 1 or 2 weeks to be secure.

[5] Depends on the implementation. Not needed in zkSync but required in Loopring.

[7] Can be accelerated with liquidity providers but will make the solution capital-inefficient.

Matter Labs

Table 2. Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework, Gluchowski (2020), accessible at: https://medium.com/matter-labs/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955

3.5 Decentralized finance - DeFi

In a centralized financial system, financial institutions are key intermediaries ensuring that a transaction can be controlled, monitored, processed in a trustworthy way. (Chen & Bellavitis, 2020). Intermediaries helped reduce transaction costs, enabling financial transactions to be conducted smoothly and efficiently in the past (Benston & Smith, 1976). The problem is that centralization of financial institutions enables to accumulate disproportionate market power and profit over time. Thus, many financial institutions have become dominant players and have decision-making power beyond the financial industry domain (Chen & Bellavitis, 2020). In contrast, in a decentralized financial system, financial transactions are not in the hands of a centralized institution but a decentralized peer-to-peer network (Treiblmaier, 2019). By reducing the participation of centralized institutions, decentralized networks can reduce transaction costs and create network effects without creating monopolies (Catalini & Gans, 2019).

Decentralized finance, shortly known as *DeFi*, emerged as an idea recently. Those enable building whole financial ecosystems based on Blockchain technology. The prerequisite for creating such an ecosystem are fully functional and sustainable decentralized protocols using Smart contracts and dapps. The most known DeFi ecosystems today are Ethereum , Polkadot, Cardano but many more are likely to be built in the future (Blockchain for DeFi, 2020).

DeFi is the most popular investment category accommodating the highest influx of VC investments) in the Blockchain industry in 2020, which can be seen in Figure 6 from The Block research.

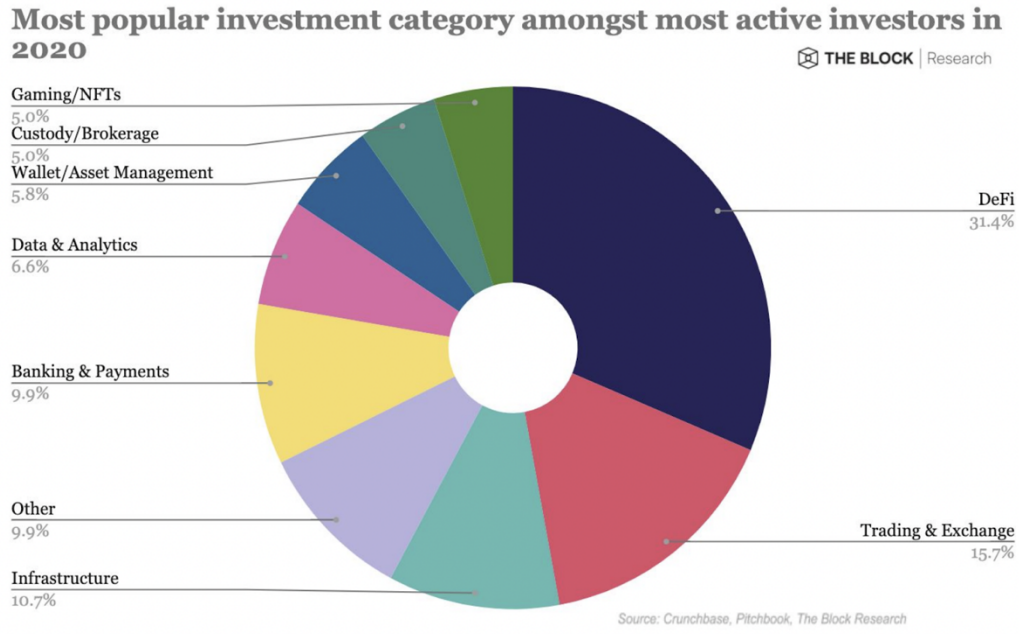


Figure 6. Most popular investment categories, source: Cermak et al. (2021)

DeFi created a wide range of use cases for individuals, developers, and institutions (Blockchain for DeFi, 2020). The basics of all DeFi protocols are smart contracts which enable automated

processes and usually refer to applications performed in parallel by a large set of validators on a Blockchain ecosystem (Schär, 2020). They have access to a rich set of established instructions and for this reason, experts from the financial field can utilize them in existing ecosystems without extensive need for know-how in Blockchain technology. This enables building a bridge between traditional finance and decentralized finance (Schär, 2020).

As seen in Figure 7, DeFi is composed of a multi-layer technology stack that includes core *infrastructure*, the *consumer* side, and *bridges* to legacy systems. Figure 7 presents an overview of the current DeFi ecosystem with a wide variety of use cases including decentralized exchanges (*dexes*), decentralized borrowing & lending, decentralized insurance and oracles.

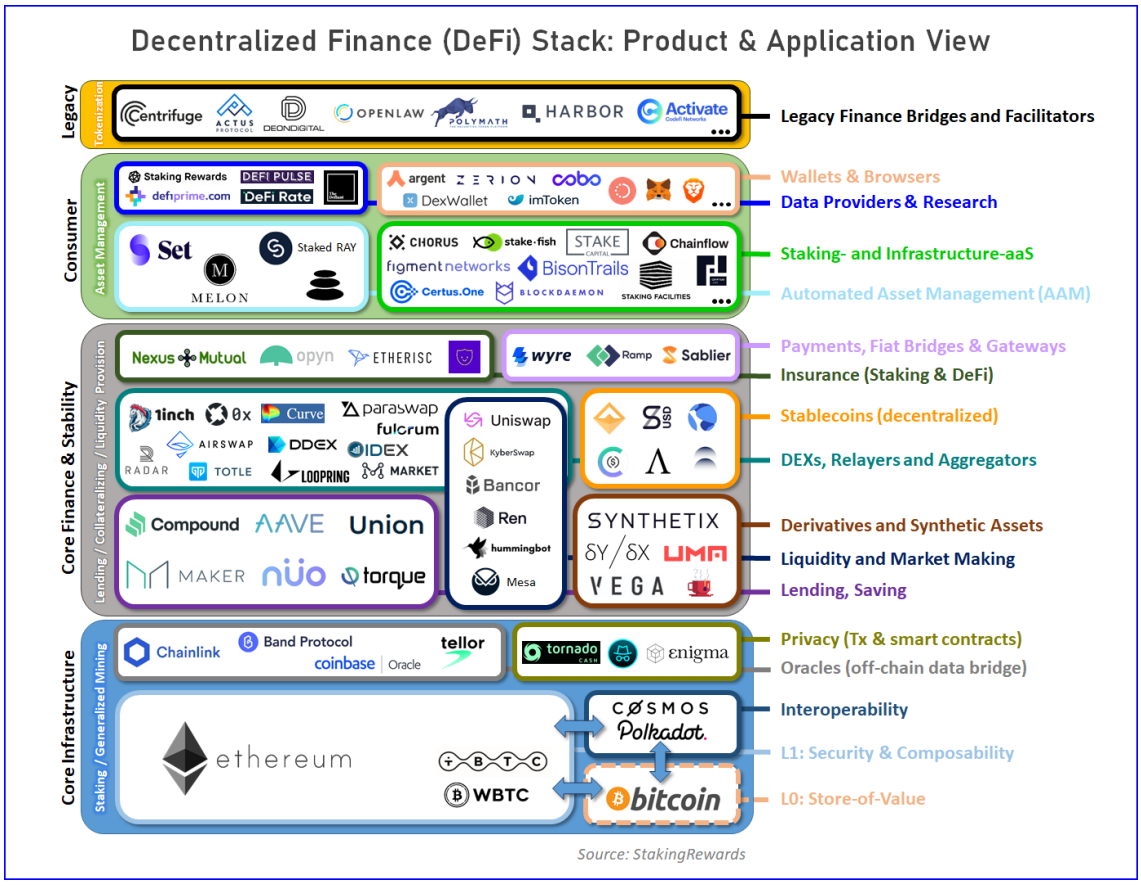


Figure 7. DeFi Digest and Common Issues, Dudka (2020), accessible at: https://www.stakingrewards.com/journal/defi-digest-ecosystem

While there are alternatives such as Polkadot/Kusama and Cardano, the Ethereum protocol is still the largest platform and the ecosystem of choice for developers when it comes to DeFi Web 3.0 *dapps* with a *total value locked* in the protocol of roughly $50 billion (and rapidly rising) which can be seen in Figure 8.

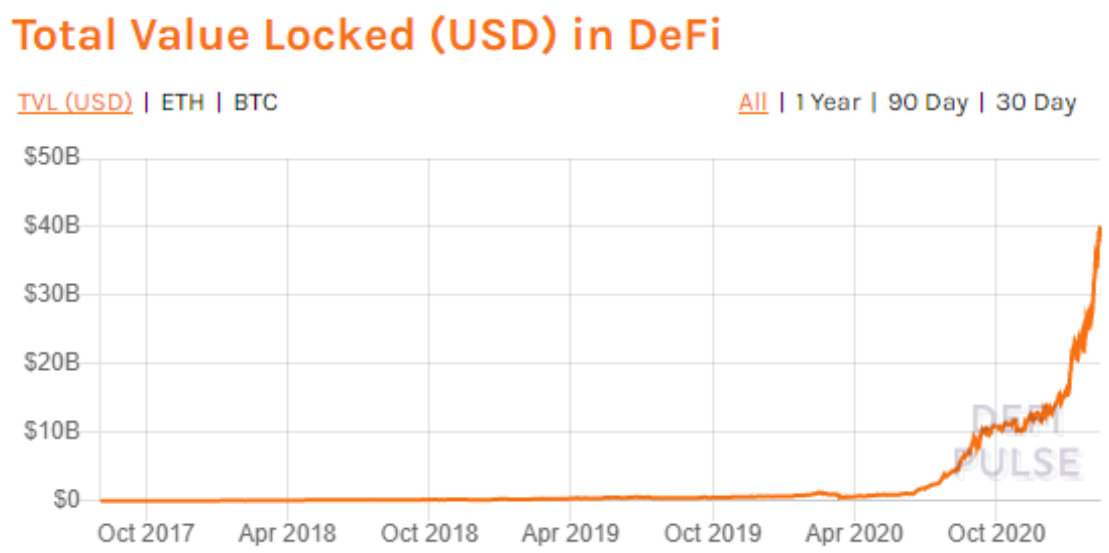


Figure 8. Total value locked in DeFi, source: DEFI PULSE, accessible at: https://defipulse.com/

Cryptocurrencies are known for their notorious volatility and the need for *stablecoins* was increasing after Tether, a company issuing the stablecoin USDT pegged to the US dollar, raised controversy because of the company's inability to provide a promised audit showing adequate reserves for their tokens.

When it comes to stablecoins, Maker DAO was one of the first projects to create a decentralized mechanism for stabilizing the value of the coin by pegging ether to the value of the US dollar. Its stablecoin *DAI* uses collateralized ether to stabilize values instead of a central authority. DAI is a token using the ERC20 standard that can be freely traded on all public (de)centralized exchanges within the Ethereum ecosystem (Stein, 2018). Any person who owns an Ethereum network compatible wallet can own, accept and transfer it using exchanges without any intermediaries.

No government has control over it, so no one can limit its issuance or exclude its use. DAI offers instant cross-border transfers with low transaction fees, and traders can accept this without the risk of volatility (Stein, 2018). Nonetheless, many other stablecoins, such as USDC, have been gaining adoption besides centralized stablecoins such as BUSD, PAX USD, USDT.

The first widely used ERC20 *decentralized exchange (dex)* was Uniswap, which introduced a special model for ensuring liquidity between two trading pairs. In centralized finance, trades are usually settled with the use of *order books* where a market maker settles the final price between two parties. Uniswap introduced a revolutionary model for settling transactions called automated market making (AMM). In this model, any token holder with a certain token pair (eth and dai for example) can provide liquidity by depositing an equal amount of tokens to a *liquidity pool* (for example 50% eth and 50% DAI) and earn fees from the Uniswap exchange for providing liquidity. This form of market making has been incentivized additionally on uniswap and other

decentralized exchanges, where it is possible to receive additional rewards in the form of additional yield. The yield is represented in additional ERC20 compatible tokens, which usually carry names such as sushi, pancake, spaghetti, yam, etc).

This model called *yield farming* swiftly gained popularity and was implemented by many decentralized exchanges such as Uniswap, Sushiswap, Mooniswap, Falconswap, Quickswap, 1inch and other platforms for providing liquidity through automated market making. Some companies have successfully forked the open source-code of uniswap and implemented their own DeFi ecosystems without scalability solutions due to centralization, such as the Binance smart chain. According to The Block research (2021), $120b in trading volume has taken place in 2020 throughout decentralized exchanges.

The idea of decentralized finance is to enable an alternative to the existing financial system that is fully decentralized, without censorship, more inclusivity, with lower fees, fully automated, and without counterparty risk (Bitkom, 2020). DeFi's idea it essentially to democratize financial services. In DeFi all actors can read the open-source code, ensuring full transparency which is unusual for centralized systems where customers have much less knowledge of what happens in the backend of a centralized financial institution (Bitkom, 2020).

DeFi stems from two important patterns in technological evolution: *Moore's Law* and *Kryder's Law* (Zetzsche & Arner, 2020). Moore's law suggests that the amount of data processing power is growing exponentially while Kryder's law says the same for increasing data storage capacity (Zetzsche & Arner, 2020). The combination of these two laws leads to lower costs. The third form is reflected in the assumption of bandwidth growth with cost reduction supported by an increase in network efficiency, which leads to a greater width of the scope per dollar invested (Zetzsche & Arner, 2020). These three evolutionary patterns enable hardware virtualization making hosting, updating, and operating decentralized systems more efficient (Zetzsche & Arner, 2020).

By eliminating the need for certain intermediaries, DeFi services are predicted to reduce the average global remittance fee from its current 7% to a significantly lower average of 3% (Hoffman, 2020).

In addition to all the above-mentioned advantages, DeFi also has certain risks. Namely, if there are coding errors, these errors can potentially create vulnerabilities that allow the attacker to drain smart contract funds (Schär, 2020). Cermak et al. (2021) estimate that $120m in total value has been exploited from DeFi protocols in 2020, indicating that DeFi is still at a nascent stage.

In 2021, hacks and exploits occurred in Alpha homora (February, $37m), YFI (March, $11m) Furucombo (March, $14m) and Paid network (March, $37m). This trend is expected to continue until DeFi reaches maturity. According to *Lindy's law,* a technology's life expectancy doubles with every year of its existance (Taleb 2012).

3.6 The impact of cryptocurrencies on developing countries

The main characteristics of developing countries are a low index of human development (HDI) and an underdeveloped industrial sphere compared to other countries (O'Sullivan & Sheffrin, 2003). More often than not, developing countries have to rely on the strength of a reserve currency to prevent commodity swings, currency volatility, and general economic stability (Coudert, Couharde & Mignon, 2013). There is no clear definition of which countries are classified as developing countries. However, most of the countries declared as developing countries have common characteristics, which can be seen as a criterion for determining which country is a developing country (Holtmeier & Sander, 2019). These similarities are reflected in inadequate food offerings for large groups of populations, low per capita income and poverty in general, lack of educational opportunities, lack of access to health care that accompanies high infant mortality rates, and low life expectancy (Holtmeier & Sander, 2019). Another problem that occurs in developing countries is low levels of social trust, as social trust seeks to improve economic growth and living standards in general (Barham et al., 1995). These characteristics lead to increasing unemployment and lower living standards.

Given the ongoing problems with the financial infrastructure today, cryptocurrencies can speed up the development process in various fields, giving underprivileged societies the necessary framework for democratic participation in a global economy. The only resource needed are internet access and to benefit from international trade and improvements in living standards through Blockchain technology (Holtmeier & Sander, 2019). For this reason, it is necessary to increase internet usage in developing countries (Tapscott & Tapscott, 2016). Cryptocurrencies such as Bitcoin could help individuals and companies facilitate transactions without having the need to set up expensive infrastructure (Holtmeier & Sander, 2019). Some cryptocurrency projects are especially focusing on banking the unbanked, to achieve greater financial inclusion of the developing world population, such as Cardano Foundation (Crypto News, 2020). Multiple wallets (and addresses) can be created on a single device and users can send and receive cryptocurrencies reliably on every computer with a browser, without having to own one. This way, underprivileged societies can also reap the benefits of more sophisticated financial transactions, even saving and lending in the future (Honohah, 2008). Reducing transaction costs could also increase the availability of microcredits, as cash transaction currently faces high costs (Holtmeier & Sander, 2019). In addition to all of the above, cryptocurrencies, mainly combined with smart contracts, can contribute to strengthening social trust and fighting corruption through a more transparent system (Holtmeier & Sander, 2019). This system can be extended from financial services, to administration and legal dispute resolution with proper governmental support in the future.

3.7 Problems caused by the emergence of cryptocurrencies and illegal activity

The development of the internet has led to a new form of crime, online crime or cybercrime. Just as all other segments of society have changed and improved illicit activities intact with the development of technology, so has the world of crime shifted into the sphere of cybercrime. The emergence and development of cryptocurrencies have created great opportunities for cybercrime expansion. This is due to the privacy, security, and reliability of cryptocurrency transactions. Anonymity is most commonly cited as the reason cryptocurrencies are suitable for criminal activity (FATF, 2019). However, tracking transactions and using them in conjunction with existing evidence material has enabled investigators to tell with certainty whether criminal activity has taken place because of the immutability and finality properties of Blockchain technology.

The FBI report from 2014 reveals that cybercriminals generally use technological advancements such as electronic payment systems and virtual currencies as a tool for convenience when buying or selling illegal goods (Ulbricht, 2014).

The use of cryptocurrencies for illicit activities is subject to public controversy because of the darknet. Bitcoin transactions can be done without KYC and AML compliance. The Bitcoin digital payment network is an alternative which provides a fast settlement layer on a quasi-anonymous way. Individuals on the dark web have been using bitcoin as a secure and private way of settling transactions internationally. This was done mainly on the online black-market known as Silk Road. Silk Road was launched in 2011 by Pirate Roberts and was shut down by the FBI and Europol in 2014. The total revenue generated from on Silk Road is estimated to be 9,519,664 btc, and the total commissions collected by Silk Road from the sales amounted to 614,305 btc. Total sales were equivalent to roughly $183 million and involved 146,946 buyers and 3,877 vendors (Ulbricht, 2014).

According to the report, illicit transactions have been falling from 2014 to 2016 (Foley, Karlsen & Putniņš, 2018). In the years 2017 and 2018, criminal activities using bitcoin have increased. Overall, in 2018 illegal transactions have amounted to 1% of all transactions, which is 7% lower than in 2012 (Chainalysis - Crypto Crime Report, 2019).

Technological advancements made cyber-attacks more common. Although many funds have been lost in the past due to hacks, exploits and phishing attacks, the Bitcoin blockchain has not been exploited. Due to the complexity of such attacks, multiple thousand wallets can be used to transfer and hide stolen funds, making it difficult for traditional financial forensics to track (Chainalysis - Crypto Crime Report, 2019).

Bitcoin is often in public debate used as an argument against terrorist financing (Eisermann, 2020). The rise of Bitcoin and other cryptocurrencies presents new challenges to combat money laundering and terrorism financing. Cryptocurrencies provide users who have the know-how to make global payments that are beyond the reach of anti-money-laundering policies and legal authorities. Also, there is a growing risk that terrorism financiers can avoid state supervision and take advantage of new sources of financing (Eisermann, 2020).

The way terrorist activities are financed differs from the way money is made, not whether it is a criminal offense of money laundering or another offense. Very often, funds to finance terrorism are created as a result of profitable criminal activities such as drugs and the arms trade. In practice, experience has shown that monetary amounts in the area of terrorism financing are "small and therefore easily passed through the regulatory network" (Eisermann, 2020). Besides, these funds often intertwine with legal cash flow sources, such as business earnings or savings. It is important to note, that cryptocurrencies are merely a tool that malicious users can use for their benefit, and therefore regulation and effective cooperation between institutions, governments, and society, in general, is needed to minimize crime and expose illicit behavior as soon as possible.

4 MILLENNIALS

4.1 The concept of millennials

The development of IT technology creates a whole new environment in which people live and work. Thanks to new technological progress, societies are becoming faster and more efficient. Education is being transformed due to technological innovation, which imposes the need for constant investments and upgrades in the educational sector. Students are not only learning how to use IT hardware and software at school, but it consumes a great part of their free time. These students are not only consumers when it comes to new technology products but a new source of knowledge (Oblinger, 2003). In the late 1980s, children were born in an extremely advanced technological environment compared to just years before. Today's students are the first generation to grow up surrounded by digital technology, from kindergarten to college. This generation is expected to be the result of the inclusion of modern digital technologies in everyday life, where all technological advantages are used for simpler communication, learning, or even playing. Due to the omnipresence of technology and more free time dedicated to experience digital products, today's students are often more digitally literate than their teachers, and the digital gap between generations is increasing year after year.

Many digital products today, such as computer games, the internet, e-mail, messenger, are integral parts of our lives (Veen & Vraking, 2006). Technology has drastically changed the way today's generation of children live, learn and think. The newest generation of people who have entered the workforce is called Millennials. Those born between 1980 and 1990 were more than 100,000. And in 2000, The New York Times, The New York Times, The New York Times. They were called millennials because of their closeness to the new millennium and growing up in the digital age (Kaifi et al., 2012). This generation has been influenced by computers and greater acceptance of non-traditional family values (Andert, 2011). For people born during this period, certain behavior is defined by the rapid adoption of technology and lack of loyalty to the existing global structure (Ingjing, 2018). As those generations have directly contributed to global technological evolution as consumers, it is characteristic of them that they are among the first to embrace, try and adopt emerging technologies or digital products.

Many positive and negative traits are characteristic of millennials. What sets millennials apart from other generations is that they're often confident, which allows them to be considered for leading positions in the workplace (Smith & Nichols, 2015). It is common knowledge that Millennials are focused on achievements. They need not only to do well but to outsmart all goals and aspirations (Kaifi et al., 2015). This leads them to seek new learning opportunities and to constantly improve their knowledge. When it comes to teamwork, Millennials enjoy working in teams and are more tolerant than previous generations (Smith & Nichols, 2015). What also separates them from other generations is that they became dependent on technology at an earlier

age than other generations. Research has shown that people who use technology in earlier years of their lives become more skilled than people who learn later. As more Millennials begin to take over, technology in the work processes is thought to be increasingly integrated (Deal, Altman & Rogelberg, 2010). Millennials expect technology to play a major role in the learning process, allowing them access to a wide range of information sources (Gibson & Sodeman, 2014).

Since millennials are a generation whose birth technology plays a big role, it can no doubt be said that it is a generation that is very familiar with cryptocurrencies and Blockchain technology. Accordingly, the next chapter will deal more closely with the study of the adoption of cryptocurrencies by millennials.

5 RESEARCH PART

5.1 Purpose statement

The purpose of the thesis is to gather more information about Blockchain technology (focusing on cryptocurrency adoption) to better understand its potential impact in the banking and finance industry, highlighting the (dis)advantages.

Since decentralized finance is a topic that is at the beginning of the adoption curve, there hasn't been much research conducted based on practice and the real potential is probably still unfolding or to unfold. With my thesis, my endeavour is to collect relevant information and organize the topic in a way that can emphasize the importance of research when it comes decentralized finance.

My method of choice for gathering information is through a survey for the general public structured by age, gender, and education where I can determine the state of mind of certain groups and identify factors that significantly contribute to making decentralized systems acceptable for mainstream usage and correlate the results with the aversion towards risk.

Furthermore, I will conduct interviews with industry experts where I will try to examine current challenges in finance and search for potential improvements Blockchain technology can bring to industry market makers in the next decade.

5.2 Research approach

To conduct the research in a structured manner, a research approach that relies on post-positivism has been chosen. More specifically, critical realism accepts there are objective realities and agreements about those realities. Critical realism is sometimes offered as an example of post-positivist positioning or even post-post-positivism.

5.3 Research objectives

The research objective is to better understand the adoption of cryptocurrencies using Blockchain technology to get a better understanding of the potential impact of DeFi on our financial system. Following the research objective, it will be possible to get an insight into the likelihood of adoption by individuals and organizations.

5.4 Research methodology

For the methodology part of the thesis, a mixed-method approach has been chosen. The term *mixed-method* refers to a newly developed research methodology that promotes the systematic integration or *mixing* of quantitative and qualitative data within a research program (Creswell & Wisdom, 2013). The main advantage of this methodology is that such integration allows for more complete use and analysis of data than a quantitative and qualitative collection and analysis separately. Research using the mixed method was first applied in social sciences and has recently been extended to natural sciences (such as medicine). Throughout the last decade, its procedures have been developed and refined to meet a wide range of research questions. (Creswell & Plano Clark, 2011). Particularly important is the fact that „mixed methods are especially useful for understanding the contradictions between quantitative and qualitative results“ (Creswell & Wisdom, 2013). In this thesis, the research was conducted in the form of a) an anonymous questionnaire and b) expert interviews.

5.4.1 Survey

Surveys play a major role in research, especially to find out what a larger group of people think. These include market research, policy surveys, customer service feedback, social science research, etc. (O'Leary, 2014). According to Kabir (2016) "a questionnaire is a research instrument that consists of a series of questions and other instructions to gather information from respondents". Although they are designed mainly for statistical data processing, there are a few exceptions. They have an advantage over some other types of research methods because they are much more economical and do not require as much effort from examiners as oral or telephone surveys and often have standardized answers that facilitate data collection. (Kabir, 2016).

There are two types of questionnaires, written and oral. In the past, written surveys were delivered to respondents by mail, but with the development of technology, today most written surveys are conducted through social networks and various online platforms. The pervasiveness of the survey is less than the pervasiveness of the interview due to the closed questions and answers and due to the very limited powers and tasks of the interviewers. Respondents are not asked to create, but to execute orders and implement instructions from the survey conscientiously and responsibly. The most common and most successful are individual, anonymous surveys. Anonymity essentially protects the privacy of respondents.

In total, 150 respondents were surveyed in the period from 28.12.2020 until 01.03.2020. The survey was delivered to the respondents by email. The target group of respondents were millennials in Vienna. With the help of an anonymous survey, the attitude of millennials in Vienna towards cryptocurrencies and openness towards adoption of cryptocurrencies have been investigated. The survey consists of several parts.

The first part of the survey (questions 1, 2, and 3) refers to general data on respondents (gender, age, and education). The fourth question of the survey is directed towards how familiar respondents are with Blockchain technology in the form of a Likert scale, where they were offered 5 options to choose from (1- not familiar at all, 5- very familiar). Questions 5-11 were formed according to the UTAUT 2 model (Venkatesh et al., 2012) considering the following components: Performance expectancy Effort expectancy, Social influence, Facilitating conditions, Hedonic motivation, Price value, and Habit.

These questions were formed on a multiple-choice basis. The following 3 questions (12, 13, and 14) are modelled using adapted questions from an official OECD research paper on Crypto Assets in the form of a Likert scale (based on UTAUT2). Questions 15-18 refer to trust in traditional financial organizations, where the goal was to find out to what extent respondents trust financial intermediaries (such as banks, payment providers, brokers, etc.), and whether the trust is directed towards CeFi or DeFi. Given the fact that cryptocurrencies are often associated with illegal or illicit activities, one part of the survey (questions 21-23) refers to the influence of the government on cryptocurrencies (attitude and restrictions on the use and potential of adoption of cryptocurrencies). The question under number 24 refers to education, specifically what the attitude of the respondents is towards implementing cryptocurrencies and Blockchain technology into formal education (in schools as one of the facultative or mandatory subjects for example). The last two questions relate to the way respondents perceive cryptocurrencies and what the sentiment is towards using in their daily lives, based on multiple choice.

5.4.2 Interview

Interviews are an important data collection technique that involves verbal communication between the researcher and the subject (Mathers, Fox & Hunn, 2000). According to Phillips (2016) "interviews are primarily conducted in qualitative research and occur when researchers ask one or more participants general, open-ended questions and record their answers". For this research, a special technological device has been chosen to capture audio which is also enabling borderless transmission between devices while ensuring safe storage (either on the device itself or using the cloud). Interviews are especially useful for revealing the story behind the participants' experiences and seeking detailed information about the topic being researched. (Phillips, 2016). According to some authors, there is a connection between the survey and the interview. Namely, interviews can be useful for monitoring individual respondents after the questionnaire was conducted in order to find out more detailed answers that were not included in the survey (McNamara, 1999). Usually, open-ended questions are asked in the hope that impartial answers will be obtained, while closed-ended questions may force participants to answer in a certain way (Creswell, 2012; McNamara, 1999). Open-ended questions give participants more opportunities to answer and give their opinion on a topic. There are several types of interviews. Therefore, whether they are conducted individually, (i.e., with one person or in groups), can be divided into *individual interviews* and *Group interviews* (Mathers, Fox & Hunn, 2000). According to the way they are implemented, we can divide them into: Face to face, Telephone, and Video, Web interview (Mathers, Fox & Hunn, 2000).

For the purposes of this master thesis, three interviews were conducted. The first interview was individual while the other two interviewees gave the interview as part of a group of two. All three interviews were conducted via Video Call using Zoom whereby the audio was recorded on a mobile recording device.

The first person interviewed on the 6th of January 2021 was H.H. Mr. H.H. was part of the traditional ecosystem until H.H. stumbled upon Blockchain. After understanding how technologically profound Bitcoin is in its simplicity, H.H. saw a potentially disruptive business model which can be used even beyond Bitcoin. Today, H.H. is heavily engaged in the Blockchain industry at the heart of Crypto Valley. Mr H. is working on a daily basis with financial institutions, unicorn companies, policy makers, universities, and banks which already have or want to obtain a banking license.

The duration of the interview was 32 minutes. The interview began with the request to approve the recording of the interview and notice that it will be solely used for carefully conducted academic research on Modul University Vienna.

The second two interviews conducted on the 12th of January 2021 involved T.T. and N.R. Both interview partners are part of the Crypto Valley community-based in Switzerland and have been

involved in Blockchain from its nascent stage. Being familiar with DeFi and working with institutions on a day-to-day basis, the objective was to obtain a complete picture when it comes to institutional and general adoption of DeFi.

T.T. (Co-Head of CVVC) is developing corporate and institutional partnerships with Crypto Valley VC. Before joining CV VC, her presence was within the United Nations, Heroes Group Switzerland and as Co-host at decentra.live, an online news show focused on Blockchain.

N.R. (Co-Head of CVVC) is building up the Blockchain incubation program at CV Labs, and scouts high-quality startups for Europe's largest Blockchain startup contest, the CV Competition. N.R. is also a mentor at the Blockchain Xcelerator at Berkeley University.

The duration of the interview was 37 minutes. The interview began with the request to approve the recording of the interview and notice that it will be solely used for carefully conducted academic research on Modul University Vienna.

6 RESULTS AND DISCUSSIONS

This chapter analyzes the results obtained through the questionnaire and interviews. The results were processed using SPSS. The aim of the survey was to find out whether the respondents are familiar with Blockchain technology, cryptocurrencies, decentralized finance, as well as whether and to what extent they think about DeFi. To get a clearer picture, 3 industry experts have been chosen for an interview.

6.1 Questionnaire

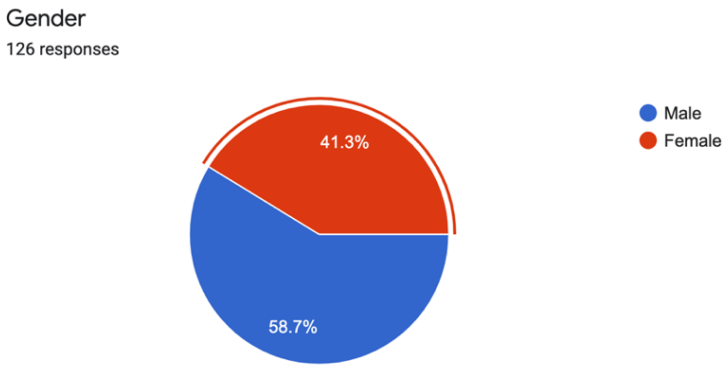


Figure 9. Survey question 1. “Gender”

Figure 9 refers to the gender of the respondents. Out of a total of 124 respondents, 73 were male (58.9%), 51 female (41.1%).

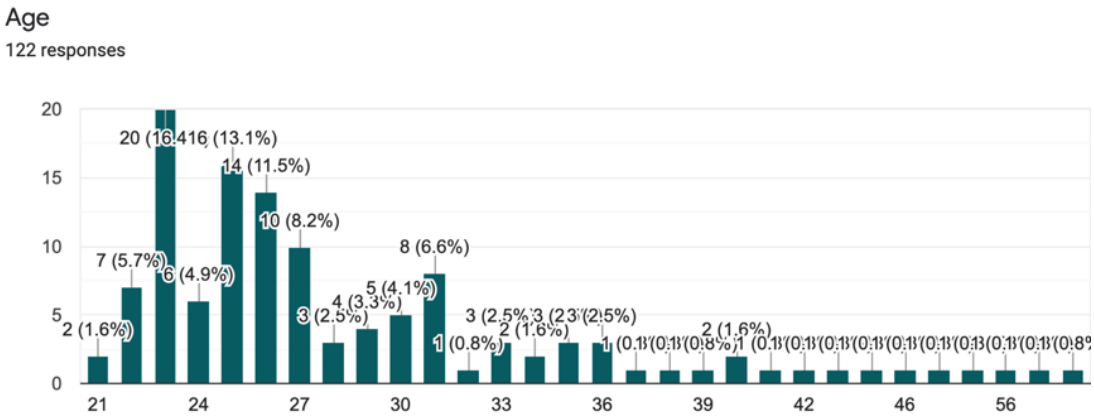


Figure 10. Survey question 2. “Age”

Figure 10 shows that most respondents who completed the survey were 23 years old (n = 20), 16.1% of them. 15 respondents were 25 years old (12.1%) and 14 respondents were 26 years old (11.3%). 14.6% of respondents were aged between 22 and 27 (n = 9).

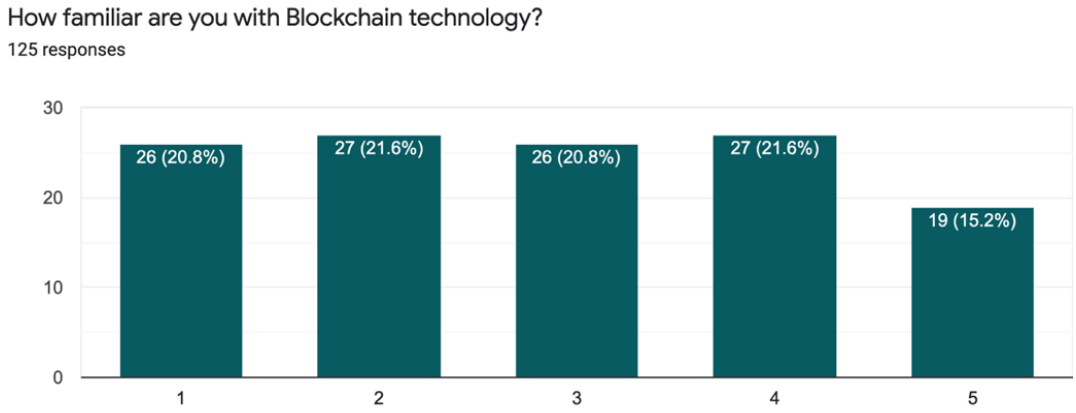


Figure 11. Survey question 4. "Familiarity with Blockchain technology" - Likert scale

Figure 11 shows that out of the total number of respondents (n = 124), 28 of them were not at all familiar with the concept of Blockchain technology (22.6%), 27 were slightly familiar (21.8%), 24 were somewhat familiar (19.4%), 26 were moderately familiar (21%), while only 18 believe to be very familiar (14.5%).

Questions 5-11 were formed according to the UTAUT2 model on a multiple-choice basis (Venkatesh et al, 2012):

The 5th question based on UTAUT2 was about *Performance expectancy.* The offered answers were:

- Using cryptocurrencies will help me achieve my financial goals completely
- Using cryptocurrencies will help me achieve my financial goals faster
- Using cryptocurrencies will increase my standard of living
- Using cryptocurrencies will not change my life in any aspect

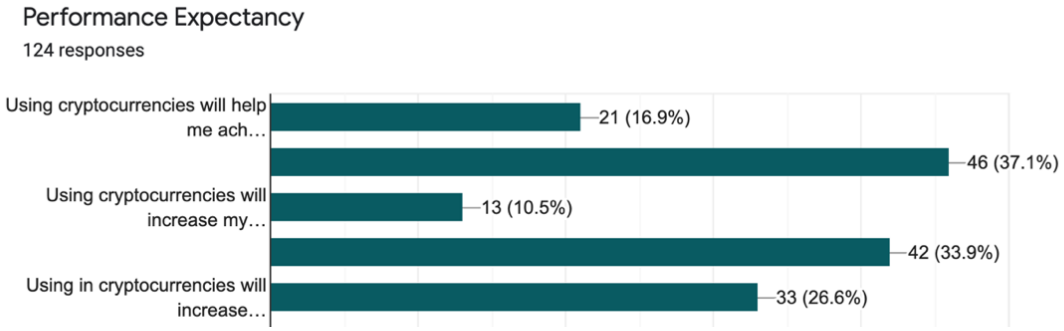


Figure 12. Survey question 5. "Performance expectancy" - Likert scale

Figure 12 refers to the first answer in the 5th Survey question „Using cryptocurrencies will help me achieve my financial goals completely“. It was marked by 21 people (17.6%). The second answer „Using cryptocurrencies will help me achieve my financial goals faster“ was marked by 44 people (37%). The third answer „Using cryptocurrencies will increase my standard of living“ was marked by 12 people (10,1%). The fourth answer „Using cryptocurrencies will not change my life in any aspect“ was marked by 42 people (35,3%).

Based on the results, it can be concluded that most respondents believe that the use of cryptocurrencies will enable them to achieve their financial goals faster. A similar percentage of respondents believe that cryptocurrencies will not change their lives in any aspect.

The 6th question based on UTAUT2 was about *Effort expectancy*. The offered answers were:

- I easily learned to invest in cryptocurrencies (14,6%)
- Using cryptocurrencies is clear and understandable to me (27,6%)
- It will be easy for me to become an expert in using cryptocurrencies in a while (37,4%)
- Using cryptocurrencies is extremely difficult for me (27,6%)

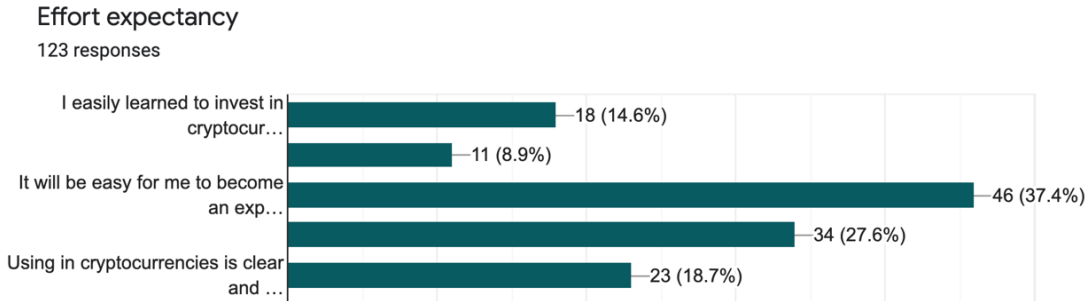


Figure 13. Survey question 6. „Effort Expectancy“ – multiple-choice

Figure 13 shows that the first answer in the 6th Survey question „I easily learned to invest in cryptocurrencies“ was marked by 18 people (14,6%). The second answer „Using cryptocurrencies is clear and understandable to me“ was marked by 34 people (27,6%). The third answer „It will be easy for me to become an expert in using cryptocurrencies in a while“ was marked by 46 people (37,4%). The fourth answer „Using cryptocurrencies is extremely difficult for me“ was marked by 34 people (27,6%). Based on the obtained results, we can conclude that most respondents (37,4%) believe that it will be easy for them to become an expert in using cryptocurrencies in a while.

The 7th question based on UTAUT2 was about *Social influence*. The offered answers were:

- My family believes that I should use cryptocurrencies
- My friends believe that I should use cryptocurrencies
- People whose opinions I value encourage me to use in cryptocurrencies
- People whose opinions I care about discourage me to use cryptocurrencies

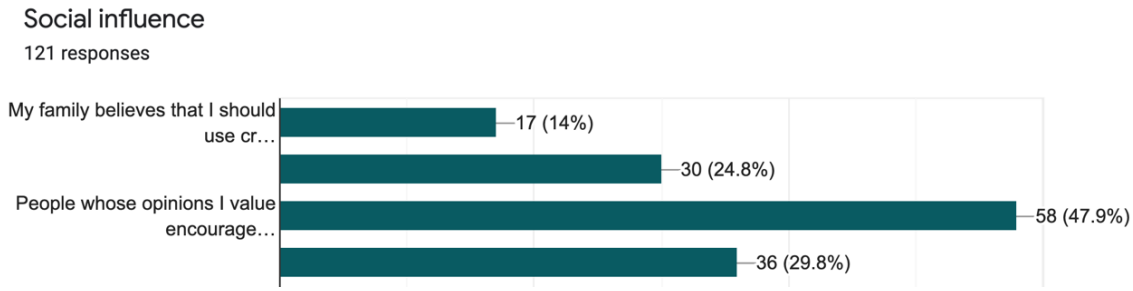


Figure 14. Survey question 7. „Social influence“ – multiple-choice

Figure 14 shows that the first answer in the 7th Survey question „My family believes that I should use cryptocurrencies“ was marked by 18 people (13%). The second answer „My friends believe that I should use cryptocurrencies” was marked by 30 people (21,7%). The third answer “People whose opinions I value encourage me to use in cryptocurrencies” was marked by 55 people (39,9%). The fourth answer „People whose opinions I care about discourage me to use crypto-currencies“ was marked by 35 people (25,4%). Based on the analysis of the 7th question from the survey, it can be concluded that the friends of the majority of respondents believe that they should use cryptocurrencies.

The 8th question based on UTAUT2 was about *Facilitating conditions*. The offered answers were:

- I have the necessary computer hardware/software to use cryptocurrencies
- I have all the necessary knowledge to use cryptocurrencies
- Using cryptocurrencies feels similar to making other online investments (stocks, bonds,...)
- I don't have all the necessary resources and knowledge to invest in cryptocurrencies

Figure 15. Survey question 8. „Facilitating conditions“ – multiple-choice

Figure 15 shows that the first answer in the 8th Survey question „I have the necessary computer hardware/software to use cryptocurrencies“ was marked by 50 people (29,2%). The second answer „I have all the necessary knowledge to use cryptocurrencies”' was marked by 34 people (19,9%). The third answer „Using cryptocurrencies feels similar to making other online investments (stocks, bonds,...)“ was marked by 40 people (23,4%). The fourth answer „I don't have all the necessary resources and knowledge to invest in cryptocurrencies“ was marked by 47 people (27,5%).

Based on the analysis of the 8th question from the survey, it can be concluded that there is a gap between respondents having the technical resources and knowledge, and respondents not having the necessary technical resources and knowledge. The majority of the respondents having the necessary resources and knowledge have used cryptocurrencies and a vast majority associates the usage of cryptocurrencies with established traditional investing.

The 9th question based on UTAUT2 was about *Hedonic motivation*. The offered answers were:

- Using cryptocurrencies helps getting business done more easily
- Using cryptocurrencies makes me happy because I am improving my technological knowledge
- Using cryptocurrencies can increase my income
- Using cryptocurrencies cannot change anything in my life

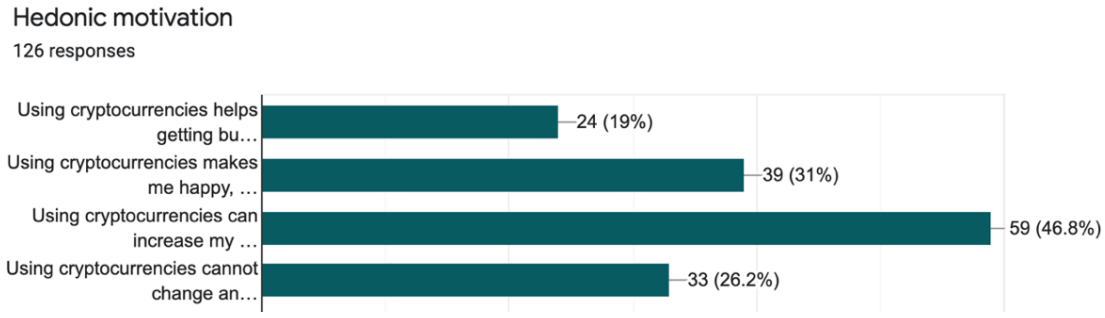


Figure 16. Survey question 9. „Hedonic motivation“ – multiple-choice

Figure 16 shows that the first answer in the 9th Survey question „Using cryptocurrencies helps getting business done more easily“ was marked by 24 people (15,9%). The second answer „Using cryptocurrencies makes me happy, because I am improving my technological knowledge“ was marked by 39 people (25,8%). The third answer „Using cryptocurrencies can increase my income“ was marked by 55 people (36,4%). The fourth answer „Using cryptocurrencies cannot change anything in my life“ was marked by 33 people (21,9%).

Based on the analysis of the 9th question from the survey, it can be concluded that more than half of the respondents think that cryptocurrencies can increase their income.

The 10th question based on UTAUT2 was about *Price value*. The offered answers were:

- Using cryptocurrencies (can) increase my costs and expenses
- Using cryptocurrencies does not increase my costs and expenses
- Using cryptocurrencies (can) increase my income
- I do not (plan to) use cryptocurrencies

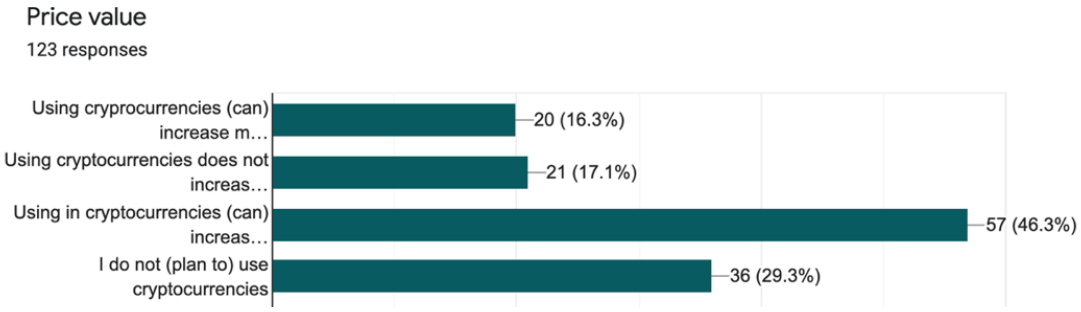


Figure 17. Survey question 10. „Price value“ – multiple-choice

Figure 17 shows that the first answer in the 10th Survey question „Using cryptocurrencies (can) increase my costs and expenses" was marked by 20 people (15,2%). The second answer „Using cryptocurrencies does not increase my costs and expenses" was marked by 21 people (15,9%). The third answer „Using cryptocurrencies (can) increase my income" was marked by 55 people (41,7%). The fourth answer „I do not (plan to) use cryptocurrencies" was marked by 36 people (27,3%).

Based on the analysis of the 10th question from the survey, it can be concluded that more than half of the respondents (n=55) think that cryptocurrencies can increase their income.

The 11th question was about Habit. The offered answers were:

- Using cryptocurrencies makes doing business easier and more convenient
- I check the price of cryptocurrencies on a regular basis
- Using cryptocurrencies does not affect my life in any way

Figure 18. Survey question 11. „Habit“ – multiple-choice

In Figure 18, the first answer in the 11th Survey question „Using cryptocurrencies makes doing business easier and more convenient“ was marked by 36 people (27,7%). The second answer „I check the price of cryptocurrencies on a regular basis“ was marked by 50 people (38,5%). The third answer „Using cryptocurrencies does not affect my life in any way“ was marked by 44 people (33,8%).

Based on the analysis of the 11th question from the survey, it can be concluded that about half of the respondents (n=50) check the price of cryptocurrencies on a regular basis.

Questions 12, 13, and 14 are modelled using adapted questions from an official OECD research on Cryptoassets using the unified theory of acceptance and use of technology (UTAUT) model.

Figure 19 refers to the 12th question from the survey refers to the activities that respondents would undertake in the next 2 years regarding the use of cryptocurrencies. The offered answers were:

- Buy (more) cryptocurrencies
- Save cryptocurrencies
- Sell (spend) cryptocurrencies
- I don't (plan to) use cryptocurrencies

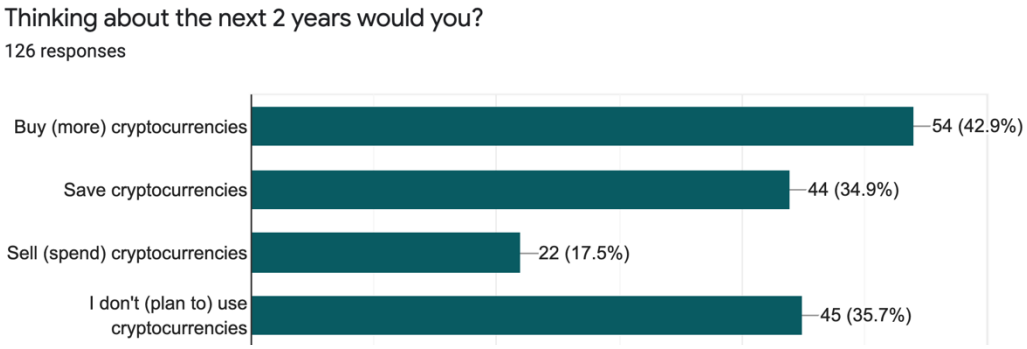


Figure 19. Survey question 12. „Thinking about the next 2 years would you?“ – multiple-choice

The first answer in the 12th Survey question „Buy (more) cryptocurrencies“ was marked by 53 people (32,7%). The second answer „Save cryptocurrencies“ was marked by 43 people (26,5%). The third answer „Sell (spend) cryptocurrencies” was marked by 22 people (41,7%). The fourth answer „I do not (plan to) use cryptocurrencies” was marked by 44 people (27,2 %).

Based on the analysis of the 12th question from the survey, it can be concluded that about half of the respondents (n=53) would buy cryptocurrencies in the next 2 years.

The 13th question from the survey refers to the thesis of whether cryptocurrencies can be easily converted into cash. The answers were presented through the Likert scale offering 5 options to choose from:

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

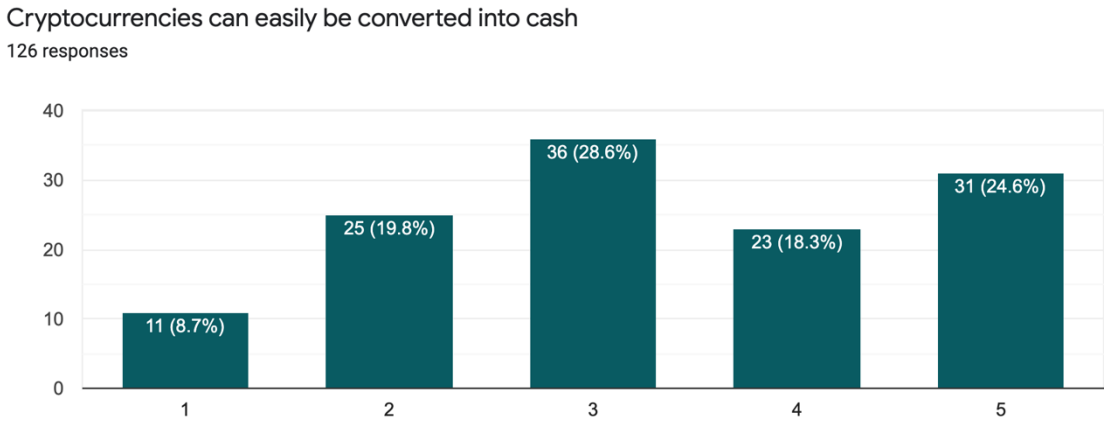


Figure 20. Survey question 13. „Cryptocurrencies can easily be converted into cash“

As visible in Figure 20, out of the total number of respondents (n = 124), 11 of them strongly disagree that cryptocurrencies can easily be converted into cash (8,9%), 25 somewhat disagree (20,2%), 34 neither agree nor disagree (29%), 23 somewhat agree (18,5%), and 29 strongly agree with it (23,4%). Based on the analysis of the 13th question, it can be concluded that the majority of respondents were undecided or indifferent.

The 13th question from the survey refers to the thesis of whether cryptocurrencies can be easily converted into cash. The answers were presented through the Likert scale offering 5 options:

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

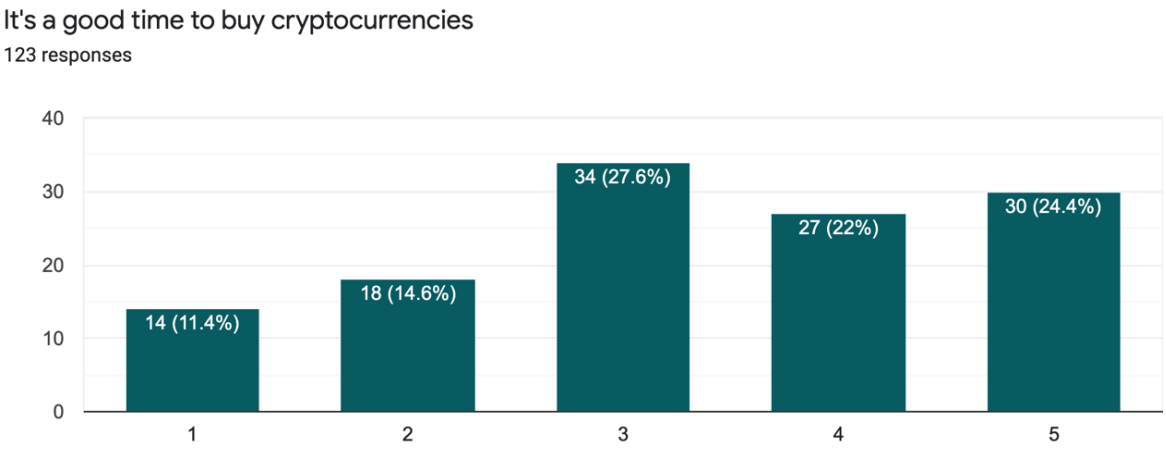


Figure 21. Survey question 14. „It's a good time to buy cryptocurrencies"

As seen in Figure 29, out of the total number of respondents (n = 124), 15 of them strongly disagree about the fact that it's a good time to buy cryptocurrencies (12,1%), 17 somewhat disagree (13,7%), 34 neither agree nor disagree (27,4%), 26 somewhat agree (21%), and 30 strongly agree (24,2%). Based on the analysis of the 14th question, it can be concluded that the majority of respondents were undecided or indifferent.

The 15th question of the survey refers to the respondent's opinion on whether to adopt or resist cryptocurrency issuance by a central bank such as the European Central Bank. The answers were presented through the Likert scale and offered 5 options:

- Resist
- Partially resist
- Neither resits nor adopt
- Partially adopt
- Adopt

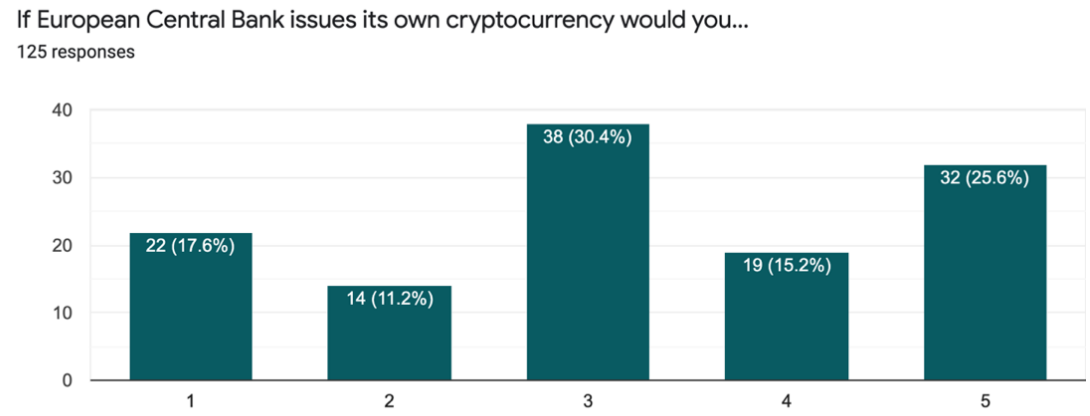


Figure 22. Survey question 15. „If the ECB issues its own cryptocurrency would you?“

As seen in Figure 30, out of the total number of respondents, 23 of them would resist (18,5%), 14 would partially resist (14%), 38 neither resist nor adopt (38%), 19 would partially adopt (15,3%), and 30 would adopt (24,2%). Based on the analysis of the 15th question, it can be concluded that the majority of respondents were undecided or indifferent.

The 16th question in the survey reflects whether the respondents would accept certain activities involving cryptocurrencies:

- Receive a salary in cryptocurrencies
- Borrow money in cryptocurrencies
- Raise capital for a business in cryptocurrencies
- Nothing

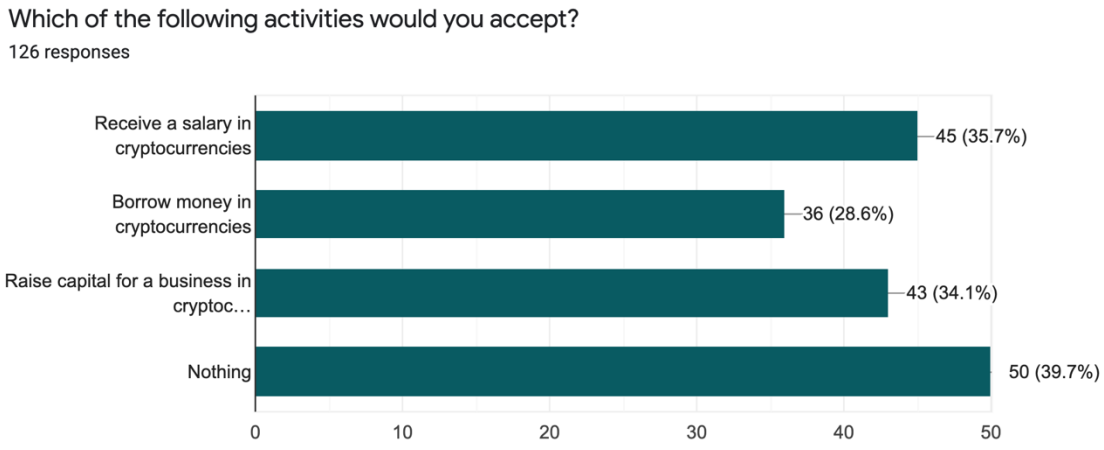


Figure 23. Survey question 16. „Which of the following activities would you accept?“ – multiple-choice

As seen in Figure 23, the first option in the 16th Survey question „Receive a salary in cryptocurrencies“ was marked by 45 people (26,3%). The second option „Borrow money in cryptocurrencies“ was marked by 35 people (20,5%). The third option „Raise capital for a business in cryptocurrencies“ was marked by 41 people (24%). The last option „Nothing“ was marked by 50 people (29,2%).

Based on the analysis of 16th question from the survey, it can be concluded that about half of the respondents (n=50) would not accept any activities related to cryptocurrencies.

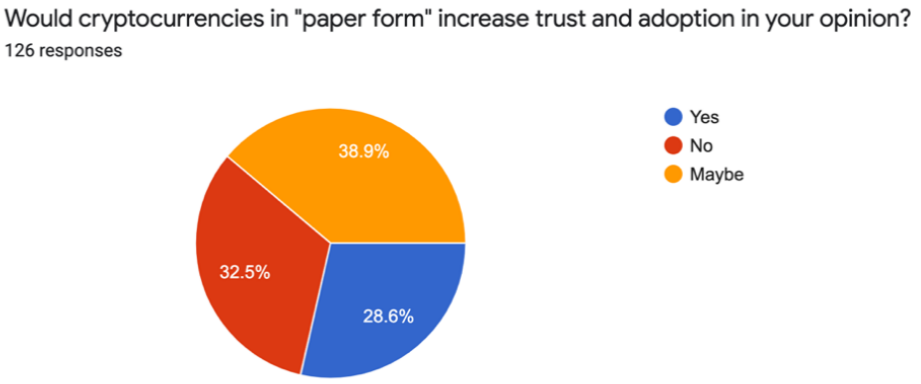


Figure 24. Survey question 17. „Would cryptocurrencies in "paper form" increase trust and adoption in your opinion?“

Figure 24 reflects the answers to the 17th question in our survey showing that 28,2% of respondents (n=35) would accept cryptocurrencies if they were in paper form. 42 of them (33,9%) would not accept, while 47 (37,9%) were undecided. Based on the analysis of the 17th question from the survey, it can be concluded that 37,9% of respondents (n=47) were undecided or indifferent.

As seen in Figure 25, the 18th question from the survey refers to whether the respondents trust centralized financial institutions more than decentralized alternatives. The answers were presented through the Likert scale offering 5 options:

- I do not trust at all
- I somewhat distrust
- Neutral
- I somewhat trust
- I trust completely

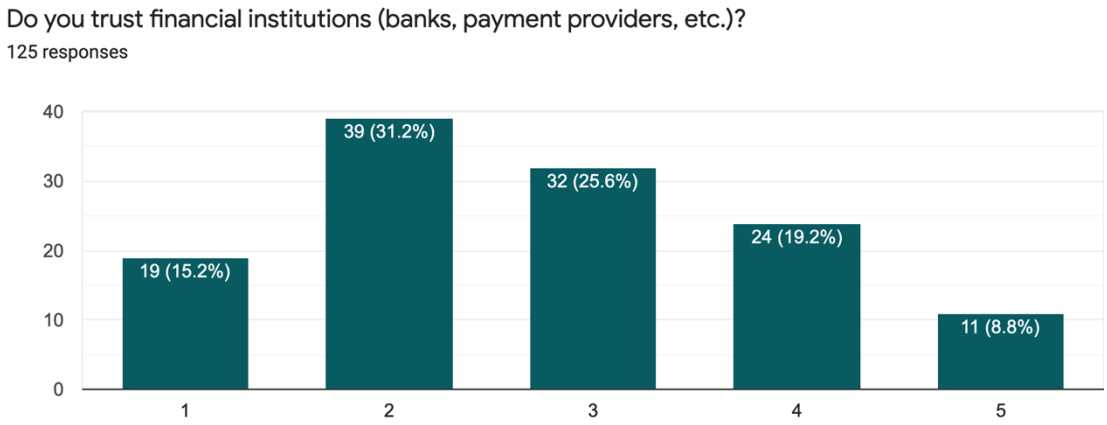


Figure 25. Survey question 18. „Do you trust financial institutions?“

Only one respondent did not answer this question. Out of the total number of respondents, 23 of them would resist (18,5%), 14 would partially resist (14%), 38 neither resist nor adopt (38%), 19 would partially adopt (15,3%), and 30 would not adopt at all (24,2%). Based on the analysis of the 15th question, it can be concluded that the majority of respondents were undecided or indifferent.

As portrayed in Figure 26, the 19th question from the survey refers to whether the respondents are familiar with the concept of decentralized finance (open finance, finance without trust-based institutions). Respondents could choose between "yes", "no", and "maybe".

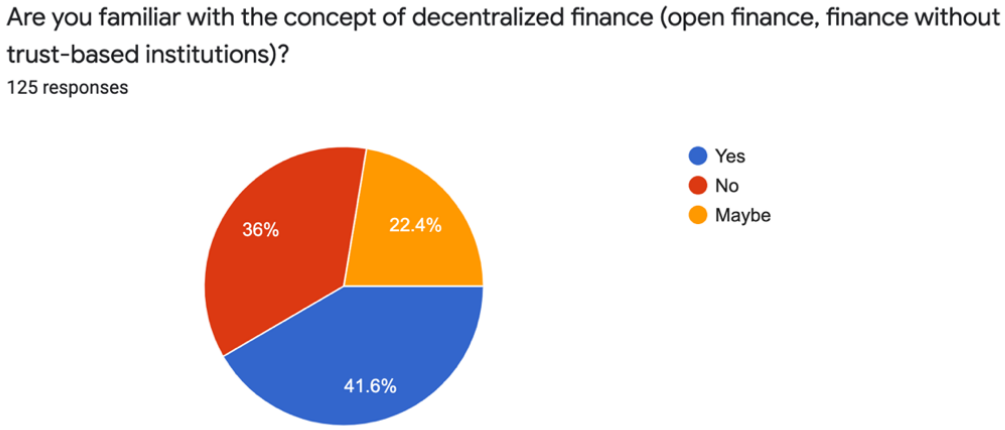


Figure 26. Survey question 19. „Are you familiar with the concept of decentralized finance?“

The Question was not answered by only one respondent. 19 out of the total number of respondents (n = 124) 51 of them (41.1%) state that they are familiar with the concept of decentralized finance, 44 (35.5%) are not familiar, while 28 (22.6%) marked the "maybe" option.

Based on the analysis of the answers from question 19, it can be concluded that most respondents believe to be familiar with the concept of decentralized finance but that cannot be claimed entirely due to the fact that many marked the answer "maybe".

Question under ordinal number 20 refers to the subjective assessment of the respondent's sentiment towards the future of decentralized finance. Using the Likert scale, the question was a comparison between decentralized finance and centralized finance and whether it would be imaginable that decentralized finance would replace banks and trust-based financial institutions. The offered answers were:

- More justice to society
- More democratic society
- More freedom of trade
- More financial privacy
- I cannot imagine a life without a bank

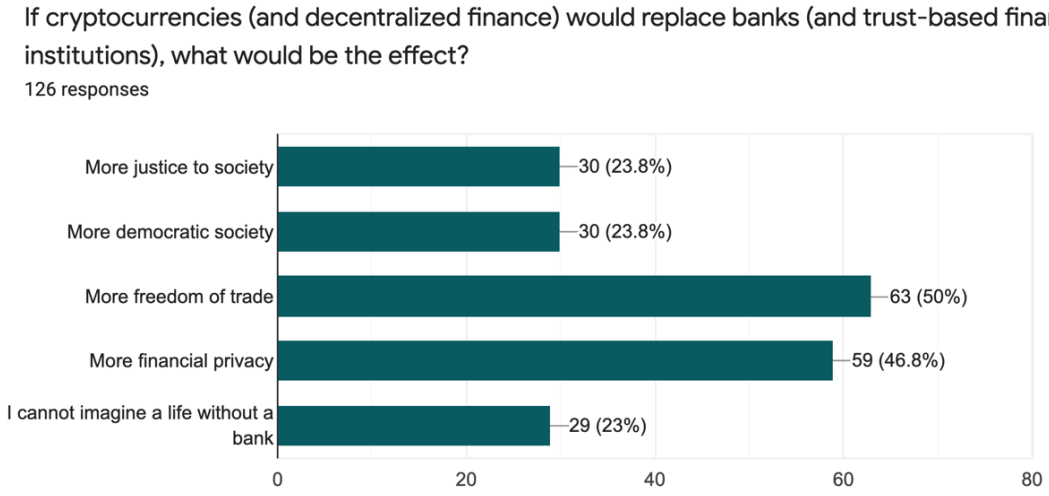


Figure 27. Survey question 20. „If cryptocurrencies (and decentralized finance) would replace banks (and trust-based financial institutions), what would be the effect?„ – multiple choice

As seen in Figure 27, the first answer in the 20th Survey question „More justice to society" was marked by 29 people (14%). The second answer „More democratic society" was marked by 30 people (14,5%). The third answer „More freedom of trade" was marked by 62 people (30%). The fourth answer „More financial privacy" was marked by 57 people (27,5%). The fifth answer „I cannot imagine a life without a bank" was marked by 29 (14%) people.

Based on the analysis of the 20th question from the survey, it can be concluded that most respondents agree that the use of cryptocurrencies and decentralized finance instead of financial institutions would mean more freedom of trade and more financial privacy.

Question 21 relates to financial education. The survey tried to get an insight whether the respondents think that financial education is in the best interest of their bank and their government.

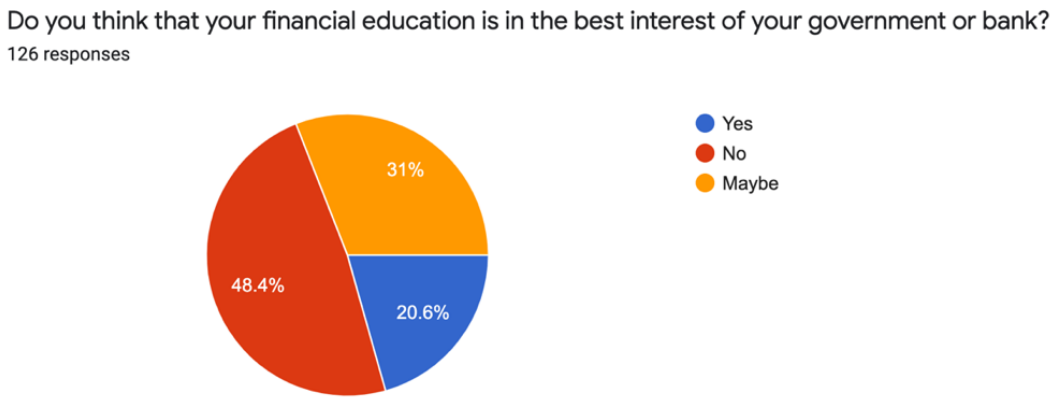


Figure 28. Survey question 21. „Do you think that your financial education is in the best interest of your government or bank?

As seen in Figure 28, the majority of respondents 47.6% (n = 59) believe that financial education is not in the interest of their bank or their government, 25 of them (20.2%) believe that there is interest, while 32.3% (n = 40) indicated the option "maybe". Based on the analysis of the results, it can be concluded that the majority of respondents believe that financial education is not in the best interest of their government and their bank.

Nowadays, cryptocurrencies are increasingly being linked to illegal activities. Based on that, the survey tried to investigate whether the respondents believe that restricting usage of cryptocurrencies is necessary by their government.

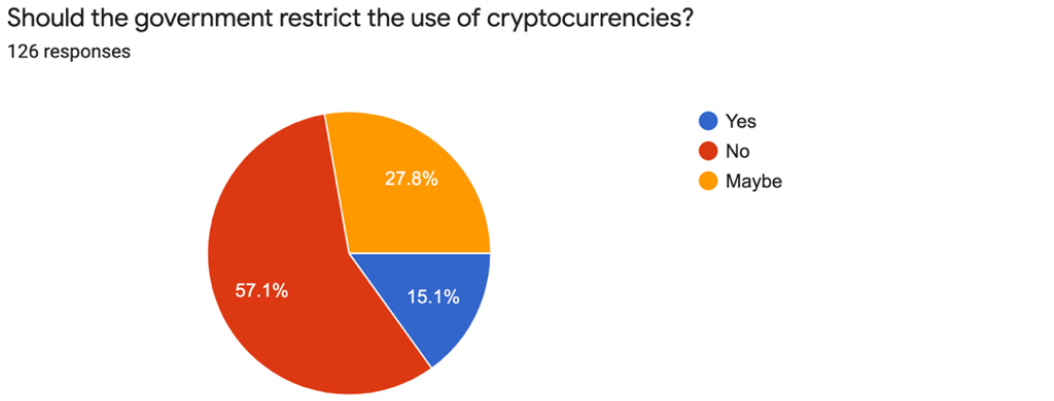


Figure 37. Survey question 22. „Should the government restrict the use of cryptocurrencies?"

As seen in Figure 29, the majority of respondents 56,5% (n = 70) stated that the government should not restrict the use of cryptocurrencies, 19 of them (15,3%) believe that it is necessary to restrict them, while 28,2 % (n = 35) selected the option "maybe". Based on the analysis of the results, it can be concluded that the majority of respondents think that the government should not restrict the use of cryptocurrencies.

The next question from the survey builds on the previous one and refers to the opinion about whether the use of cryptocurrencies would increase cybercrime.

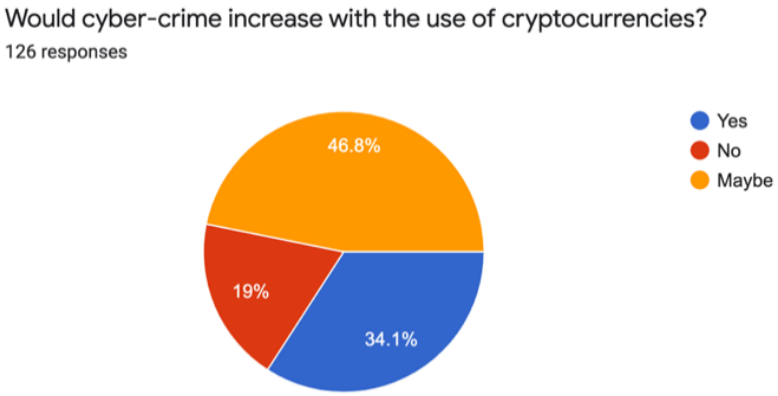


Figure 30. Survey question 23. „Would cyber-crime increase with the use of cryptocurrencies?„

Figure 30 represents the perceived association of cryptocurrencies with cybercrime by respondents. Out of the total number of respondents (n = 124), 44 of them (35.5%) believe that cybercrime would increase with the use of cryptocurrencies, 17.7% (n = 22) believe that this is not the case, while most of them (n = 58) 46.8% marked the option "maybe".

Based on the analysis of the data obtained by the survey, it can be concluded that the majority of respondents are undecided or indifferent.

Question 24 from the survey was asking about the educational aspect and whether the respondents think that it is necessary to include “Basics of cryptocurrencies and the use of Blockchain technology in finance” as a compulsory subject in school or university.

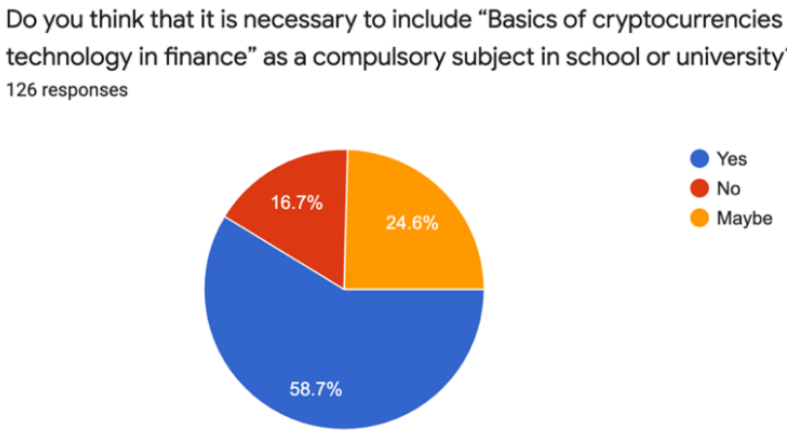


Figure 31. Survey question 24. "Blockchain and cryptocurrencies as a school subject?"

As seen in Figure 31, more than half of the respondents 58.1% (n = 72) believe that this subject should be part of a regular curriculum in schools or universities, 16.9% of them (n = 21) believe that it is not necessary, while 25% (n = 31) are undecided or indifferent.

Based on the analysis of this question, it can be concluded that the majority of respondents believe that it is necessary to include "Basics of cryptocurrencies and the use of Blockchain technology in finance" as a compulsory subject in school or university.

The 25th question in the survey refers to the value aspect of cryptocurrencies (such as bitcoin). The respondents had to choose between 4 different options:

- Worthless
- Digital gold
- Speculative asset
- Money for criminals and terrorists

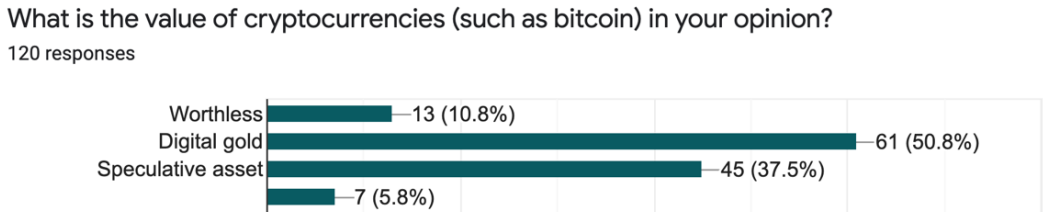


Figure 41. Survey question 25. "What is the value of cryptocurrencies (such as bitcoin)

Figure 41 shows the perceived value of cryptocurrencies by respondents. The first answer in the 25th Survey question stating „Worthless" was marked by 13 respondents (10,5%). The second option „Digital gold" was chosen by 58 respondents (46,8%). The third option „Speculative

asset“ was marked by 45 respondents (36,3%). The fourth answer „Money for criminals and terrorists” was the final answer of 8 respondents (6,5%).

Based on the analysis of 25th questions from the survey, it can be concluded that roughly half of the respondents (n=58) believe that cryptocurrencies (such as bitcoin) are “Digital gold”.

The last question was asking what disturbs them the most when it comes to cryptocurrencies. The offered answers were:

- Missing education
- Uncertainty in regulation
- Too difficult to use
- Opinions of friends and family
- Price fluctuation
- Negative news
- No support from my government

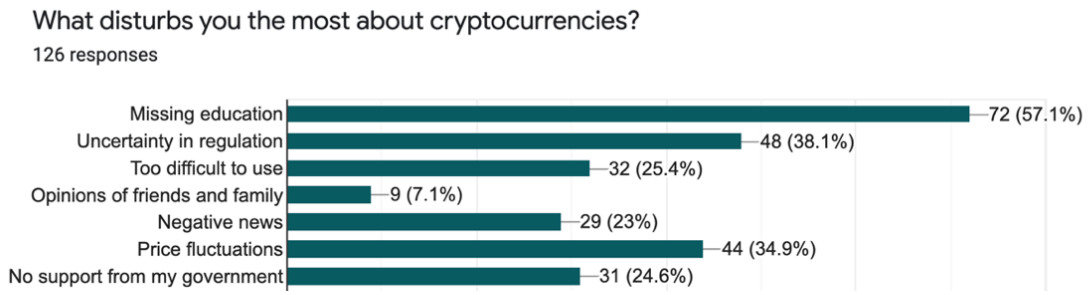


Figure 43. Survey question 26. “What disturbs you the most about cryptocurrencies?“- multiple choice

As seen in Figure 43, the first answer in the 25th Survey question „Missing education“ was marked by 70 people (26,9 %). The second answer „Uncertainty in regulation“ was marked by 46 people (17,7%). The third answer „Too difficult to use“ was marked by 32 people (12,3%). The fourth answer „Opinions of friends and family“ was marked by 9 people (3,5%). The fifth answer „Price fluctuation“ was marked by 43 people (16,5%). The sixth answer „Negative news“ was marked by 32 people (12,3%). The seventh answer „No support from my government“ was marked by 28 people (10,8%). The largest percentage (26,9%) of respondent’s state that the lack of education is what hinders them the most from using cryptocurrencies.

6.2 Hypothesis analysis

H1: Millennials who are familiar with Blockchain technology think cryptocurrencies can easily be converted into cash.

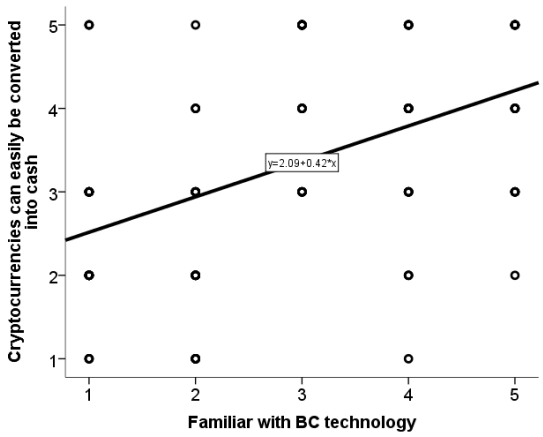


Figure 44. Millennials who are familiar with Blockchain technology think cryptocurrencies can easily be converted into cash (Source: SPSS output)

Result Spearman coefficient:

As seen in Figure 44, the results of the correlation analysis using Spearman coefficient is significant (rho=0,478, p=0,000). In this respect, the results indicate that familiarity with Blockchain technology correlates with the belief that it is easier to convert cryptocurrencies into cash.

Future research significance:

Familiarity with Blockchain technology positively impacts the trust in seamless exchange between cryptocurrencies and cash. One of the major concerns when it comes to cryptocurrencies is convertibility between fiat and cryptocurrencies. Nowadays, centralized exchanges are predominantly used but decentralized exchanges are starting to emerge and gain adoption. Those could amplify adoption of truly decentralized cryptocurrencies, lower the barriers of trust when it comes to store wealth on a decentralized network, similar to a bank. The trust in seamless exchange and knowledge about Blockchain technology could further amplify with the emergence of CBDCs, possibly making the exchange process less bureaucratic. The real impact of implementation and adoption of CBDC's in this aspect could be subject of further research.

Hypothesis 1 (Familiarity with Blockchain : Cryptocurrencies smoothness of exchange) can be **corroborated.**

H2: Millennials who are familiar with Blockchain technology would accept to receive a salary in cryptocurrency

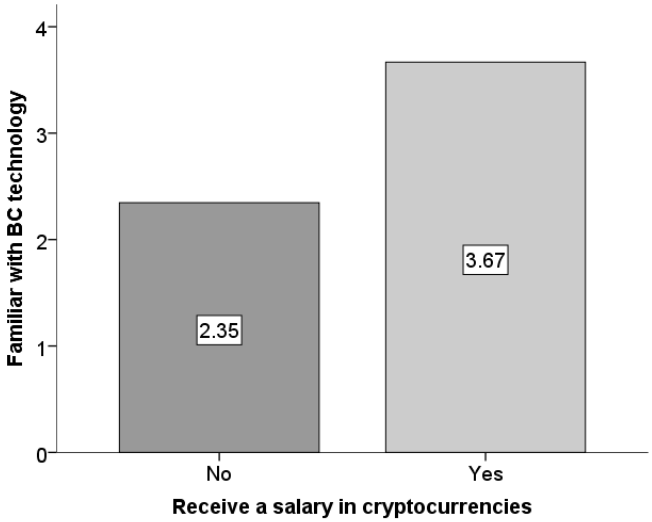


Figure 45. Millennials who are familiar with Blockchain technology would accept to receive a salary in cryptocurrency (Source: SPSS output)

Result:

As seen in Figure 45, the result of the independent samples t test is significant (t=0,572; df=121; p<0,001). In this regard, the familiarity with blockchain has an impact on accepting a salary in cryptocurrencies.

Significance for future research:

With the rising knowledge about Blockchain technology, public and private companies are starting to explore possibilities of integrating cryptocurrencies in their existing payroll process. The trend of receiving a salary in cryptocurrencies could increase in the future as employers get encouraged from regulators. This could indicate that knowledge about Blockchain technology, cryptocurrencies could be regarded as a possible medium of exchange between employers and employees, potentially improving the efficiency of the payroll process. In this research, factors such as regulatory or tax uncertainty have not been covered but with rising adoption of CBDC's, adoption of cryptocurrencies for payroll purposes could significantly increase, without knowledge about Blockchain technology. From an employee perspective, future research could explore further factors of adoption such as psychological perception of stability (or non-volatility) when it comes to accepting a salary in cryptocurrencies.

Hypothesis 2 (Familiarity with Blockchain: Salary acceptance) can be **corroborated.**

H3: Millennials who believe that cryptocurrencies can increase their income would buy more cryptocurrencies in the next 2 years.

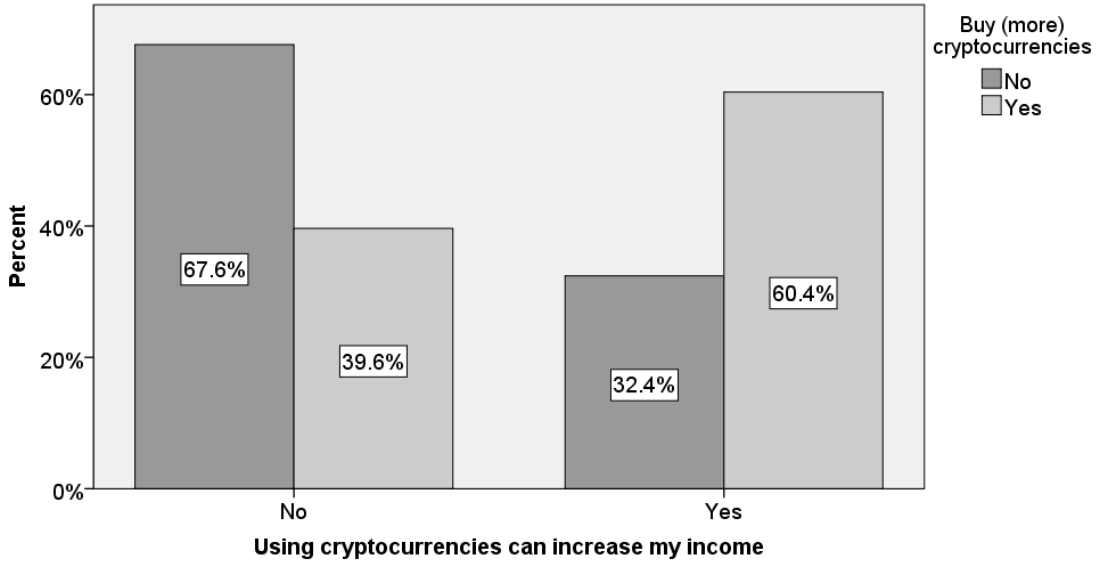


Figure 46. Millennials who believe that cryptocurrencies can increase their income would buy more cryptocurrencies in the next 2 years (Source: SPSS output)

Result:

As seen in Figure 46, the result of the $\chi 2$ test of independence is significant ($\chi 2$=8,528; df=1, p<0,003, phi=0.279). This could indicate that millennials who think that cryptocurrencies can increase their income impacts the desire of buying more cryptocurrencies in the next 2 years.

Significance for future research:

Although millennials generally believe that cryptocurrencies can contribute to an income increase, many still believe that it's best not to buy or invest in the next 2 years. The respondents could be hesitant because of ongoing pandemic and concerns about the current state of the economy. Cryptocurrencies have not been promoted or perceived as a hedge against monetary uncertainty and inflation. Whether uncertainty stems from financial, technological or other factors has not been covered in this research. Future research could focus on how respondents react to economic uncertainty in a global pandemic, how inflation impacts the decision-making ability and what role CBDC's play in wealth creation or preservation.

Hypothesis 3 (Cryptocurrencies can increase income: Willingness to buy) can be **corroborated.**

H4: Millennials who are familiar with DeFi believe that the government should restrict the use of cryptocurrencies.

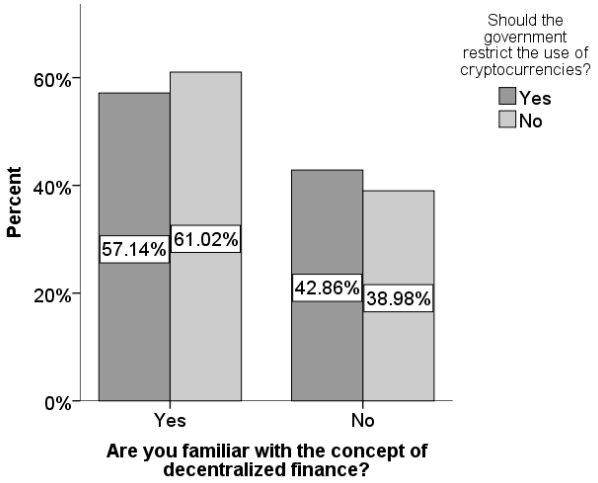


Figure 47. Millennials who are familiar with DeFi believe that the government should restrict the use of cryptocurrencies (Source: SPSS output)

Result:

Relating to Figure 47, the results of the χ2 test is not significant (χ2=1,000; df=1; p<1,000, phi=-0.031). In respect to this, familiarity with the concept of Decentralized Finance does not impact the belief that the government should impose restrictions on cryptocurrencies. Respondents who were undecided or indifferent (group"maybe") have been excluded from the analysis.

Significance for future research:

Although decentralized currencies are on the rise, most respondents could be unsure about the potential of DeFi and how regulation could impact their financial freedom in the long-term. In the upcoming decade the familiarity with Blockchain could improve, resulting in less indifference or indecisiveness. The group "maybe" could be assymetrically informed and this could improve in the future once the population becomes more comfortable in using them daily. The current result could be influenced by confusing regulatory signals of countries that have not shown a clear direction when it comes to adoption of cryptocurrencies. Although some countries support the idea of decentralization of finance, other have announced further restrictions. Such market signals could impact further adoption of decentralized finance by the public which could be covered in further research.

Hypothesis 4 (Familiarity with DeFi : Restriction of cryptocurrencies) can be **rejected.**

H5: Millennials who believe that financial education is in the best interest of their government or bank are more likely to adopt cryptocurrencies issued by the ECB.

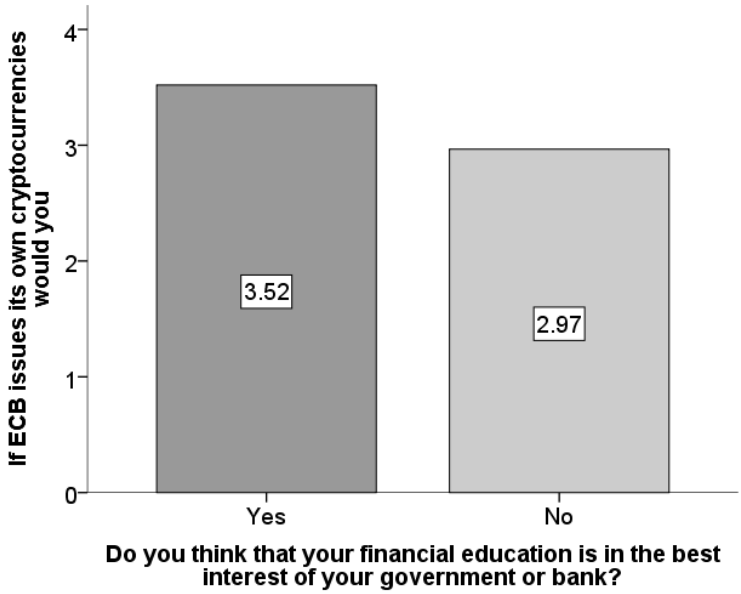


Figure 48. Millennials who believe that financial education is in the best interest of their government or bank would adopt cryptocurrencies issued by the ECB (Source: SPSS output)

Result:

Relating to Figure 48, the result of the t test of independence is not significant (F=1,554; df=81; p<0,124). In respect to this, the perception about financial education from governments and banks does not impact the potential adoption of cryptocurrencies issued by the ECB (such as the digital euro for example).

Significance for future research:

The outcome of the result could be due to the lack of understanding the benefits decentralization of finance brings to society. The trust in fully decentralized or partly centralized currencies is open for further research. Factors that could influence the results could range from difficulties with dealing with bureaucracy, monetary stability, or distrust in formal institutions. Centralized currencies that have been under governmental control and supervision are the standard today, and decentralized currencies could prove to be beneficial in the future. Whether governments or banks are open to provide millennials with better education about Blockchain technology and cryptocurrencies which would improve financial literacy is open for future research.

Hypothesis 5 (Perceived financial education: Adoption of CBDC's) can be **rejected.**

H6: Millennials who trust in financial institutions think that cryptocurrencies are digital gold. (more digits)

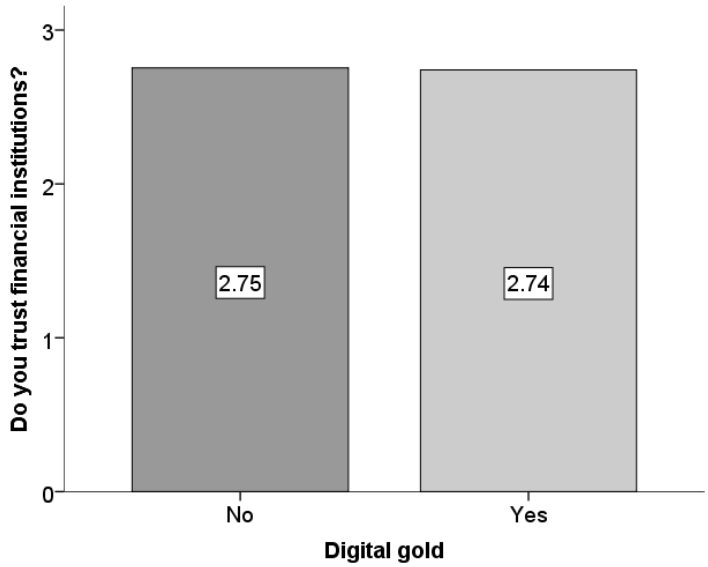


Figure 49. Millennials who trust in financial institutions think that cryptocurrencies are digital gold (Source: SPSS output)

Result:

In Figure 49, the result of the independent samples t test is not significant (t=0,059; df=121; p<0,953). In respect to this, millennials' belief that cryptocurrencies are digital gold is not impacted by trust in financial institutions.

Significance for future research:

Although many financial institutions are starting to acknowledge that cryptocurrencies (such as bitcoin) can be viewed as an asset, many believe that it is rather a speculative tool. And although the negative sentiment around cryptocurrencies is decreasing, many still believe that they have no intrinsic value. Further research could focus on how intrinsic value is perceived and which stakeholders are crucial in defining the term *intrinsic value.* Future research could focus on asset performance during a global pandemic and cover the question whether cryptocurrencies can be perceived as a hedge against uncertainty in difficult economic conditions. In this regard, trust in financial institutions after the economic consequences of the pandemic are known could be analyzed with special emphasis on CBDCs as a hedge against economic uncertainty.

Hypothesis 6 (Trust in financial institutions : Bitcoin as a store of value) can be **rejected.**

H7: Millennials who believe that their financial education is in the best interest of the bank or government think that it is necessary to include “Basics of cryptocurrencies and the use of blockchain technology in finance” as a compulsory subject in school or university.

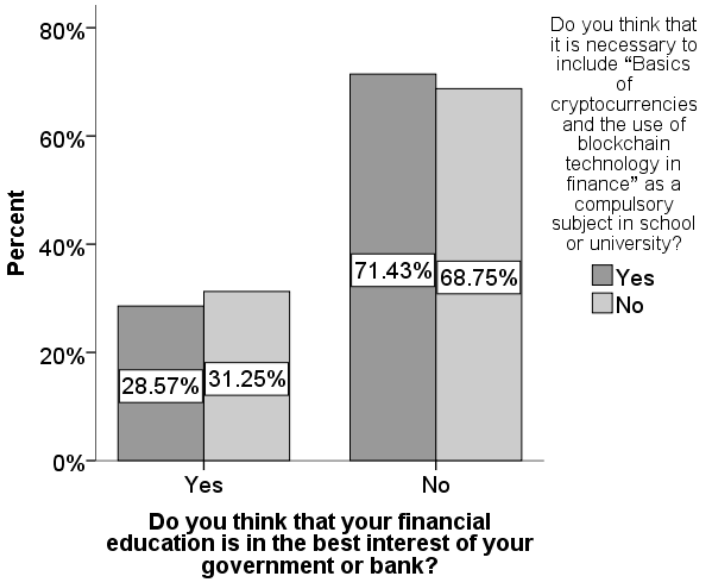


Figure 50. Millennials who believe that their financial education is in the best interest of the bank or government think that it is necessary to include “Basics of cryptocurrencies and the use of blockchain technology in finance” as a compulsory subject in school or university (Source: SPSS output)

Result:

As seen in Figure 50, the result of the χ2 test is not significant (χ2 = 0.000, df=1, p<1.000, Phi= 0.024). Indifferent or indecisive respondents marking the option "maybe" have been excluded from the analysis. In respect to this, the belief that financial education is in the best personal interest does not seem to impact the belief that Blockchain should be a subject taught in school or university.

Significance for future research:

Blockchain in formal education is still not well-established and the benefits of including Blockchain as a subject taught in school or university could be known after more companies, institutions or governments fully adopt and realize the potential in keeping up to date with technological advancements. Future research could focus on general financial literacy after Blockchain becomes more established in formal education.

Hypothesis 7 (Perceived financial education obtained : Blockchain education) can be **rejected.**

H8: Millennials who trust in financial institutions believe that the government should restrict the use of cryptocurrencies.

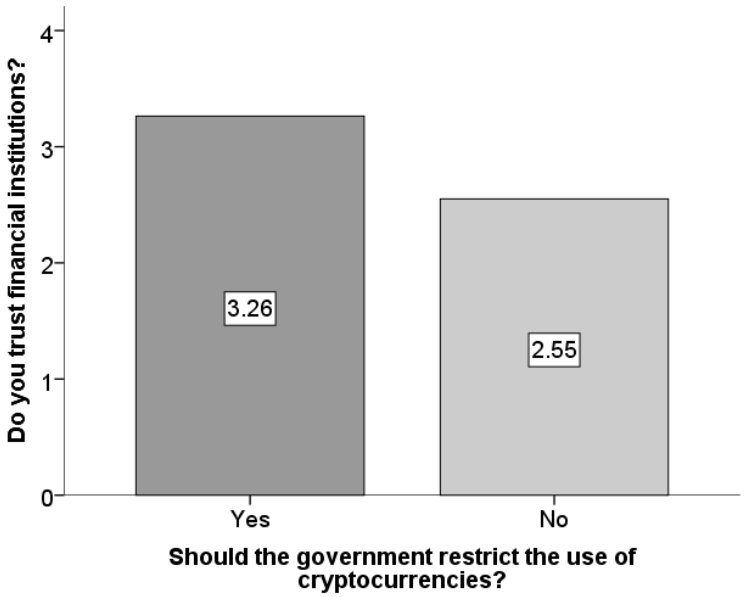


Figure 51. Millennials who trust in financial institutions believe that the government should restrict the use of cryptocurrencies (Source: SPSS output)

Result:

As seen in Figure 51, the result of independent samples t test is significant (M=3,26) (t=2.321; df=86; p<0.023). In this regard, trust in financial institutions positively impacts the belief that the government should restrict the use of cryptocurrencies.

Significance for future research:

Although financial institutions have been providing society with crucial organizational needs, recent economic downturns have negatively impacted the trust in financial institutions. Due to the heavy influence of disinformation, many believe that cryptocurrencies are not compliant with policies such as anti-money-laundering and know-your-customer regulation. Some governments have been restricting the use of cryptocurrencies which could have impacted the sentiment in the public when it comes to their usage and adoption. Further research could show how CBDCs influence the trust in financial institutions and whether the belief towards more restriction when it comes to cryptocurrencies has shifted with increased adoption.

Hypothesis 8 (Restriction of cryptocurrencies : Trust in financial institutions) can be **corroborated.**

H9: Millennials who cannot imagine a life without a bank think that cybercrime is likely to increase with the use of cryptocurrencies

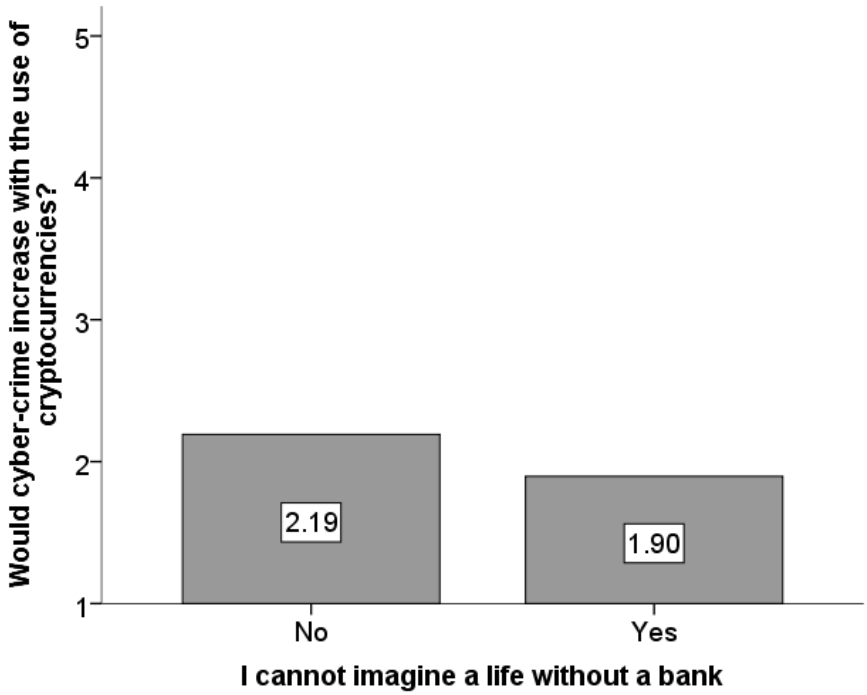


Figure 52. Millennials who cannot imagine a life without a bank think that cybercrime would increase with the use of cryptocurrencies (Source: SPSS output)

Result:

As seen in Figure 52, the independent samples t test is not significant (t=1,549; df=121; p<0,124). In respect to this, millennials who cannot imagine a life without a bank does not contribute to the belief that cyber-crime would increase with the use of cryptocurrencies.

Significance for future research:

Cyber-crime and the perception of using cryptocurrencies for illegal purposes has impacted the effort to improve the regulation of trustworthy technologies. The belief that money has to be held in traditional centralized institutions is one of the factors that could contributing to the fact that some millennials cannot imagine a life without a bank. Further research could investigate whether respondents perceive distributed ledger technologies as a safe haven for their earnings in the future, once the fear of losing funds due to hacking, phishing or quantum-computing dimishes.

Hypothesis 9 (Imagining life without a bank : Belief in cybercrime increase) can be **rejected.**

H10: Millennials who are influenced by negative news think that cryptocurrencies are money for criminal and terrorists.

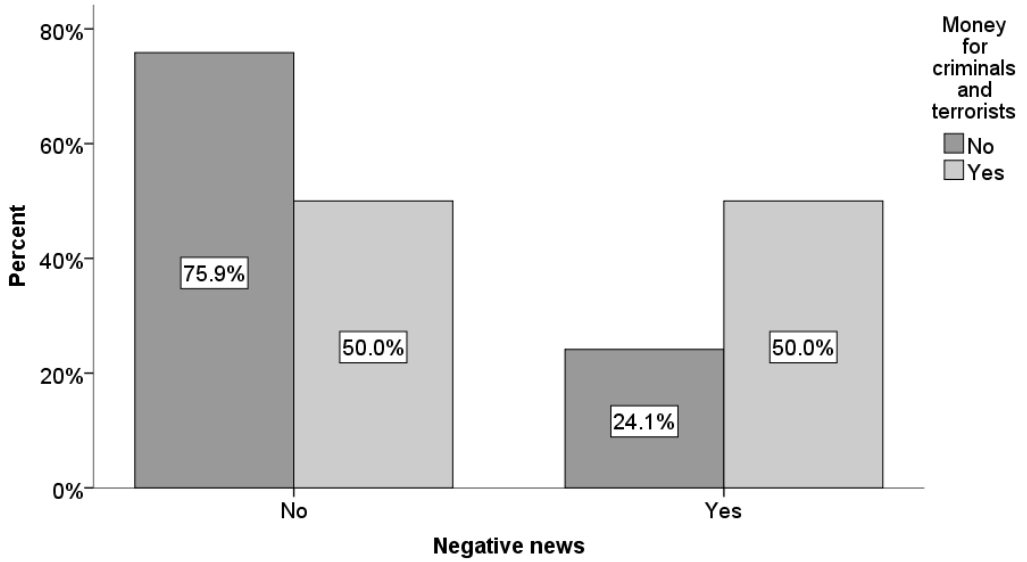


Figure 53. Millennials who are influenced by negative news think that cryptocurrencies are money for criminal and terrorists (Source: SPSS output)

Result:

As seen in Figure 53, the result of $\chi 2$ test is not significant ($\chi 2 = 1.438$, df=1, p=0.230, phi= 0.145). In respect to this, negative news seem to not contribute to the belief that cryptocurrencies are money for criminals and terrorists.

Significance for future research:

News mentioning that cryptocurrencies are used predominantly as a tool for illicit activities has been a widely discussed issue. This trend is likely going to shift in the future once the industry matures and benefits of using cryptocurrencies for non-illicit purposes start to be more apparent. Further research could show that benefits such as immutability, transparency and decentralization amplify the perceived utility of using cryptocurrencies. This could ultimately diminish the belief that cryptocurrencies are money for criminals and terrorists, which is often the notion in mainstream media today.

Hypothesis 10 (Negative news : Usage of cryptocurrencies for illicit activities) can be **rejected.**

6.3 Interview results

6.3.1 First expert interview

H.H. was part of the traditional ecosystem until H.H. stumbled upon Blockchain. After understanding how technologically profound Bitcoin is in its simplicity, H.H. saw a potentially disruptive business model which can be used even beyond Bitcoin. Today, H.H. is heavily engaged in the Blockchain industry at the heart of Crypto Valley. Mr H. is working on a daily basis with financial institutions, unicorn companies, policy makers, universities, and banks which already have or want to obtain a banking license.

What led you to enter the world of Blockchain technology and direct your interests towards it?

I was working in the hedge fund industry and when I learned about Bitcoin, it completely blew my mind. I realized that Blockchain can have applications in the hedge fund industry in terms of providing more transparency, saving costs and optimizing fund structures more efficiently. I really saw that it could be the future of investment funds. In the last 10 years, the regulatory hurdles were quite big, but this is definitely changing now. The investor had the need for more transparency about investments and Blockchain is perfectly suited for that.

Back then, I worked for a big hedge fund in the DACH region, and the company didn't have the appetite at that point to experiment with Blockchain technology and due to high regulatory uncertainty, it was a good decision. But at the same time, if you want to have the first-mover advantage, you need to take risks. After discovering Crypto valley, my visions for the future changed and I wanted to follow my passion.

After I moved to Switzerland, my conclusion was that there is a tremendous gap between traditional finance and Blockchain startups, and I founded the Multichain Asset Managers Association (MAMA Global) which would help build synergies and to nourish the connection between the two ecosystems.

MAMA is about education and on the other is the help with regulatory proposals. We also partner with universities to give lectures to students talking about traditional ways of managing assets and then how to do it on-chain. The greatest joy is educating students so that they can explore different possibilities which the 21st century has to offer and for them to get insights from the industry.

Is there a personal milestone that you're proud of?

Last year we were invited to the world economic forum (WEF) and presented our way of teaching students using an innovative protocol which enables an individual to set-up their own hedge funds. We have received an award for the teaching method, and we plan to educate C-level executives using this approach.

What do you think about DeFi in 5 years?

I'm very excited about the future of DeFi but I don't see a real merge between CeFi and DeFi by definition. What is DeFi? Something on the Blockchain? The point is that it is controlled by someone and that's inherently against the logic and the current definition of decentralized finance.

We must understand that a company is a centralized entity and therefore not DeFi by definition. A company is an entity which is highly regulated, and DeFi means freedom and disintermediation.

What are the main challenges for asset managers when it comes to the adoption of DeFi?

Although the companies would like to use DeFi, they don't want to give away control (especially when it comes to assets under management). This goes against the principles and the current definition of DeFi, where everybody should be in control of their assets, without any counterparty risk. But from all risks, the regulatory risk is the most significant that legacy companies are afraid of. From my experience, regulators love the idea on a personal level, but the regulatory system is not necessarily awarding initiators of disruptive regulation. Big companies are being faced with a lot of regulation and staying compliant is a cost which every business needs to include in their business model. From this perspective, big companies are not that agile as startups since internal systems cannot be changed back and forth without a great increase in cost. The regulatory challenges have almost diminished in Switzerland, and I believe that this will be a big push for DeFi, but we are doing our best to educate and to make CeFi ready for DeFi, as well as the other way around. I believe there is a healthy future for both of them.

6.3.2 Second expert interview

Both interview partners are currently based in Zug, Switzerland working in the most well-known Blockchain incubator in the world – Crypto valley. It counts more than 4.400 Blockchain enthusiasts working in 850 companies including unicorns and smaller startups in December 2020. In addition to the venture capital expertise, CV operates the incubator CV Labs, which has been offering entrepreneurial advisory services, coworking spaces, and consulting in Switzerland, Liechtenstein and soon in the UAE. CV VC is a founding partner of the Swiss Blockchain Federation, a public-private partnership that fosters a standard of excellence for the Blockchain sector and tries to connect corporates with startups.

T.T. (Co- Head, CryptoValley VC) is currently in charge of the corporate and institutional side of CV Labs.

T. holds a BSc in Political science & International relations from University of California, MA in Global economy & Strategy from Yonsei University, and a MA in International affairs from University of St. Gallen. Her career started with the United Nations Organization, researching think-tanks and tech companies in Europe and Asia.

Before joining CV VC, T.T. was a Client relationship and project manager in Heroes Group AG helping businesses develop appropriate enterprise solutions and effective marketing strategies. T.T. was a co-host at decentra.live, an online news show focused on Blockchain related topics.

N.R. (Co- Head of CV VC) helps build up the Blockchain incubation program at CV Labs, and scouts high quality startups for Europe's largest Blockchain startup contest, CV Competition. N.R. holds a Bachelor's degree in International Business Administration with the major in International Entrepreneurship and is a mentor at Blockchain Xcelerator, the newest lab at the Center for Entrepreneurship in the School of Engineering at the University of Berkeley.

When it comes to adoption, how are traditional financial organizations reacting to Blockchain technology and decentralized finance?

N.R.:

We see traditional financial institutions' interest growing year by year. I saw that already in 2017 during a research project within a major Swiss bank. Already at that point banks were researching Blockchain technology and in my opinion it was only a matter of time that others started experimenting as well. The interest is definitely growing and that's why I see a bright future for Blockchain technology. When it comes to decentralized finance, it is hard to predict how financial organizations will end up reacting to it ultimately, but it is not a topic that they could afford ignoring entirely. I believe the market will change towards more decentralization and traditional institutional players will need to adapt. What is certain is that more and more financial institutions will end up adopting in one way or another, now that the regulatory landscape has become clearer.

T.T.:

Regulators have helped with providing guidelines but at the moment it is still too early to predict what it will look like exactly in the end. If we look at the past 10 years, the road was paved with uncertainty in the digital asset space. Many organizations have been dismissing Blockchain and digital assets altogether, although benefits have been known for years, but this is changing as more and more systematically relevant financial institutions are embracing it without being too open about it. This spike in institutional adoption wouldn't be the case if people wouldn't see a genuine store of value in bitcoin in my opinion. The adoption aspect was an important milestone and also a contributing factor as to why traditional financial institutions are taking this topic more seriously. They have realized that they need to be open for innovation and to embrace technological changes in order to stay relevant. The past economic struggles are a sign, and I believe that not only the average consumer but also financial institutions should realize that something needs to change for a better future. And I believe that Blockchain, digital assets, and decentralized finance should definitely be part of a healthy, sustainable, fully-functioning financial system in the new economy.

7 CONCLUSION

7.1 First research question

The first research question is about the extent to which cryptocurrencies have been adopted by millennials.

First, a thorough review of the available literature is presented. In order to gain more significant insights into the research question, an anonymous questionnaire was conducted on 124 randomly selected participants. Using this approach, we obtained an answer to the question of whether millennials use cryptocurrencies in their daily lives, what is their opinion about cryptocurrencies in general, their trust spectrum and whether cryptocurrencies fit in their financial picture for the next ten years.

Out of a total of 124 respondents, 73 were male and 51 female. To find out to what extent millennials have accepted cryptocurrencies, we first asked them about their subjective perception of whether they are familiar with Blockchain technology. Of the total number of respondents, 22.6% are not familiar with the term, 14.5% are largely familiar, and the rest are partially familiar. Almost a third of respondents believe that the use of cryptocurrencies will help them achieve their financial goals faster, while 42 of them believe that cryptocurrencies do not affect their lives in any manner. Almost half of the respondents think that they would easily master the use of cryptocurrencies, and people whose opinion they care about think that they should invest in cryptocurrencies. Almost a third of the total number of respondents believe that with the help of cryptocurrencies, they could increase their monthly income, and would check the value of cryptocurrencies on a daily basis. In the next two years, half of the respondents plan to buy more cryptocurrencies. A large number of respondents believe that cryptocurrencies can be easily converted into regular money and that now is the right time to buy cryptocurrencies.

If the ECB would issue a cryptocurrency, a large number of respondents would accept it, and even a large number of them would accept to receive a salary in cryptocurrencies. The research has shown that the respondents don't trust financial institutions and 41% are familiar with the term "decentralized finance". Many believe that DeFi and cryptocurrencies contribute to greater freedom and potentially provide more financial privacy. It is interesting to note that the majority is convinced that financial education and know-how about Blockchain technology is important but at the same time, most believe that the state and banks have no interest in educating citizens and improving their financial literacy overall. Many believe that Blockchain and cryptocurrencies know-how should be part of formal education. More than half of the respondents believe that governments should not restrict the use of cryptocurrencies but at the same time more than half believe that cyber-crime would increase with the use of cryptocurrencies. The

most widely impactful question is about the value of cryptocurrencies (such as bitcoin), where the majority stated that they believe it's *digital gold* and an instrument for speculation as well. What prevents the majority from using cryptocurrencies is insufficient education or lack thereof.

7.2 Second research question

The second research question relates to whether the phenomenon and adoption of cryptocurrencies leads to greater decentralization of finance and whether it has a future in our existing micro- and macroeconomic system. With the appropriate use of research methods, analysis of existing literature, as well as interviews with three professionals from the industry, we obtained an answer to the research question. The research question focuses primarily on the advantages and disadvantages of DeFi and its disruptive potential.

The first interview was conducted with Mr. H.H., who until the advent of Blockchain technology was working in the traditional financial industry. Mr. H.H. believes that the emergence of Blockchain in the financial industry is here to stay and that interest about DeFi within legacy institutions is increasing year after year. However, a merge of DeFi and CeFi is unlikely, at least in the short term, because changing existing databases is a long-term decision and must be carefully thought over. In his opinion, certain companies and financial institutions are still sceptical about DeFi. Although they all want to use some aspects of DeFi, they do not want to give up control entirely. What is quite certain is that companies are careful when it comes to acceptance of DeFi in the traditional space, mainly because of regulatory uncertainty in the past. N.R. believes education is key for mainstream adoption of Blockchain technology and believes that in the future, with the appropriate legal framework, there is a sustainable future for both DeFi and CeFi.

The other two interviews were conducted with T.T. and N.R. What we were most interested in was how traditional financial organizations react to Blockchain technology and DeFi. According to Mr. N.R., the interest of traditional financial institutions in DeFi is growing year after year. N.R. noticed that already in 2017 while being involved in a research project of a major Swiss bank. N.R. noticed that banks were already researching Blockchain technology at that time, and that it was only a matter of time before it would be applied in practice. Interest is growing among institutional stakeholders and that is why N.R. foresees a bright future for industry applications of Blockchain technology. When it comes to DeFi, N.R. states that it is too difficult to predict how financial organizations will eventually react to this new business model phenomenon. N.R. believes that the market will change towards greater decentralization on one hand but that legacy institutions will have difficulties building bridges without proper know-how. What is certain is that more and more financial institutions will eventually have to embrace DeFi in one way or another.

On the other hand, T.T. reflected on the past 10 years, and states that the road has been paved with uncertainty when it comes to cryptocurrencies and digital assets. This made many organizations reject Blockchain and digital assets altogether, although benefits have been known for years. T.T.believes that it's difficult for bigger systemically relevant financial institutions to embrace Blockchain because it brings change and uncertainty. That's why many legacy institutions have been hesitant in the past to announce publicly that they have been experimenting with Blockchain technology and be open about it without a clear direction of policy makers. T.T. believes that that the current leap in institutional adoption would not be the case if, in her opinion, people would not see the benefits and some value in bitcoin. This acceptance of the public was an important milestone and also a factor that contributed to why legacy financial institutions take this topic now more seriously. They realized that they must be open to innovation and embrace technological change in order to be prepared for a more decentralized, trustless, transparent future. Past economic struggles are a sign that it's not only in the average consumers' but also financial institution's interest that we have a reliable future-proof economic system based on delivering value to the people. T.T. also believes that Blockchain, cryptocurrencies and DeFi should definitely be part of a healthy, sustainable, fully functional financial system in the new economy.

7.3 Third research question

Although fiat currencies have been used in the past and today to finance illicit activities, the question arises; "Can cryptocurrencies be a more modern way of financing illicit or illegal activities?"

The emergence of the internet has led to a new form of crime commonly known as online crime or cybercrime. Companies and governments have dedicated efforts towards a higher level of cybersecurity but as security changes, the methods and behavioral patterns of criminals change as well. Their activities have become more sophisticated, and many have realized that there are benefits to using cryptocurrencies. The emergence and development of Blockchain technology have created great opportunities for the expansion of cybercrime. The FBI reports reveal that criminals generally try to keep up with the latest trends when it comes to achieving their goals. This is especially evident with the emergence of cryptocurrencies as means of payment. Cryptocurrencies have been used for money laundering, finance terrorism and engage in other criminal activities in the past decade to a certain degree.

Most of the respondents from the survey conducted for the purposes of this master thesis believe that criminal activities have increased with the increasing adoption of cryptocurrencies. Although, they have the opinion that state governments should not limit or prohibit their use. This attitude could be the consequence of the media chase on cryptocurrencies and Blockchain technology in general. Criminal activities involving cryptocurrencies amount to only 1% shown by the FBI report from 2018 and which is negligible in relation to the figures mentioned in the

media.
In any case, the use of cryptocurrencies should be placed in the legal framework in order to reduce the level of illegal activities to a minimum.

7.4 General conclusion

In recent years, we have witnessed various types of changes that have taken place in the financial industry. From year to year, creative destructions bring technological innovations that change our lives and our economy. One of these changes was the advent of Blockchain technology with the emergence of Bitcoin. Cryptocurrencies are generally designed for enabling peer-to-peer transactions without intermediaries such as banks or any other third-party trusted intermediary. They are completely digital, and their robustness is based on cryptography. Bitcoin specifically is a network that hasn't been hacked or made otherwise vulnerable since its inception. The role of other cryptocurrencies is increasing as more, and projects get public acceptance in the form of adoption year after year. Blockchain technology has surpassed the framework of economics and finance and is fortifying its presence in all sectors where trust plays a role. Undoubtedly, it will play a significant role in increasing the efficiency of almost all public institutions, corporations and small businesses.

Recently, inspired by international sanctions, bans, bureaucracy and a growing desire for free trade, Decentralized Finance emerged. It brought inclusivity for the un- or underprivileged, free trade and the democratization of money without supervision and restrictions. However, freedom and security are oftentimes on the opposite side of the measurement scale, which is why problems are arising due to the emergence of DeFi. That's why the society and individual actors in the DeFi ecosystem need to have responsibility in mind in order to prevent criminal activities from happening (such as terrorism and money laundering). The Blockchain community needs to bear in mind that illegal transactions which cannot be linked to particular individuals will be linked to the most common denominator, which is why many can believe that Blockchain or cryptocurrencies are the common enemy.

Namely, based on the official information provided by the FBI, it can be concluded that illicit activities spiked in 2019, when scams involving cryptocurrencies reached 2.1% of total activity. For that reason, privacy coins are used predominantly and demand more attention than other cryptocurrencies. The situation next year changed, and the number of total illegal activities including scams, ransomware, darknet transactions, terrorism financing, online money laundering decreased to 0.34%.

Regardless of that, it is in the interest of every state to limit the use of cryptocurrencies for illegal purposes, and for that reason proper regulation is one of the most important challenges for a sustainable digital future. Some countries, such as Switzerland and Liechtenstein, were among the first to provide a framework for regulation in the DLT, Blockchain and cryptocurrencies

space. Other countries have decided to completely restrict the usage of cryptocurrencies, but most of them are still seeking long-term regulatory clarity. The problem in regulating cryptocurrency transactions is the fact that it operates on a network that is detached from the traditional system, in a permissionless and decentralized manner, where traditional KYC and AML compliance rules cannot be imposed. Contributing to this issue is that criminals are often quicker in adoption of innovative technologies than regulators. Consequently, pursuing legal action once criminal behavior patterns are detected is not possible without evidence which fits in the definition of the regulator.

Based on a survey conducted on 124 randomly selected respondents, as well as based on 3 interviews with experts in this field, we can conclude that most Millennials are familiar with the concept of both cryptocurrency and Blockchain, which is logical given that it is the generation that most easily accepts innovations in terms of technology. Interestingly, half of them are still not prepared to adopt cryptocurrencies, which could be due to lack of formal education in this field.

When it comes to the experts which have been interviewed in order to get a more complete picture, they are all of the opinion that DeFi is the future of the economy and that the situation on the financial scene has changed greatly with its appearance.

8 LITERATURE

Adam, Hayes (2020), What Happens to Bitcoin After All 21 Million Are Mined.

Adler, John (2019), The Why's of Optimistic Rollup, accessible at: https://medium.com/@adlerjohn/the-why-s-of-optimistic-rollup-7c6a22cbb61a

Adrian, Stein (2018), Reliable money in DeFi: stablecoins, accessible on: https://blog.zerion.io/defi-and-reliable-money-stablecoins-9d87098b495d

Anderson, Luke & Holz, Ralph & Ponomarev, Alexander & Rimba, Paul & Weber, Ingo (2016), New kids on the block: an analysis of modern blockchains.

Andert, Darlene. (2011). Alternating leadership as a proactive organizational intervention: addressing the needs of the baby boomers, generation xers and millennials. Journal of Leadership, Accountability & Ethics.

Antonopoulos, Andreas (2014), Mastering Bitcoin: unlocking digital cryptocurrencies.

Antonopoulus, Andreas (2015), Mastering Bitocin – unlocking digital cryptocurrencies, O'reilly.

Arnold, Martin (2018), Davos: Blockchain Can no Longer be Ignored. Financial Times.

Attaran, Mohsen, Gunasekaran, Angappa, (2019), Applications of Blockchain Technology in Business: Challenges and Opportunities, Cham, Switzerland: Springer International Publishing.

Bahga, Arsheep, Madisetti, Vijau, (2016), Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications.

Baliga, Arati, (2017), Understanding Blockchain Consensus Model, Corporate CTO Office.

Bambara, Joseph J. & Allen, Paul R. (2018), Blockchain a practical guide to developing business, Law and Technology Solutions, McGraw- Hill Education.

Barham, Vicky, Boadway, Robin, Marchand, Maurice, & Pestieau, Pierre, (1995). Education and the poverty trap. European Economic Review, accessible on: https://doi.org/10.1016/0014-2921(94)000407

Bashir, Imran (2017), Mastering Blockchain, Packt, Graz.

Benston, George J., Smith, Clifford W., (1976), A transaction cost approach to the theory of financial intermediation.

Berentsen, A., Schär, F. (2017), Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung. Norderstedt: Books on Demand. ISBN: 978-3-7386-5392-2

Bernstein J., Daniel (2009), Introduction to post-quantum cryptography, Department of Computer Science, University of Illinois at Chicago.

Bitcoin Mining, (2017), available at : https://powercompare.co.uk/bitcoin/ , accessed on: 04.01.2021.

BitFury Group (2015), Public versus Private Blockchains: Part 1: Permissioned Blockchains, accessible on: https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf

Bitkom (2020), Decentralized Finance (DeFi) – A new Fintech Revolution? The Blockchain Trend explained.

Bonneau, Joseph, Miller, Andrew, Clark Jeremy, Narayanan, Arvind, Kroll, Joshua, Felten, Edward, (2015), *Source: Research perspectives and challenges for bitcoin and cryptocurrencies,* Security and Privacy IEEE.

Burniske Chris & Tatar Jack (2017), Cryptoassets The Innovative Investor's Guide To Bitcoin And Beyond.

Buterin, Vitalik (2013), Ethereum White Paper. GitHub. Available: https://Blockchain-lab.com/pdf/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, Vitalik (2016), "What is Ethereum?". Ethereum Official webpage. Available: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

Carter Hoffman (2020), What is DeFi and Why is Everyone Talking About it?, accessible on: https://www.tradefinanceglobal.com/posts/what-is-defi-decentralized-finance/

Casino, Fran, Dasaklis, Thomas & Patsakis, Constantinos (2018), A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics.

Catalini, Christian, Gans, Joshua S., (2019), Some simple economics of the Blockchain, accessible on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598

Cermak, Honkasalo, Zheng, Rogers, Todd, Dantoni, Hoffman, Igamberdiev (2021), Digital asset outlook, The Block - research, accessible at: https://www.theblock-crypto.com/post/88463/2021-digital-asset-outlook

Chainalysis (2019), Crypto Crime Report - Decoding increasingly sophisticated hacks, darknet markets, and scams.

Chaum, David (1981), Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, Berkley.

Congressional Budget Office (2020), Report on the Troubled Asset Relief Program— March 2020.

ConsenSys (2020), Blockchain for Decentralized Finance (DeFi), accessible on: https://consensys.net/Blockchain-use-cases/decentralized-finance/

Coudert, Virginie & Couharde, Cécile & Mignon, Valerie. (2013), Pegging Emerging Currencies in the face of Dollar Swings, Applied Economics.

Cos (2020), Bitcoin's Proof of Work: The problem of the Byzantine Generals, accessible at:https://medium.com/swlh/bitcoins-proof-of-work-the-problem-of-the-byzantine-generals-33dc4540442

Creswell, John W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Los Angeles: Sage.

Creswell, John W., & Plano Clark, V. L. (2011). Designing and conducting mixed methods research (2nd ed.). Thousand Oaks, CA: Sage Publications.

Crosby, Michael, Nachiappan, Siva, Pattanayak, Pradan, Verma, Sanjeev, Kalyanaraman, Vignesh, (2016), Blockchain Technology: Beyond Bitcoin in Applied Innovation Review, Sutardja Center for Entrepreneurship & Technology, Berkeley.

Crypto Compare, (2015) , accessible on: https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/

Crypto Compare, (2015) ,accessible on: https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/

Crypto News, 2020, https://cryptonews.net/en/news/altcoins/339019/

Daniel Eisermann (2020), Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges.

Danny Yang, Philip Treleaven & Richard Gendal Brown (2017), Blockchain technology in Finance, IEEE Computer Security.

Data Flair, *Advantages and Disadvantages of Blockchain Technology*, accessible at: https://data-flair.training/blogs/advantages-and-disadvantages-of-Blockchain/.

Deal, Jennifer, Altman, David, & Rogelberg, Steven (2010), Millennials at work: what we know and what we need to do (if anything). Journal of Business & Psychology.

Dexter, Shawn. Ethereum Roadmap Update (2018): Casper & Sharding Release Date, accessible at: https://www.mangoresearch.co/ethereum-roadmap-update/

Digiconomist (2020), Bitcoin Energy Consumption Index - Digiconomist, accessible at: https://digiconomist.net/bitcoin-energy-consumption

Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley (2020), Decentralized finance.

Dudka, Gleb (2020), DeFi Digest and Common Issues, accessible at: https://www.stakingrewards.com/journal/defi-digest-ecosystem

Drescher, Daniel (2017), BLOCKCHAIN BASICS- A NON-TECHNICAL INTRODUCTION IN 25 STEPS, Apres, Frankfurt.

Egor Zmaznev, Bitcoin and Ethereum evolution (2017), CENTRIA UNIVERSITY OF APPLIED SCIENCES..

Eli Dourado & Jerry Brito (2014), Cryptocurrency, from The New Palgrave Dictionary of Economics, Online Edition.

European Parliament, (2017), *How Blockchain technology could change our lives,* accessible at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf.

Fabian Schär (2020), Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, accessible at: https://www.researchgate.net/publication/340061422_Decentralized_Finance_On_Blockchain-_and_Smart_Contract-based_Financial_Markets

FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, accessible at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Felea, Mihai, Albastroiu, Irina, (2013), *Defining the Concept of Supply Chain Management and its Relevance to Romanian Academics and Practitioners,* accessible at: https://www.researchgate.net/publication/265674819_Defining_the_concept_of_SCM_and_its_relevance_to_romanian_academics_and_practitioners.

Ferraro, Thomas (2009), U.S. Senate votes to ban executive bonuses, Reuters.

Forman, Christopher, Henkel, Joachim, Leiponen, Aija, Thomas, Llewellyn, Altmann, Peter, Halaburda, Hanna & Obermeier, Daniel. (2019), The Trust Machine? The Promise of Blockchain-Based Algorithmic Governance of Exchange, Academy of Management Proceedings.

Furrer, F.J. Roger A. Grimes, (2020) Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Informatik Spektrum 43.

Fran Casinoa, Thomas K. Dasaklisb & Constantinos Patsakis, (2019), A systematic literature review of Blockchain-based applications:Current status, classification and open issues, Elsevier.

Gibson, Lindsey & Sodeman, William. (2014), Millennials and Technology: Addressing the Communication Gap in Education and Practice. Organization Development Journal.

Gluchowski, Alex (2020), Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework, Matter labs, accessible at: https://medium.com/matter-labs/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955

Golosova, Julija, Romanovs, Andrejs, (2018), The Advantages and Disadvantages of the Blockchain Technology, Latvia.

Guo, Ye & Liang, Chen, (2016), Blockchain application and outlook in the banking industry, Financial Innovation.

Gupta, Manav, (2018), Blockchain for dummies, Hoboken.

Gurguc, Zeynep & Knottenbelt, William (2019), Cryptocurrencies: overcoming barriers to trust and adoption, Imperial College, London.

Gwyneth Iredalecefi (2020), CeFi vs DeFi, accessible on: https://101Blockchains.com/defi-vs-cefi/

Hayek, Friedrich, (1944), The road to serfdom. Chicago: University of Chicago Press.

Holotiu, Friedrich, Pisani, Francesko, Moormann, George J., (2017), *The Impact of Blockchain Technology on Business Models in the Payments Industry,* International Conference on Wirtschaftsinformatik.

Honohan, Patrick, (2008), Cross-country variation in household access to financial services. Journal of Banking & Finance, accessible at: https://doi.org/10.1016/j.jbankfin.2008.05.004.

Huber, Raffael (2021), Bitcoin's energy consumption, Bitcoin suisse research, accessible at: https://www.bitcoinsuisse.com/research/decrypt/bitcoins-energy-consumption

Ivana Cunjak Mataković & Hrvoje Mataković (2018), Cryptocurrencies – sophisticated code of manipulation, International Journal of DIGITAL TECHNOLOGY & ECONOMY Volume 3, Number 1.

Jamie Bertlet (2016), The Darknet, Inside the digital underworld.

Jingjing Jiang, (2018), Millennials stand out for their technology use, accessible on: https://www.pewresearch.org/fact-tank/2018/05/02/millennials-stand-outfor-their-technology-use-but-older-generations-also-embrace-digital-life

Joseph E. Stiglitz (2017), The revolution of information economics: The past and the future, Cambridge.

Kabir, Syed Muhammad, (2016), METHODS OF DATA COLLECTION.

Kaifi, Belal, A., Nafei, Wageeh A., Khanfar, Nile M., & Kaifi, Maryam M. (2012). A multi-generational workforce: managing and understanding millennials. International Journal of Business & Management.

Keynes, John Maynard, (1936), The general theory of employment, interest and money. London: Macmillan.

Khadka, Roshan, (2020), The impact of Blockchain technology in banking, CENTRIA UNIVERSITY OF APPLIED SCIENCES.

Klaus Schwab (2017), The Fourth Industrial Revolution: What It Means and How to Respond.

Konstantinos Christidis & Michael Devetsikiotis (2016), Blockchains and smart contracts for the internet of things, IEEEAccess, vol. 4.

Lambert, Thomas, Liebau, Daniel & Roosenboom, Peter (2020), Security Token Offerings. SSRN Electronic Journal. 10.2139/ssrn.3634626.

Laura Franke, Marco Schletz & Soren Salomo (2020), Designing a Blockchain Model for the Paris Agreement's Carbon Market Mechanism.

Lawrence J. White (2009) THE CREDIT-RATING AGENCIES AND THE SUBPRIME DEBACLE, Critical Review.

Leising, Matthew (2017), The Ether Thief, accessible at: https://www.bloomberg.com/features/2017-the-ether-thief/

Light, John, (2017), The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin, accessible at: https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9, accessed on 30.12.2020.

Lisk (2019), Proof of Work, accessible at: https://lisk.io/what-is-Blockchain

Madeleine Gartz & Ida Iinderbrandt (2017), Are Cryptocurrencies the Future of Money?, Stockholm, Sweden.

Maher Alharby & Aad van Moorsel (2017), BLOCKCHAIN-BASED SMART CONTRACTS: A SYSTEMATIC MAPPING STUDY, DOI: 10.5121/csit.2017.71011.

Marchenkova, Anastasia (2019), When can a quantum computer destroy bitcoin?, accessible at: https://www.amarchenkova.com/2019/09/13/quantum-computer-bitcoin/

Mathers, Nigel, Fox, Nick & Hunn, Amanda (2000), Using Interviews in a Research Project.

McKinsey (2015), Beyond the Hype: Blockchains in Capital Markets, McKinsey & Company.

McLean, Bethany & Nocera, Joe (2011), All the Devils Are Here: The Hidden History of the Financial Crisis.

McNamara, Carter (1999), General Guidelines for Conducting Interviews, Authenticity Consulting, LLC, accessible on: http://www.managementhelp.org/evaluatn/intrview.htm

Merkle, Ralph (1979), A certified digital signature, BNR INc., Palo Alto, California, 94304.

Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson & Neha Narula (2018), The Impact of Blockchain Technology on Finance: A Catalyst for Change, International Center for Monetary and Banking Studies (ICMB).

Min Xu, Jeanne M. David & Suk Hi Kim (2018), The Fourth Industrial Revolution: Opportunities and Challenges.

Moritz Holtmeier & Philipp Sandner (2019), The impact of cryptocurrencies on developing countries, Frankfurt School Blockchain Center.

Morris, David Z. (2016), Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting, Fortune, accessible at: https://fortune.com/2016/05/15/leaderless-Blockchain-vc-fund/

Nakamoto Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, Arvind, Bonneau, Joseph, Felten Edward, Miller Andrew & Goldfeder, Steven (2016), Bitcoin and cryptocurrency technologies, Princeton University Press.

Nguyen, Q.K., (2016), Blockchain- A Financial Technology for Future Sustainable Development. In: Proceedings – 3rd International Conference on Green Technology and Sustainable Development, GTSD 2016, pp. 51–54.

O'Leary, Zina (2014). The essential guide to doing your research project (2nd ed.). London: SAGE.

Oblinger Diana (2003), Boomers, Gen-Xers, and Millennials: Understanding the "New Students", accessible on: https://er.educause.edu/articles/2003/1/boomers-genxers-and-millennials-understanding-the-new-students

O'Sullivan, Artur, & Sheffrin, Steven M. (2003) Economics: Principles in action. Needham, Mass.: Prentice Hal.

Park, Sunoo, Specter, Michael, Narula, Neha & Rivest, Ronald (2020), Going from Bad to Worse: From Internet Voting to Blockchain Voting.

Peck, Morgan (2016), Hard Fork" Coming to Restore Ethereum Funds to Investors of Hacked DAO, IEEE Spectrum: Technology, Engineering, and Science News.

Phillips Andrew (2016), Research tools: interviews & questionnaires, accessible on: https://lled500.trubox.ca/2016/225

Piscini, Eric, Guastella, Joe, Rozman, Alex & Nassim, Tom (2017), Blockchain trust economy, Deloitte, University press.

Piscini, Eric, Hyman, Gys & Henry,Wendy (2017), Blockchain: trust economy - taking control of digital identity, Deloitte, University press.

Popper, Nathaniel (2016), Hacker May Have Taken $50 Million From Cybercurrency Project, The New York Times.

Rainer Böhme, Nicolas Christin, Benjamin Edelman & Tyler Moore (2015), Bitcoin: Economics, Technology, and Governance, Journal of Economic Perspectives.

Randall Dodd & Paul Mills (2008), Outbreak: U.S. Subprime Contagion, International Monetary Fund, accessible at: https://www.imf.org/external/pubs/ft/fandd/2008/06/dodd.htm

Reitwießner, Christian (2016), zkSNARKs in a Nutshell, accessible at: https://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf

Robby Houben (2015), Bitcoin: there are two sides to every coin", ICCLR, Vol. 26, Issue 5.

Robert Herian (2019), Regulating Blockchain, Critical Perspectives in Law and Technology.

Robleh, Ali, Barrdear, John, Clews, Roger, Southgate, James, (2014), Innovations in Payment Technologies and the Emergence of Digital Currencies. Bank of England.

Rosa Righi, R., Alberti, A. M., & Singh, M. (2020), Blockchain Technology for Industry 4.0, Springer Singapore.

Rosalind Z. Wiggins, Thomas Piontek & Andrew Metrick (2014), The Lehman Brothers Bankruptcy A: Overview, yale program on financial stability case study.

Sams, Robert (2015), A Note on Cryptocurrency Stabilisation: Seigniorage Shares.

Samuel, Joel (2018), The future of cryptocurrency is trust, accessible at: https://joelgsamuel.medium.com/the-future-of-cryptocurrency-is-trust-aa53f1cc476f

Sandner Philipp, Welpe Isabell, & Tumasjan Andranik (2019). Der Blockchain Faktor. BoD - Books on demand

Sayeed, Sarwar, Gisbert, Hector Marco (2019), Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack, accessible at: https://www.researchgate.net/publication/332737156_Assessing_Blockchain_Consensus_and_Security_Mechanisms_against_the_51_Attack.

Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht (PDF). 27 September 2014. p. 6. Archived from the original (PDF) on 20 February 2014.

Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš (2018), Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?.

Seang Sothearath & Torre Dominique (2018), Proof of Work and Proof of Stake consensus protocols: a Blockchain application for local complementary currencies, Gestion (GREDEG CNRS), France.

Seba Bank (2021), Seven regulatory developments for 2021, The digital regulator.

Sebastian E. Peyrott (2017), An Introduction to Ethereum and Smart Contracts.

Shor, P.W. (1994), Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134.

Smith, Travis & Nichols, Tommy (2015), Understanding the Millennial Generation.

Song, Woochul, Shi, Stone, Xu, Victoria, Gill, Gurshahib, (2016), Advantages & disadvantages of Blockchain technology.

Songara, Ankit & Chouhan, Lokesh (2017), Blockchain: A Decentralized Technique for Securing Internet of Things, Conference paper.

Swan, Melanie (2015), Blockchain: Blueprint for a new economy. Beijing: O'Reilly.

Szabo, Nick (1997), Smart Contracts: Formalizing and Securing Relationships on Public Networks, First Monday, Volume 2.

Taleb, Nassim, (2012), Antifragile: Things that gain from disorder. Random House.

Tapscott, Dan (2018), Blockchain Revolution – How the Technology Behind BITCOIN and other cryptocurrencies is changing the World, CEO, Microsoft Corporation.

Tapscott, Dan, & Tapscott, Alex (2016). Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. New York: Penguin Random House LLC

Tar, Andrew, (2018), *Proof-of-Work, Explained*, accessible at: https://cointelegraph.com/explained/proof-of-work-explained.

Tasca Paolo & J. Tessone Claudio (2020), A Taxonomy of Blockchain Technologies:Principles of Identification and Classification, Ledger journal.

The Law Library of Congress (2018), Regulation of Cryptocurrency Around the World, Global Legal Research Center.

Thin, Wai Yan Maung, Dong, Naipeng, Bai, Guangdong & Dong, Jin Song, (2018), *Formal Analysis of a PoS Blockchain,* National University of Singapore.

Treiblmaier, H. & 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, and F. Witte (New Jersey, NJ), 105–124. doi: 10.1142/9781786346391_0006

Veen, Wim & Vrakking, Ben (2006), Homo Zappiens, Growing up in a Digital Age. London: Network Continuum Education.

Vigna, Paul & Casey, Michael (2016), The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Picador.

Vigna, Paul (2016), Chiefless Company Rakes in More than $100 Million, The Wall Street Journal.

Viswanathan, Surya & Shah, Aakash (2018), The Scalability Trilemma in Blockchain, accessible at: https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df

William Metcalfe (2020), Ethereum, Smart Contracts, DApps.

Wood, Gavin (2017a). Ethereum: a secure decentralized generalized transaction ledger. Gavin Wood Official website, accessible at: http://gavwood.com/paper.pdf

Yan Chen & Cristiano Bellavitis (2020), Blockchain disruption and decentralized finance: The rise of decentralized business models, in Journal of Business Venturing Insights.

Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Xiangping & Wang, Huaimin. (2017), An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, Big-DataCongres

9 APPENDICES

9.1 Appendix A: Questionnaire

1. Gender: Male Female

2. Age _____

3. Formal education:

- Primary school
- High school
- University

4. How familiar are you with Blockchain technology? (1- Not familiar, 5- Very familiar)

1. 2. 3. 4. 5.

5. Performance Expectancy - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- Using cryptocurrencies will help me achieve my financial goals completely
- Using cryptocurrencies will help me achieve my financial goals faster
- Using cryptocurrencies will increase my standard of living
- Using cryptocurrencies will not change my life in any aspect

6. Effort expectancy - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- I easily learned to invest in cryptocurrencies
- Using cryptocurrencies is clear and understandable to me
- It will be easy for me to become an expert in using cryptocurrencies in a while
- Using cryptocurrencies is extremely difficult for me

7. Social influence - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- My family believes that I should use cryptocurrencies
- My friends believe that I should use cryptocurrencies
- People whose opinions I value encourage me to use in cryptocurrencies
- People whose opinions I care about discourage me to use cryptocurrencies

8. Facilitating conditions - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- I have the necessary computer hardware/software to use cryptocurrencies
- I have all the necessary knowledge to use cryptocurrencies
- Using cryptocurrencies feels similar to making other online investments (stocks, bonds,...)
- I don't have all the necessary resources and knowledge to invest in cryptocurrencies

9. Hedonic motivation - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- Using cryptocurrencies helps getting business done more easily
- Using cryptocurrencies makes me happy, because I am improving my technological knowledge
- Using cryptocurrencies can increase my income
- Using cryptocurrencies cannot change anything in my life

10. Price value - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- Using cryptocurrencies (can) increase my costs and expenses
- Using cryptocurrencies does not increase my costs and expenses
- Using cryptocurrencies (can) increase my income
- I do not (plan to) use cryptocurrencies

11. Habit - Adapted from the UTAUT2 scale (Venkatesh et al., 2012)

- Using cryptocurrencies makes doing business easier and more convenient
- I check the price of cryptocurrencies on a regular basis
- Using cryptocurrencies does not affect my life in any way

12. Thinking about the next 2 years would you? (Adopted from the OECD)

- Buy (more) cryptocurrencies
- Save cryptocurrencies
- Sell (spend) cryptocurrencies
- I don't (plan to) use cryptocurrencies

13. Cryptocurrencies can easily be converted into cash - Adopted from OECD, 2019, (1- Disagree, 5-Agree).

1. 2. 3. 4. 5.

14. It's a good time to buy cryptocurrencies - Adopted from OECD, 2019, (1- Disagree, 5-Agree).

1. 2. 3. 4. 5.

15. If European Central Bank issues its own cryptocurrency would you... (1- Resist, 5- Adopt)

1. 2. 3. 4. 5.

16. Which of the following activities would you accept?

- Receive a salary in cryptocurrencies
- Borrow money in cryptocurrencies
- Raise capital for a business in cryptocurrencies
- Nothing

17. Would cryptocurrencies in paper form increase trust and adoption in your opinion?

- Yes
- No
- Maybe

18. Do you trust financial institutions (banks, payment providers, etc.)? (1- I do not trust at all, 5- I trust completely).

1. 2. 3. 4. 5.

19. Are you familiar with the concept of decentralized finance (open finance, finance without trust-based institutions)?

- Yes
- No
- Maybe

20. If cryptocurrencies (and decentralized finance) would replace banks (and trust-based financial institutions), what would be the effect?

- More justice to society
- More democratic society
- More freedom of trade
- More financial privacy
- I cannot imagine a life without a bank

21. Do you think that your financial education is in the best interest of your government or bank?

- Yes
- No
- Maybe

22. Should the government restrict the use of cryptocurrencies?

- Yes
- No
- Maybe

23. Would cyber-crime increase with the use of cryptocurrencies?

- Yes
- No
- Maybe

24. Do you think that it is necessary to include “Basics of cryptocurrencies and the use of Blockchain technology in finance” as a compulsory subject in school or university?

- Yes
- No
- Maybe

25. What is the value of cryptocurrencies (such as bitcoin) in your opinion?

- Worthless
- Digital gold
- Speculative asset
- Money for criminals and terrorists
- Other

26. What disturbs you the most about cryptocurrencies?

- Missing education
- Uncertainty in regulation
- Too difficult to use
- Opinions of friends and family
- No support from my government
- Price fluctuation
- Negative news

9.2 Appendix B: Interviews

9.2.1 First expert interview

H.H. was part of the traditional ecosystem until H.H. stumbled upon Blockchain. After understanding how technologically profound Bitcoin is in its simplicity, H.H. saw a potentially disruptive business model which can be used even beyond Bitcoin. Today, H.H. is heavily engaged in the Blockchain industry at the heart of Crypto Valley. Mr H.H. is working on a daily basis with financial institutions, unicorn companies, policy makers, universities and licensed crypto banks.

What led you to enter the world of Blockchain technology and direct your interests towards it?

I was working in the hedge fund industry and when I learned about Bitcoin, it completely blew my mind. I realized that Blockchain can have applications in the hedge fund industry in terms of providing more transparency, saving costs and optimizing fund structures more efficiently. I really saw that it could be the future of investment funds. In the last 10 years, the regulatory hurdles were quite big, but this is changing now. The investor have more transparency about investments and Blockchain is perfectly suited for that.

Back then, I worked for a big hedge fund in the DACH region, and the company didn't have the appetite at that point to experiment with Blockchain technology and due to high regulatory uncertainty, it was a good decision. But at the same time, if you want to have the first-mover advantage, you need to take risks. After discovering Crypto valley, my visions for the future changed and I wanted to follow my passion.

After I moved to Switzerland, my conclusion was that there is a tremendous gap between traditional finance and Blockchain startups, and I founded the Multichain Asset Managers Association (MAMA Global) which would help build synergies and to nourish the connection between the two ecosystems.

MAMA is about education and on the other is the help with regulatory proposals. We also partner with universities to give lectures to students talking about traditional way of managing assets and then how to do it on-chain. The greatest joy is educating students so that they can explore different possibilities which the 21st century has to offer and to get insights from the industry.

Is there a personal milestone that you're proud of?

Last year we were invited to the world economic forum and presented our way of teaching students using an innovative protocol which enables an individual to set-up their own hedge funds. We have received an award for the teaching method, and we plan to educate C-level executives with this approach.

What do you think about DeFi in 5 years?

I'm very excited about the future of DeFi but I don't see a real merge between CeFi and DeFi by definition. What is DeFi? Something on the Blockchain? The point is that it is controlled by someone and that's inherently against DeFi.

We must understand that the concept of a company is not "DeFi" inherently. The one is highly regulated, and on the other hand is more freedom.

What are the main challenges for asset managers when it comes to the adoption of DeFi?

Although the companies would like to use DeFi, they don't want to give away control of the assets. This goes against the principles and the current definition of DeFi, where everybody should be in control of their assets, without any counterparty risk. But from all risks, the regulatory risk is the most significant that established companies are afraid of, because it cannot "make you" but it can certainly "break you" very fast. Regulators love the idea on a personal level, but the regulatory system is slow. Big companies are being faced with a lot of regulation and staying compliant is a cost that every business needs to include in their business model. From this perspective, big companies are not that agile as startups since internal systems cannot be changed back and forth without a great increase in cost. The regulatory challenges have almost diminished in Switzerland and I believe that this will be a big push for DeFi, but we are doing our best to educate and to make CeFi ready for DeFi, as well as the other way around. I believe there is a healthy future for both of them.

9.2.2 Second expert interview

Both interview partners are currently based in Zug, Switzerland working in the most well-known Blockchain incubator in the world – Crypto valley. It counts more than 4.400 Blockchain enthusiasts working in 850 companies including unicorns and smaller startups in December 2020. In addition to the venture capital expertise, CV operates the incubator CV Labs, which has been offering entrepreneurial advisory services, coworking spaces, and consulting in Switzerland, Liechtenstein and soon in the UAE. CV VC is a founding partner of the Swiss Blockchain Federation, a public-private partnership that fosters a standard of excellence for the Blockchain sector and tries to connect corporates with startups.

T.T. (Co- Head, CryptoValley VC) is currently in charge of the corporate and institutional side of CV Labs.

T.T. holds a BSc in Political science & International relations from University of California, MA in Global economy & Strategy from Yonsei University, and a MA in International affairs from the University of St. Gallen.

Her career started with the United Nations Organization, researching think-tanks and tech companies in Europe and Asia.

Before joining CV VC, T.T. was a Client relationship and project manager in Heroes Group AG helping businesses develop appropriate enterprise solutions and effective marketing strategies. T.T. was a co-host at decentra.live, an online news show focused on Blockchain-related topics.

N.R. (Co- Head of CV VC) helps build up the Blockchain incubation program at CV Labs, and scouts high-quality startups for Europe's largest Blockchain startup contest, CV Competition. N.R. holds a Bachelor's degree in International Business Administration with a major in International Entrepreneurship and is a mentor at Blockchain Xcelerator, the newest lab at the Center for Entrepreneurship in the School of Engineering at the University of Berkeley.

When it comes to adoption, how are traditional financial organizations reacting to Blockchain technology and decentralized finance?

N.R.:

We see traditional financial institutions' interest growing year by year. I saw that already in 2017 during a research project within a major Swiss bank. Already at that point banks were researching Blockchain technology and in my opinion, it was only a matter of time that others started experimenting as well. The interest is growing and that's why I see a bright future for Blockchain technology. When it comes to decentralized finance, it is hard to predict how financial organizations will end up reacting to it ultimately, but it is not a topic that they could afford ignoring entirely. I believe the market will change towards more decentralization and traditional institutional players will need to adapt. What is certain is that more and more financial institutions will end up adopting in one way or another, now that the regulatory landscape has become clearer.

T.T.:

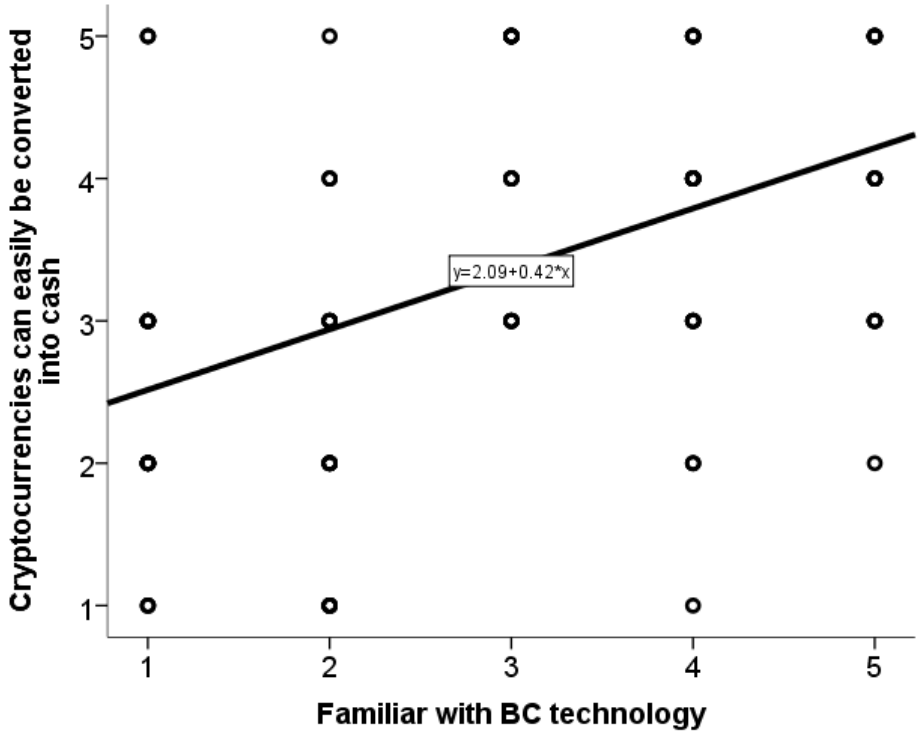
Regulators have helped with providing guidelines but at the moment it is still too early to predict what it will look like exactly in the end. Looking at the past 10 years, the road was paved with uncertainty in the digital asset space. Many organizations have been dismissing Blockchain and digital assets altogether, although benefits have been known for years, but this is changing as more and more systematically relevant financial institutions are embracing it without being too open about it. This spike in institutional adoption wouldn't be the case if people wouldn't see a genuine store of value in bitcoin in my opinion. The adoption aspect was an important milestone and also a contributing factor as to why traditional financial institutions are taking this topic more seriously. They have realized that they need to be open for innovation and to embrace technological changes in order to stay relevant. The past economic struggles are a sign, and I believe that not only the average consumer but also financial institutions should realize that something needs to change for a better future. And I believe that Blockchain, digital assets, and decentralized finance should definitely be part of a healthy, sustainable, fully-functioning financial system in the new economy.

9.3 Appendix C: SPSS output

H1: Millennials who are familiar with Blockchain technology think cryptocurrencies can easily be converted into cash

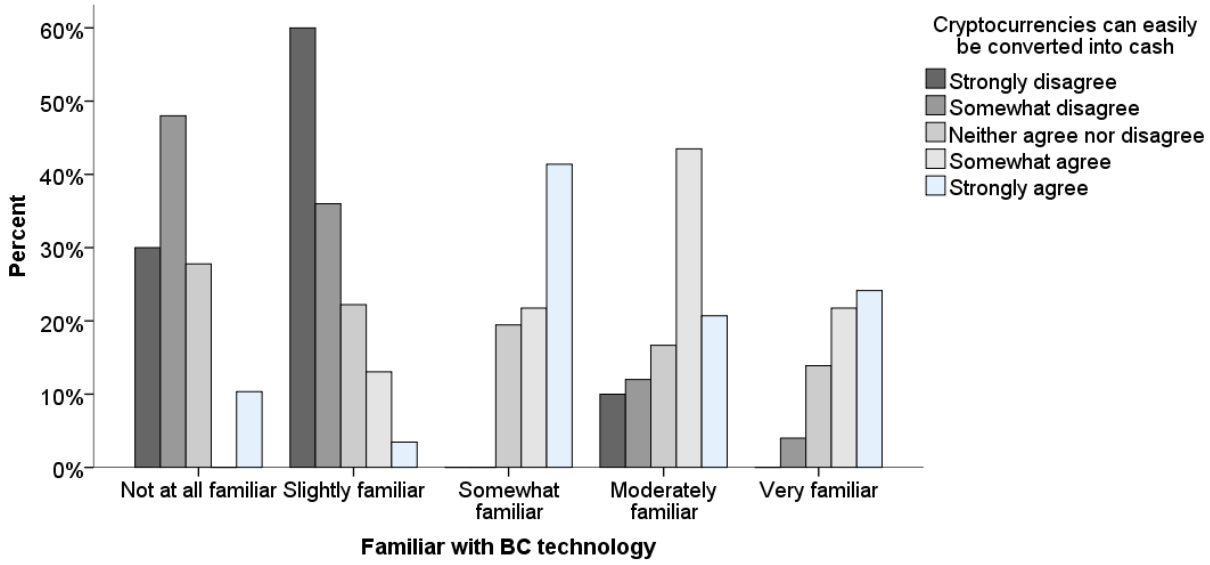
Correlations

			Q4_Familiar_with_BC_technology	Cryptocurrencies can easily be converted into cash
Spearman's rho	Q4_Familiar_with_BC_technology	Correlation Coefficient	1.000	.478**
		Sig. (2-tailed)	.	.000
		N	123	123
	Cryptocurrencies can easily be converted into cash	Correlation Coefficient	.478**	1.000
		Sig. (2-tailed)	.000	.
		N	123	124



Q4_Familiar_with_BC_technology * Cryptocurrencies can easily be converted into cash Crosstabulation

			Cryptocurrencies can easily be converted into cash					
			Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
Q4_Familiar_with_BC_technology	Not at all familiar	Count	3	**12**	**10**	0	3	28
		% of Total	2.4%	9.8%	8.1%	0.0%	2.4%	22.8%
	Slightly familiar	Count	6	**9**	**8**	3	1	27
		% of Total	4.9%	7.3%	6.5%	2.4%	0.8%	22.0%
	Somewhat familiar	Count	0	0	**7**	**5**	**12**	24
		% of Total	0.0%	0.0%	5.7%	4.1%	9.8%	19.5%
	Moderately familiar	Count	1	3	**6**	**10**	**6**	26
		% of Total	0.8%	2.4%	4.9%	8.1%	4.9%	21.1%
	Very familiar	Count	0	1	**5**	**5**	**7**	18
		% of Total	0.0%	0.8%	4.1%	4.1%	5.7%	14.6%
Total		Count	10	25	36	23	29	123
		% of Total	8.1%	20.3%	29.3%	18.7%	23.6%	100.0%


Cryptocurrencies can easily be converted into cash
Strongly disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Strongly agree
Percent
60%
50%
40%
30%
20%
10%
0%
Not at all familiar
Slightly familiar
Somewhat familiar
Moderately familiar
Very familiar
Familiar with BC technology

.

H2: Millennials who are familiar with Blockchain technology would accept to receive a salary in cryptocurrency

Group Statistics

	Receive a salary in cryptocurrencies	N	Mean	Std. Deviation	Std. Error Mean
Q4_Familiar_with_BC_technology	No	78	**2.35**	1.257	.142
	Yes	45	**3.67**	1.187	.177

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Q4_Familiar_with_BC_technology	Equal variances assumed	.531	.468	**-5.726**	**121**	**.000**	-1.321	.231	-1.777	-.864
	Equal variances not assumed			-5.815	96.308	.000	-1.321	.227	-1.771	-.870

H3: Millennials who believe that cryptocurrencies can increase their income would buy more cryptocurrencies in the next 2 years

Using cryptocurrencies can increase my income * Buy (more) cryptocurrencies Crosstabulation

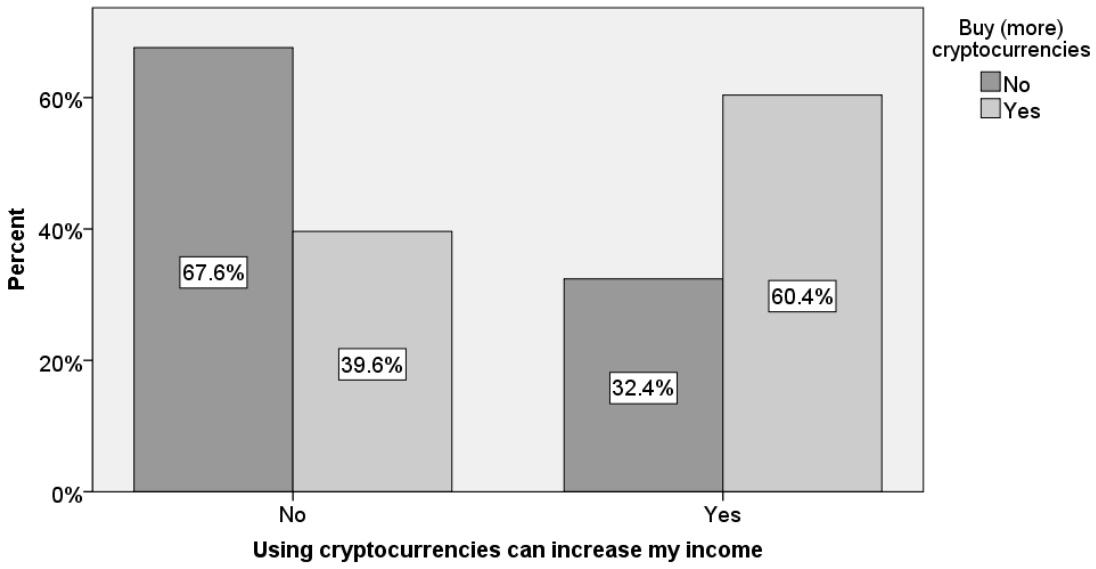
			Buy (more) cryptocurrencies		
			No	Yes	Total
Using cryptocurrencies can increase my income	No	Count	**48**	21	69
		% of Total	38.7%	16.9%	55.6%
	Yes	Count	23	**32**	55
		% of Total	18.5%	25.8%	44.4%
Total		Count	71	53	124
		% of Total	57.3%	42.7%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	9.628[a]	1	.002		
Continuity Correction[b]	**8.528**	**1**	**.003**		
Likelihood Ratio	9.710	1	.002		
Fisher's Exact Test				.003	.002
Linear-by-Linear Association	9.550	1	.002		
N of Valid Cases	124				

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	**.279**	.002
	Cramer's V	.279	.002
N of Valid Cases		124	



H4: Millennials who are familiar with DeFi believe that the government should restrict the use of cryptocurrencies

Are you familiar with the concept of decentralized finance (open finance, finance without trust-based institutions)? * Should the government restrict the use of cryptocurrencies? Crosstabulation

			Should the government restrict the use of cryptocurrencies?		
			Yes	No	Total
Are you familiar with the concept of decentralized finance (open finance, finance without trust-based institutions)?	Yes	Count	8	36	44
		% of Total	11.0%	49.3%	60.3%
	No	Count	6	23	29
		% of Total	8.2%	31.5%	39.7%
Total		Count	14	59	73
		% of Total	19.2%	80.8%	100.0%

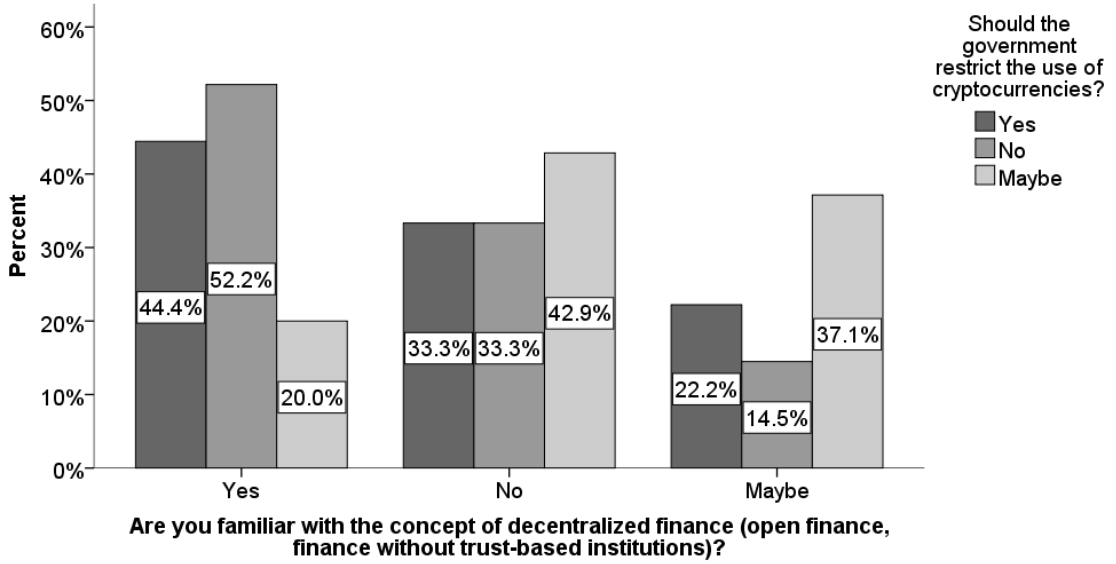
Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.071[a]	1	.790		
Continuity Correction[b]	**.000**	**1**	**1.000**		
Likelihood Ratio	.070	1	.791		
Fisher's Exact Test				1.000	.510
Linear-by-Linear Association	.070	1	.791		
N of Valid Cases	73				

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	**-.031**	.790
	Cramer's V	.031	.790
N of Valid Cases		73	

Maybe group excluded from analysis and results respresented in appendix:



H5: Milennialls who believe that financial education is in the best interest of their government or bank would adopt cryptocurrencies issued by the ECB

Descriptives

If ECB issues its own cryptocurrencies would you

	N	**Mean**	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Yes	25	**3.52**	1.475	.295	2.91	4.13	1	5
No	58	**2.97**	1.498	.197	2.57	3.36	1	5

Maybe	40	**3.25**	1.149	.182	2.88	3.62	1	5
Total	123	**3.17**	1.395	.126	2.92	3.42	1	5

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
If ECB issues its own cryptocurrencies would you	Equal variances assumed	.076	.783	**1.554**	**81**	**.124**	.554	.357	-.155	1.264
	Equal variances not assumed			1.564	46.229	.125	.554	.355	-.159	1.268

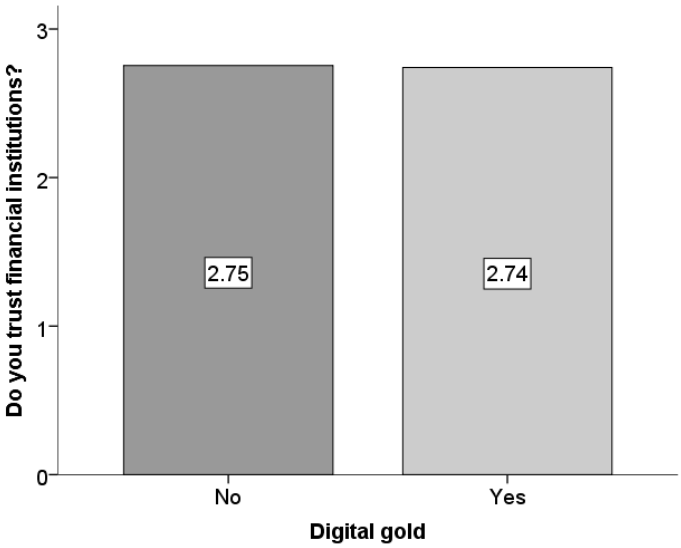
H6: Millennials who trust in financial institutions think that cryptocurrencies are digital gold.

Group Statistics

	Digital gold	N	**Mean**	Std. Deviation	Std. Error Mean
Do you trust financial institutions (banks, payment providers, etc.)?	No	65	**2.75**	1.173	.145
	Yes	58	**2.74**	1.178	.155

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Do you trust financial institutions (banks, payment providers, etc.)? (1- I do not trust at all, 5- I trust completely).	Equal variances assumed	.034	.854	**.059**	**121**	**.953**	.012	.212	-.408	.433
	Equal variances not assumed			.059	119.301	.953	.012	.212	-.408	.433



H7: Millennials who believe that their financial education is in the best interest of the bank or government think that it is necessary to include "Basics of cryptocurrencies and the use of blockchain technology in finance" as a compulsory subject in school or university

Do you think that your financial education is in the best interest of your government or bank? * Do you think that it is necessary to include "Basics of cryptocurrencies and the use of blockchain technology in finance" as a compulsory subject in school or university? Crosstabulation

			Do you think that it is necessary to include "Basics of cryptocurrencies and the use of blockchain technology in finance" as a compulsory subject in school or university?			
			Yes	No	Maybe	Total
Do you think that your financial education is in the best interest of your government or bank?	Yes	Count	16	5	4	25
		% of Total	12.9%	4.0%	3.2%	20.2%
	No	Count	40	11	8	59
		% of Total	32.3%	8.9%	6.5%	47.6%
	Maybe	Count	16	5	19	40
		% of Total	12.9%	4.0%	15.3%	32.3%
Total		Count	72	21	31	124
		% of Total	58.1%	16.9%	25.0%	100.0%

Do you think that your financial education is in the best interest of your government or bank? * Do you think that it is necessary to include "Basics of cryptocurrencies and the use of blockchain technology in finance" as a compulsory subject in school or university? Crosstabulation

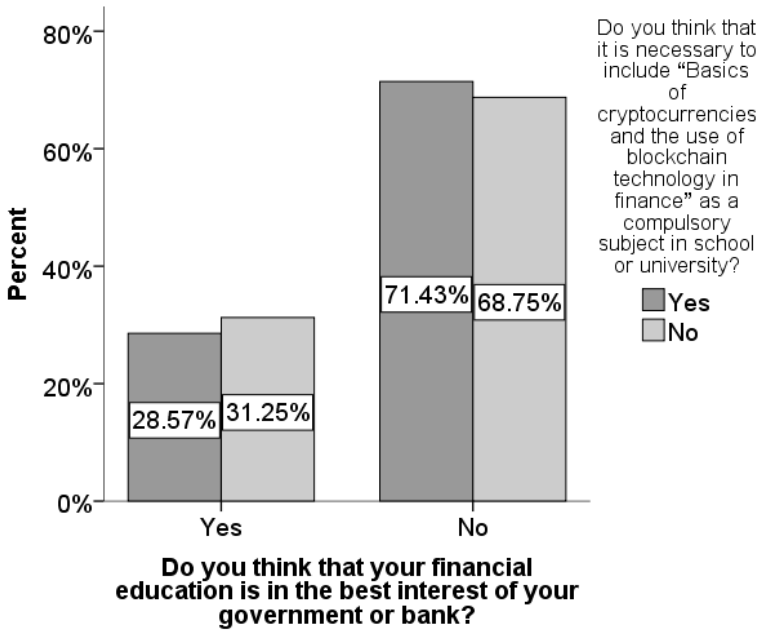
			Do you think that it is necessary to include "Basics of cryptocurrencies and the use of blockchain technology in finance" as a compulsory subject in school or university?		
			Yes	No	Total
Do you think that your financial education is in the best interest of your government or bank?	Yes	Count	16	5	21
		% of Total	22.2%	6.9%	29.2%
	No	Count	40	11	51
		% of Total	55.6%	15.3%	70.8%
Total		Count	56	16	72
		% of Total	77.8%	22.2%	100.0%

Chi-Square Tests

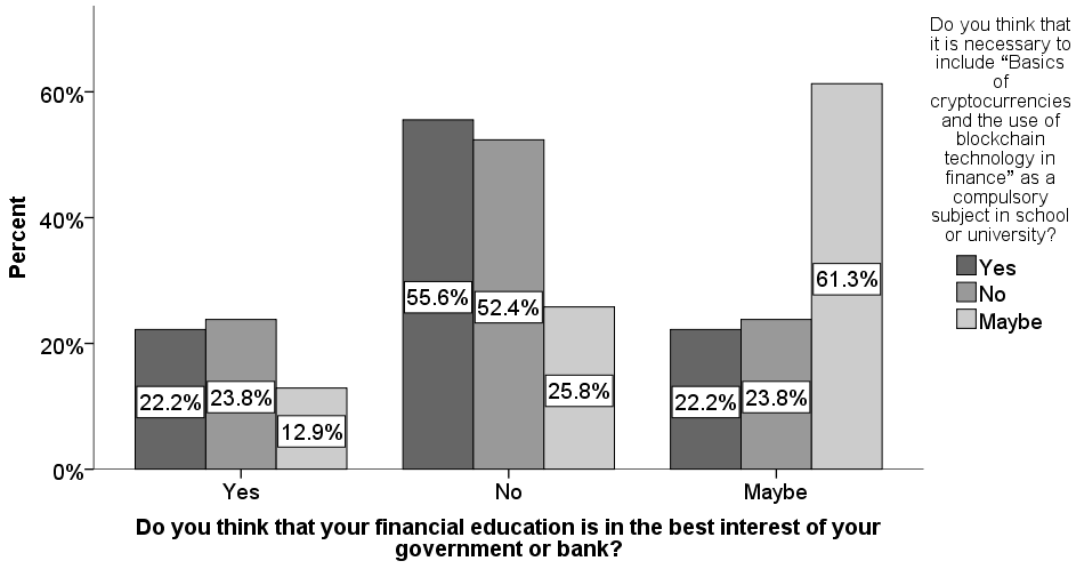
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.043[a]	1	.835		
Continuity Correction[b]	**.000**	**1**	**1.000**		
Likelihood Ratio	.043	1	.836		
Fisher's Exact Test				1.000	.531
Linear-by-Linear Association	.043	1	.836		
N of Valid Cases	72				

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	**-.024**	.835
	Cramer's V	.024	.835
N of Valid Cases		72	



Maybe group excluded from analysis and results respresented in appendix:



H8: Millennials who trust in financial institutions believe that the government should restrict the use of cryptocurrencies.

Descriptives

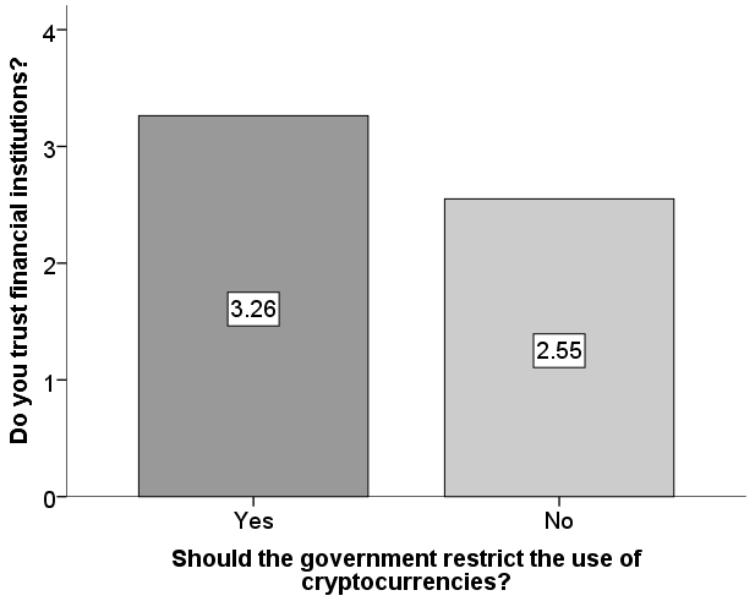
Do you trust financial institutions (banks, payment providers, etc.)? (1- I do not trust at all, 5- I trust completely).

	N	**Mean**	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Yes	19	**3.26**	1.284	.295	2.64	3.88	1	5
No	69	**2.55**	1.157	.139	2.27	2.83	1	5
Maybe	35	**2.86**	1.061	.179	2.49	3.22	1	5
Total	123	2.75	1.171	.106	2.54	2.96	1	5

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Do you trust financial institutions	Equal variances assumed	.804	.372	**2.321**	**86**	**.023**	.712	.307	.102	1.323

(banks, payment providers, etc.)? (1- I do not trust at all, 5- I trust completely).	Equal variances not assumed			2.186	26.599	.038	.712	.326	.043	1.382



H9: Millennials who cannot imagine a life without a bank think that cybercrime would increase with the use of cryptocurrencies

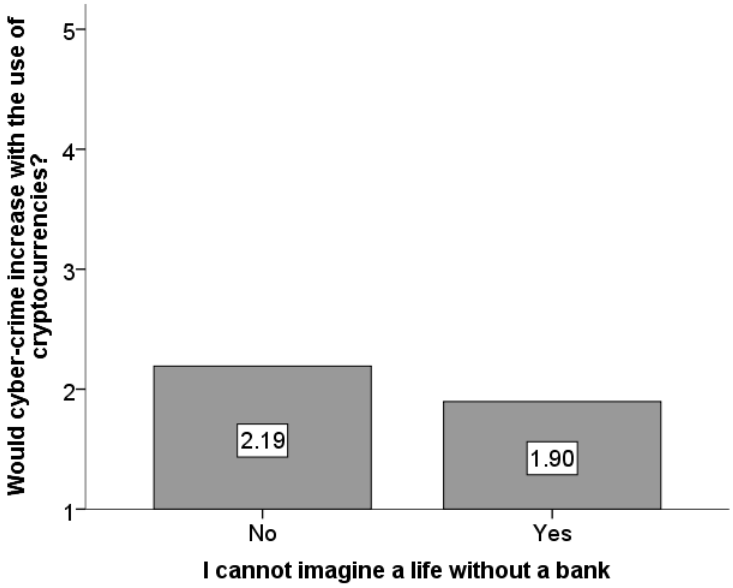
Group Statistics

	I cannot imagine a life without a bank	N	**Mean**	Std. Deviation	Std. Error Mean
Would cyber-crime increase with the use of cryptocurrencies?	No	94	**2.19**	.871	.090
	Yes	29	**1.90**	.976	.181

Independent Samples Test

	Levene's Test for Equality of Variances	t-test for Equality of Means

		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Would cyber-crime increase with the use of cryptocurrencies?	Equal variances assumed	3.700	.057	**1.549**	**121**	**.124**	.295	.190	-.082	.672
	Equal variances not assumed			1.458	42.664	.152	.295	.202	-.113	.703



H10: Millennials who are influenced by negative news think that cryptocurrencies are money for criminal and terrorists

Negative news * Money for criminals and terrorists Crosstabulation

	Money for criminals and terrorists	Total

			No	Yes	
Negative news	No	Count	**88**	4	92
		% of Total	71.0%	3.2%	74.2%
	Yes	Count	**28**	4	32
		% of Total	22.6%	3.2%	25.8%
Total		Count	116	8	124
		% of Total	93.5%	6.5%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.614[a]	1	.106		
Continuity Correction[b]	**1.438**	**1**	**.230**		
Likelihood Ratio	2.305	1	.129		
Fisher's Exact Test				.203	.118
Linear-by-Linear Association	2.593	1	.107		
N of Valid Cases	124				

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	**.145**	.106
	Cramer's V	.145	.106

N of Valid Cases	124