TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Rait Leinus 204778IVCM

Cryptocurrency as a Replacement for Traditional Online Payment Methods

Master's thesis

Supervisor: Alexander H. Norta
PhD

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Rait Leinus 204778IVCM

Krüptovaluuta traditsiooniliste interneti maksemeetodite asendusena

Magistritöö

Juhendaja: Alexander H. Norta
PhD

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Rait Leinus

16.05.2022

Abstract

When implemented correctly cryptocurrency can solve traditional banking system problems such as daily transfer limits, high additional transfer charges, double spending and fractional reserve banking. Cryptocurrencies are currently rarely used as a payment method. The aim of this paper is to find out how to increase cryptocurrency usage as a payment method. Case study research method was used in which 8 subjects with relevant experience in the field of finance, blockchain and/or cryptocurrency were interviewed using a semi-structured interview format. Interview results were thematically analysed. Results indicate that in first world countries the most relevant blocker is absence of regulations which acts as the main blocker. The absence of regulations is currently in the interest of governments and central banks in order to maintain their control over the current monetary system as cryptocurrency opposes a danger to this world order. In addition, results show that in the case of regulatory issues being solved, all the subsequent issues and their relevance will then emerge and resolve in a certain pattern.

This thesis is written in English and is 56 pages long, including 5 chapters, 5 figures and 1 table.

Annotatsioon

Krüptovaluuta traditsiooniliste interneti maksemeetodite asendusena

Korrektse implementatsiooni korral suudab krüptovaluuta lahendada selliseid traditsioonilise pangandussüsteemi probleeme nagu näiteks päevased ülekande limiidid, kõrged ülekande lisatasud, topeltkulutamine ja osareserviga pangandus. Hetkel kasutatakse krüptovaluutat maksemeetodina harva. Selle töö eesmärk on uurida, kuidas suurendada krüptovaluuta kasutamist maksemeetoditena. Uurimistöö meetodina kasutati juhtumuuringut. Tehti 8 pool-struktureeritud intervjuud subjektidega, kellel on asjakohane kogemus finants, blokiahela või krüptovaluuta alal. Intervjuu tulemuste töötlemisel kasutati temaatilist analüüsi. Tulemused näitavad, et esimese maailma riikides on kõige olulisemaks takistajaks puudulikud määrused. Puudulikud määrused on hetkel valitsuste ja keskpankade huvides, et säilitada oma kontrolli rahasüsteemi üle, mida krüptovaluutad ohustavad. Lisaks näitavad tulemused, et kui puudulikude määruste probleem lahendada, siis kõik järgnevad probleemid kerkivad esile ja saavad lahendatud kindla mustri alusel.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 56 leheküljel, 5 peatükki, 5 joonist, 1 tabelit.

List of abbreviations and terms

SWIFT	Society for Worldwide Interbank Financial Telecommunication
SEPA	Single Euro Payments Area
P2P	peer-to-peer, person-to-person or private-to-private payments
SSD	SEPA Direct Debit transaction
PoW	Proof of work blockchain consensus mechanism
PoS	Proof of stake blockchain consensus mechanism
DoS	Denial of Service
IAS 7	International Accounting Standards Board 2017, para 6
IFRS	International Financial Reporting Standards Foundation
DeFi	Decentralized Finance
KYC	Know Your Customer

Table of contents

List of figures

List of tables

1 Introduction

The first cryptocurrency, named Bitcoin, was developed in 2009 [1]. In its essence cryptocurrency is a currency and a digital payment system which can be used to make transactions. During the time of this writing, there exists 10108 cryptocurrencies according to CoinMarketCap [2]. Though the actual number is unknown since all cryptocurrencies might not be registered on CoinMarketCap.

The advantages of cryptocurrency transactions, compared to traditional fiat currency based transactions, rely on blockchain technology. Blockchain technology provides the possibility for properties such as decentralization, transparency, open source, autonomy and immutability [3]. When implemented correctly, these properties offer better security for online transactions compared to traditional money transfers.

Cryptocurrencies, especially Bitcoin, have been in the centre of media attention since 2017. The cryptocurrency market capital rose significantly from around 20 billion USD to 800 billion USD. At the time of this writing the market capital is 1.2 trillion USD. Nevertheless, cryptocurrencies have not found widespread usage as a payment method.

In this thesis we gathered all the relevant issues as to why cryptocurrency usage as a payment method has stayed low despite widespread attention among the general public. Furthermore, the discovered issues are sorted by order of relevance and their solutions are presented.

1.1 Context

We juxtapose cryptocurrency as a payment method with traditional online payment methods. First, when we say cryptocurrency payments, we mean end-to-end transactions that are done via decentralized cryptocurrencies without the conversion to a fiat currency in-between. Secondly, it is important to understand the exact meaning of traditional online payment methods in our context.

Personal checks, money orders and cash payments are used in online transactions whereas these methods are all problematic for the buyer since there is no guarantee that the goods will be delivered as promised [4]. Though still practiced in some parts of the world e.g. United States of America, we will not account these payment methods in our research as these types of payments require some degree of physical intervention to be conducted in the real world as opposed to the digital domain.

Traditional bank transfers rely on Nostro and Vostro accounts which means that when the two banks exchange money, they do not really move the physical money but rather have accounts on each other's bank and during a transfer both of the banks change the balance of their accounts. When two banks do not have direct accounts on each other's banks they use a third party bank. This creates a chain of transactions which quickly becomes expensive because of the transaction fees.

There are two main systems used in traditional cross-border money transfers, that offer secure transfers which are Society for Worldwide Interbank Financial Telecommunication (SWIFT) system and Single Euro Payments Area (SEPA) system in the European Union [1]. One of the disadvantages of the traditional systems is the time it takes to make international transactions which might take up to five days in some cases [1]. The SWIFT and SEPA systems at their core are secure protocols which are used by the issuer and acquirer banks to conduct secure payments between eachother via bank transfers.

Currently the dominant type of online payment method are the card networks. Card network participants consists of consumers, issuers, merchants, acquirers and network operators [4]. Consumer is issued a card by the issuer which is usually a bank that has registered in the card network. Merchants use acquirer banks at their online ecommerce platform. When a payment is made, the issuer bank transfers money to the acquirer bank via the network. Credit card network transaction fees are in the range of 2.5% of the whole transaction amount plus a fixed sum which costs on average 0.10 euros. Visa, MasterCard and Amex are the dominant card networks.

Traditional bank transfer based transactions either direct, through SWIFT, SEPA or card networks are all included in our research as traditional online payment methods. These methods all use fiat currency, central banks and central institutions as their foundation.

All of the before mentioned payment methods have their strengths and weaknesses and thus are utilized in different situations. Since 2017 as blockchain started gaining recognition in wider audiences, cryptocurrency has led to big expectations towards changing the financial sector and the way payments are made despite marginal utilization in the real world [5].

1.2 Problem Statement

Cryptocurrency market capital has seen an exponential growth in the last five years. Starting from 26 billion USD and for a short period of time peaking at 2,94 trillion USD.

Figure 1 Total Cryptocurrency Market Capital [2].

Because of the extensive trading there is also a considerable amount of media attention which rises even more when Bitcoin price fluctuates [6]. Coupled with the number of available cryptocurrencies which exceeds 10000, these signs indicate a hype among the cryptocurrency domain.

There are some major companies that have recently started to accept cryptocurrencies as a payment method such as Mastercard, Microsoft, Starbucks, Tesla, Amazon, Visa, Paypal [6]. But these payments are usually converted into fiat currency during the transaction. Mastercard and Visa do allow their customers to pay with cryptocurrency but the transactions in their networks are still done by converting the cryptocurrency to conventional fiat currency before moving it in their network [7] [8]. Visa recently started to accept payments in the cryptocurrency USD Coin directly, which is a centralized stablecoin cryptocurrency [8].

Currently in Estonia the possibility of using cryptocurrency as a payment method does not exist. Some countries such as China and Russia have banned the use of cryptocurrencies [9]

Taking into account the current situation we decided to formulate the problem statement as follows: Despite rising in mainstream popularity, cryptocurrencies are rarely used as a direct payment method in day to day transactions such as in ecommerce.

The traditional banking system services problems that cryptocurrencies can solve include crashes that occur because of technical issues, account hacking, daily transfer limits, high additional transfer charges, double spending and fractional reserve banking [10]. Cryptocurrency usage at a large scale would contribute to a more secure and fairer monetary system.

1.3 Research Objective

The main objective of this thesis was to understand how to increase decentralized cryptocurrency usage as a payment method at a large scale. This objective was divided into smaller pieces in order to better understand the details of the issue at hand:

- Compare cryptocurrency ecosystem to traditional payment methods ecosystem.
- Describe the reasons why cryptocurrency payments have not found widespread usage among other payment methods.
- Introduce the necessary steps to increase cryptocurrency usage as a payment method.

1.4 Thesis Structure

This dissertation is structured into five chapters. Chapter 1 provides the introduction. Chapter 2 covers background and related academic work in the form of literature review. Chapter 3 describes the methodology of the conducted research. Chapter 4 analyses the results. Chapter 5 provides conclusions.

Chapter 1 provides a brief introduction to cryptocurrency. Furthermore, it describes the context of our thesis by clearly defining the meaning of cryptocurrency and traditional

payment methods in this work. Followed by a problem statement and the research objectives and finalized with the description of the thesis structure.

Chapter 2 covers necessary background and related work in order to understand the topic. Necessary background includes the concepts of banking, digital payment systems, blockchain and cryptocurrency.

Chapter 3 describes the selected case study methodology in detail. Providing research questions, case and subject selection, describing the data collection procedure, data analysis procedure and data validation procedure.

Chapter 4 covers the results in detail in the form of case and subject descriptions and evaluation of validity. The results are divided thematically from which propositions are generated in turn from which hypotheses are generated.

Chapter 5 concludes the research findings as a summary, relates them to existing evidence, provides impact and implications, as well as limitations of the work and suggestions for future work.

2 Overview of the Traditional Payment Methods, Blockchain, Cryptocurrencies and Related Work

This chapter covers concepts which are required in order to understand the empirical part of the research. We relied on earlier studies to give an overview of the concepts and their related work.

2.1 Traditional Online Payment Systems

Online Payment Systems are defined as payments that are initiated, processed and received electronically [11]. First payment systems that were created were strongly connected to account-based bank transfers [11]. Further down along there has been the development of mobile payments, P2P (peer-to-peer, person-to-person or private-to-private) payments, card network payments and digital wallet payments [11]. All of these payment systems have two things in common in which they use fiat currency to transfer funds and require a centralized intermediary entity to help make the transaction.

2.1.1 Bank Transfer

European Union has developed the Single Euro Payment Area (SEPA) which allows 500 million citizens of European Union to make and receive over 100 billion payments each year [12]. SEPA Direct Debit (SDD) is a service where consumers can make euro payments using a single bank account and single set of instructions [12]. SSD faces increasing cybercrime attacks with fraud in the forefront [12].

Typical examples of SSD payments are recurring payments such as television subscription, gym subscription etc. [12].

In SSD there are three actors involved – creditor, debtor and their banks [12]. Creditor is the person or company who collects funds from the debtor's bank account, debtor provides funds from his/her bank account and their banks represent the respective entities [12].

When the creditor draws funds from another bank account there must be an acquired SSD mandate first that is given by the debtor [12]. During the transaction the creditor sends a request with information about the amount of the transaction to his/her bank that will start

the process to request the amount from the debtor's bank account [12]. The debtor only needs to provide a signature of the mandate and has no prior knowledge of the direct debit being charged to his/her bank account [12]. The debtor will have knowledge only after creditor sends a receipt by using best effort service without guarantee or when the funds have already been withdrawn from the account [12]. This enables the exposure for a large number of possible frauds [12].

The SSD process is shown in the figure 2. First, the mandate is signed by the debtor and is notified to the creditor bank (known as acquisition) [11]. Secondly the creditor bank sends a validation request for the received mandate to the debtor bank who will in turn return the validation (known as validation) [11].

During the SSD request the creditor generates a receipt, sends it to its bank and the creditor bank then sends an SSD request to the Debtor Bank which debits the SSD on debtors account [11]. The debtor bank then communicates the result to the creditor bank and then the creditor bank credits the amount on the creditor's account [11].

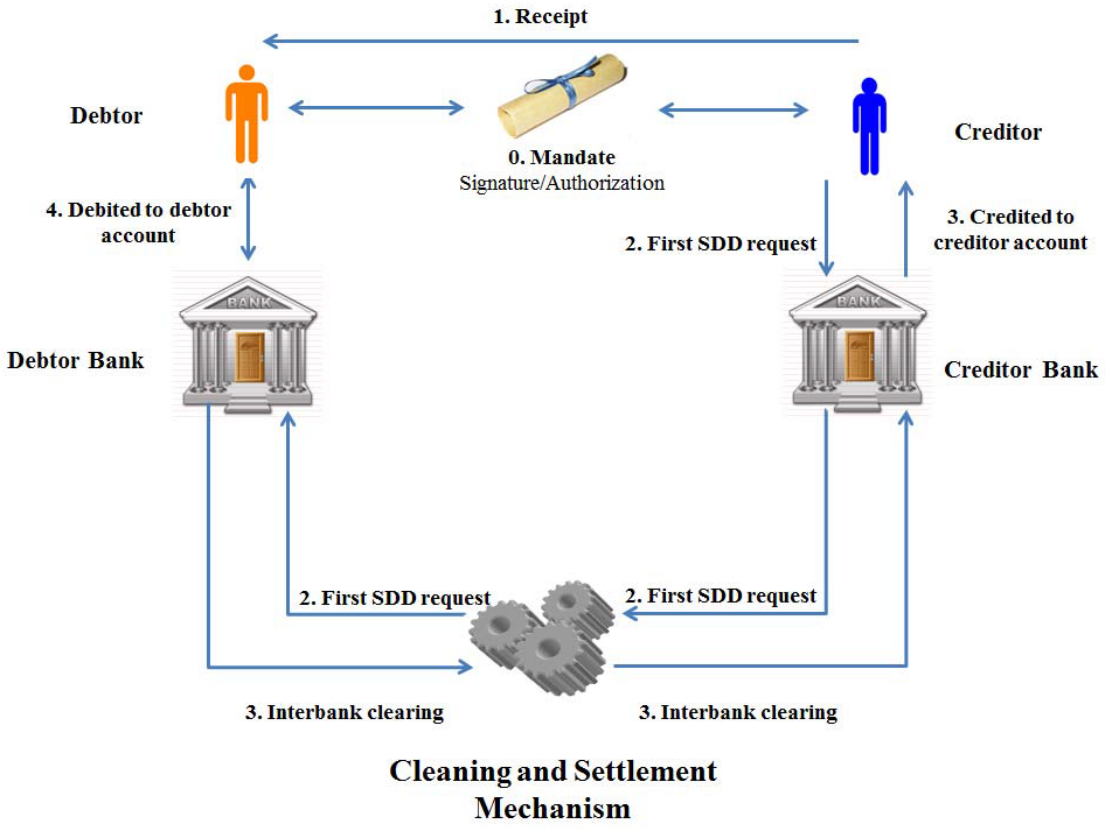


Figure 2 SEPA Direct Debit process [11]

There are other similar payment systems that rely on banks to exchange money such as the SWIFT or local direct payments between banks. In principle these systems are similar and thus are not covered here.

2.1.2 Mobile Payments

Mobile payments are seen as a sub-category of e–payments where during a transfer of funds the mobile phone is involved in both the initiation and confirmation of the payment [11]. Mobile payments engaged by internet companies are a promising alternative to less developed countries because of their non-reliable bank structures [11].

2.1.3 P2P Payments

Peer-to-peer payments are instant money transfers via a service provider where the money is sent from one account to another where the service provider validates the payment although it might not yet have been added to the bank account [11]. This payment system requires an intermediary such as PayPal to make the transaction [11]. Another known P2P transaction company is Wise, formerly known as TransferWise.

2.1.4 Card Network

Card network payments are the most commonly used payment method worldwide [13]. Nevertheless, card frauds are an easy cybercrime target because a significant amount can be withdrawn without the owner's knowledge [13].

There are exists multiple card networks, the most widely known of them are Visa, Mastercard and American Express in the United States. A card network usually issues a credit card or a debit card to the customer. The customer can then use the card to make purchases. But while for the cardholder it is an easy way to make a purchase, there is a complex system behind the scenes that involves many entities.

As shown in Figure 3, the card payment flow consists of a series of steps. First, the card holder enters the card details on the merchant internet page, secondly the merchant requests authorization of the card, thirdly, the bank sends the authorization request to the card issuer and then, the card issuer accepts or refuses the transaction [13]. After the response, the bank sends the response to the merchant who then completes the transaction if the authorization request was accepted [13].

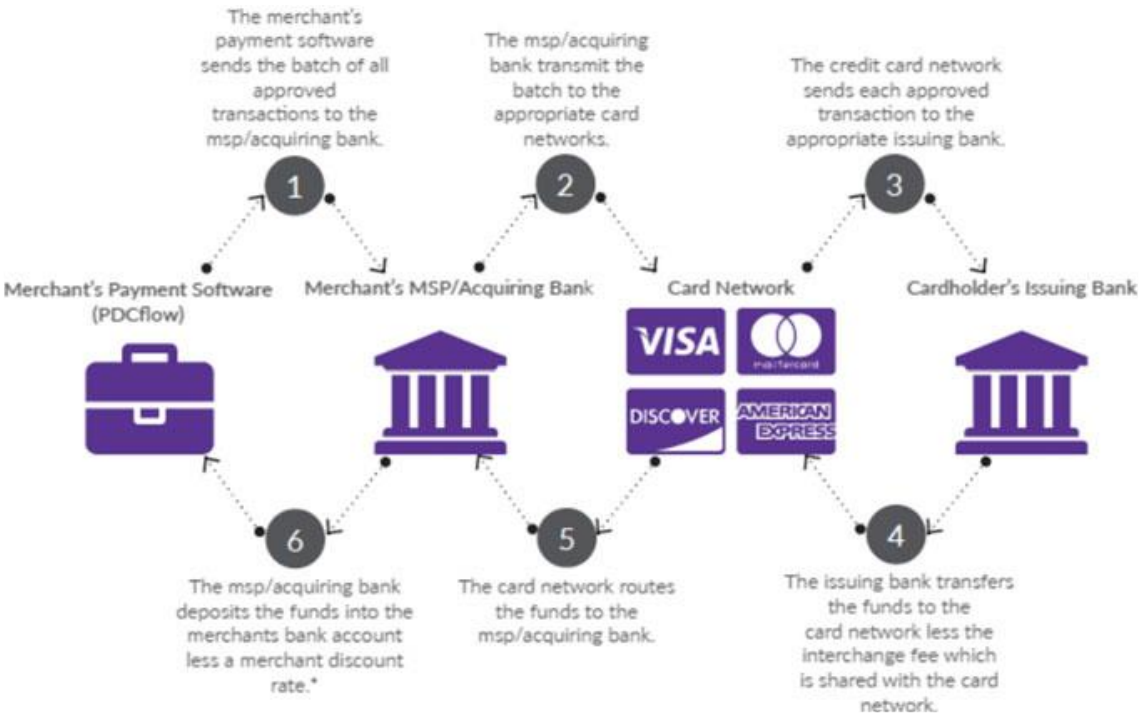


Figure 3 Card transaction validation flow [13]

2.1.5 Digital Wallet

Digital wallet is a digital storage that fulfils similar tasks as a physical wallet by providing the possibility to store identification information, cash and credit payments and storing tokens such as vouchers and bus tickets [11].

2.2 Blockchain

Blockchain is a tamper evident and tamper resistant digital ledger which can work without a central repository and a central authority [14]. This provides the community of users to record transactions in a shared ledger and no transaction can be changed once it is published [14].

2.2.1 Blockchain Categorization

Blockchain networks are categorized based on their permission model [14]. Permission model determines who maintains the public blocks [14]. There are two kind of networks based on this categorization - permissionless and permissioned [14].

Permissionless blockchain networks are decentralized and open to anyone to publish new blocks without the need from an authority [14]. Usually permissionless blockchain

platforms are open source and freely available as anyone can read and write to the blockchain [14]. In order to prevent malicious users to publishing blocks that subvert the system, a consensus mechanism is utilized which requires users to expend or maintain resources [14]. Examples of permissionless consensus mechanisms include proof of work and proof of stake [14].

Permissioned blockchain networks require users that publish new blocks to be authorized by some sort of authority [14]. This allows the mining of a new block to be much less expensive computationally since there is no need to waste resources on picking the miner [14]. On the other hand, permissioned blockchain user needs to have trust in the entity that controls who can publish new blocks and hence diminishing the decentralization aspect of the system [14]. Permissioned blockchain networks are used when the blockchain needs to be more tightly controlled and protected by the organization [14].

2.2.2 Consensus Mechanism

Consensus mechanism is one of the most important aspects of a blockchain implementation. Consensus mechanism declares the properties of the blockchain implementation and thus orchestrates how the specific blockchain implementation works.

Consensus properties can be divided into four major groups such as structural properties, block & reward properties, security properties and performance properties [15]. Structural properties define how nodes are participating in the network [15].

Block and reward properties are useful to differentiate cryptocurrencies in quantitative way [15]. They do not characterise different consensus mechanisms directly but do have an impact on how a consensus is achieved [15]. Block and reward properties include the genesis date of the first block, block reward for creating a new block, total supply when dealing with a cryptocurrency and block time which represents the average time to create a new block [15].

Security properties include authentication, non-repudiation, censorship resistance and attack vectors [15]. A consensus algorithm must satisfy all of these properties [15]. Attack vectors imply attack vectors applicable to a consensus mechanism [15]. There are attack vectors that are applicable to all consensus mechanism such as adversary tolerance, Sybil protection and Denial of Service (DoS) resistance [15]. But there are also attack vectors

that apply only to some consensus mechanisms [15]. Performance properties include fault tolerance, throughput, scalability, latency and energy consumption [15].

Consensus mechanisms can be grouped as incentivised consensus models, which include Proof of Work, Proof of Stake and Hybrid Consensus mechanisms [15]. Another group of consensus mechanisms are non-incentivised consensus mechanisms that are primarily used in private blockchain systems and are not suitable for cryptocurrency application [15].

Proof of work consensus mechanism works in way where publishing a new block requires a resource-intensive computational task. This enables the possibility of transactions between untrusted parties as it requires more computational power to attack the system. More than 51% of the computational power is required to attack the system [14]. The disadvantages of PoW are that it is computationally intensive by design, thus having a large power consumption and it induces hardware arms race [14].

Proof of stake enables a less computationally intensive barrier to publish new blocks by enabling the stakeholders control the system [14]. But the downside is that nothing prevents the formation of a pool of stakeholders to centralize the power [14]. 51% attack is possible in case of enough financial power instead of computational power as was the case with Proof of work [14].

There exist many more consensus mechanisms that are not discussed here [16] [17] [18]. Whereas proof of work is inherently the most secure consensus mechanism but overall the trend is that in order to have faster performance by creating more blocks in the same time some kind of trade-offs must be made usually in the security properties of the blockchain implementation.

2.2.3 Blockchain Components

Blockchain technology utilizes many well-known computer science mechanisms such as cryptographic hash functions, cryptographic nonce, transactions, asymmetric-key cryptography, addresses, ledgers and blocks [14].

Cryptographic hash functions are used to create addresses, unique identifiers, securing the block data by hashing it and storing it to the block header, securing the block header by hashing it and publishing it within the next block's header [14]. When the block header

includes a hash representation of the block data, it is secured because the block header digest is stored into the next block [14].

Cryptographic nonce is a random number that is used once which is combined with data to produce different hash digest for the same data [14]. The cryptographic nonce is utilized in the proof of work consensus model [14].

Transaction is a representation of interaction between different parties [14]. One block can contain zero or more transactions [14]. For some blockchain implementations it is important to create new blocks even if they are with zero transactions in order to maintain the security of the network [14]. The transaction data can be any information but the mechanism typically works the same way by having inputs and outputs [14]. The inputs consist of the list of digital assets that are transferred, usually referencing the source of the assets and the proof of access in the form of a digital signature which is signed by the private key [14]. Outputs include the account identifiers that will receive the assets, how much these accounts will receive and might include a set of conditions the new owner must meet to spend the received value [14]. The authenticity of the sender's access to the assets is proven by the digital signature that is created by the sender's private key which can at any time be verified by the associated public key [14].

The asymmetric-key cryptography which is also known as public key cryptography is used to digitally sign transactions and verify signatures generated with the private keys, public keys are also used to derive addresses and the asymmetric-key cryptography mechanism overall gives the ability to verify that the user who is in possession of the private key is capable of signing the transaction [14].

Addresses are used to declare where to and from the assets are sent during a transaction. Each blockchain implementation may have a different method to derive an address, but usually it is derived from the network user's public key along with additional data such as version number or checksums and is then hashed with a cryptographic hash function [14]. The digest of the hash is the address.

The collection of all the transactions is called a ledger [14]. In the beginning, pen and paper ledgers have been used to keep track of the exchange of goods, more recently they have been stored digitally in large conventional central databases [14]. Blockchain

technology enables the ledger ownership and physical architecture to be distributed by using a large set of computers that have backups around the world [14].

Blockchain network users submit transactions to the network via software which in turn sends the transactions to a node within the blockchain network [14]. The submitted transactions are then propagated to the other nodes and once a publishing node adds the new transactions to the blockchain, the new block is created [14]. The other nodes will check the validity and authenticity of the transactions in a published block and will not accept it if it is invalid [14]. Different blockchain implementations require different number of validations in order for the block to be regarded as valid.

2.3 Cryptocurrency

The first cryptocurrency that was presented to the world was Bitcoin. Since then there have been developed large numbers of other cryptocurrencies which are all called collectively as altcoins – meaning alternative coins. There is third way of classifying cryptocurrencies – stablecoins. Stablecoins are usually tied in value with some form of traditional financial assets in order to alleviate the price volatility. Cryptocurrency payment gateways are a new technological development that aims to provide access to traditional payment gateways while using cryptocurrency.

2.3.1 Bitcoin

Bitcoin was first published to the world in a white paper by the pseudonym Satoshi Nakamoto in the year 2008 [19]. Bitcoins advantages over the traditional payment systems include anonymity, transparency, independence from central banks, operational efficiency and trust [19].

Bitcoin is a decentralized peer-to-peer payment system and a digital currency which uses the blokchain proof of work consensus mechanism [20]. It does not have a central repository, server or a central administrator for transaction processing [20]. Payments are recorded in the public ledger which is available for all users [20].

Today’s trading relies on financial institutions who act as trusted third parties for electronic payments processing [20]. Bitcoin was proposed as a solution to leave out the third party by solving the double spending problem with using peer-to-peer distributed

servers with a time stamp and creating a chronological order of transactions with a proof using digital signatures and hash functions [20]. The assumption is that the system is safe as long as the honest nodes have more processing power [20].

While in paper Bitcoin transactions seems to solve all the problems that traditional payment systems have, in reality the situation has evolved to be different and there are multiple problems with Bitcoin. Problems include lack of knowledge on how to use cryptocurrency, volatility, exchange instability, lack of government regulation, slow transaction speed, restricted use case because of infrastructure limitations, storage problems where losing a secure password means that the asset is gone forever [21]. Currently Bitcoin has high volatility which prevents to place a correct valuation for goods and services [22].

Although Bitcoin is by far the most well-known cryptocurrency, [23] found that there is only a small number of users who use bitcoin as a medium of exchange and it is mostly considered as a speculative investment instead of an alternative currency [23]. According to [24], Bitcoin transactions cover only a negligible proportion of all global transactions and Bitcoin is used as a medium of exchange in a small domain [24].

2.3.2 Altcoins

Since the socio-economic success of Bitcoin there have been introduced thousands of different cryptocurrency implementations. All of these implementations are collectively called altcoins.

Many altcoins have made changes to the Bitcoin blueprint to meet its gaps and create a superior cryptocurrency but not all of the implementations have had genuine intentions [25]. Because of the market hype there are many implementations that look to make a quick profit from the situation.

Some of the more known genuine altcoins include Litecoin (LTC), Bitcoin Cash (BCH), Bitcoin Gold (BTG), Zcash (ZEC) and Ether (ETH) [25].

Litecoins main difference is a shortened block time from 10 to 2,5 minutes in order to increase the networks transactions limit [25]. This comes with a cost of having more orphaned blocks which means that blocks which have been solved by miners but have not been chosen as the continued path are not getting rewarded [25].

Bitcoin Cash is a fork from the original Bitcoin blockchain that aims to solve its scaling problems by increasing the block size from 1 megabyte to 8 megabytes which allows the amount of transactions that take place within the 10 minutes to increase eightfold [25]. Critics argue that this leads to greater centralization as larger blocks require greater work which concentrates the mining process to larger nodes [25].

Bitcoin Gold is another fork which changed the mining hash from 'SHA-256' to 'Equihash' in order it to be ASIC technology resistant so that more users can mine Bitcoin Gold more fairly as the ASIC miners have created a market monopoly because of its expensive equipment prices [25].

Zcash differs from Bitcoin by having a shorter block size from 10 minutes to 2.5 minutes, but the key fundamental difference is that Zcash uses zero-knowledge proofs in order to hide transaction values which in turn increases the privacy of the transactions [25].

Ethereum network is powered by the currency Ether and is significantly different to Bitcoin [25]. Ethereum uses the blockchain concept to power a Turing-complete virtual machine which can process codes and scripts [25]. This allows for smart-contracts which offer mathematically binding agreements which [25]. Because of this, in addition to the functionality of being a currency, Ethereum offers functions other than currency as well [25]. Similarly, to Bitcoin, the before mentioned and also a lot of other altcoins still have the issue of being extremely volatile in comparison to fiat currencies.

2.3.3 Stablecoins

Because of the high volatility issues with traditional cryptocurrencies, stablecoins have been introduced to the market which have a stable value by being tied to another asset [26]. Stablecoins incorporate the benefits of traditional cryptocurrencies, such as immutability and the security of transactions while addressing the issue of volatility [27].

In terms of market capitalization, the four largest stablecoins are Tether (USDT), USD Coin (USDC), Paxos Standard (PAX), TrueUSD (TUSD) [28]. These stablecoins meet all the requirements to be defined as cash equivalents by the International Accounting Standards Board 2017 (IAS 7) although the existing International Financial Reporting Standards Foundation (IFRS) rules do not allow fiat-backed stablecoins to be reported as

cash because stablecoins are not a generally accepted medium of exchange in which financial statements may be created [27].

2.3.4 Cryptocurrency Payment Gateway

[29] provides a system design shown in Figure 4 which enables to buy services and goods with cryptocurrencies through traditional payment gateways.

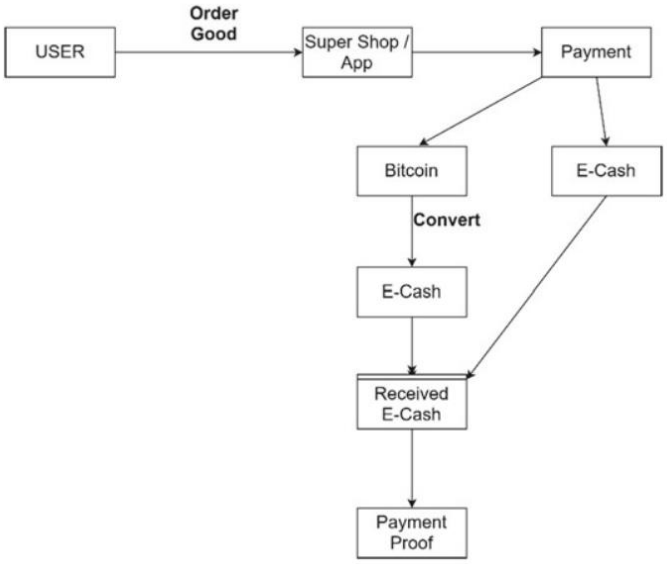


Figure 4 Cryptocurrency Payment Gateway [29]

Mastercard and Visa have already started to use a similar approach [7] [8]. This gives the opportunity for customers to pay with cryptocurrency in the global card network infrastructure.

Fundamentally this approach introduces more commission fees for the customers because in addition to card network commissions there are added cryptocurrency transaction fees and also cryptocurrency to fiat currency exchange fees. Instead of a simplified system with less intermediaries this approach introduces more complexity and intermediaries.

To leverage the cryptocurrency advantages it should be used directly as a peer-to-peer payment system.

3 Case Study Design

Case study research design was chosen due to the explorative nature of the given research topic. The design of the research follows guidelines that are provided by the book “Case Study Research in Software Engineering [30]”.

Case study provide a deeper understanding of the topic that is researched [30]. This aligns with our goal since existing literature proposes different problems that can be attributed to the low usage of cryptocurrencies. Our aim is to understand, by observing the patterns, as to why cryptocurrencies are used so little compared to traditional payment methods.

Because of the exploratory nature of the topic, inductive research was conducted. Inductive research means that the researcher first observes, then identifies patterns from the observations and from the emerged patterns sets up hypotheses and relates them to existing theory or proposes a new theory [30].

3.1 Research Questions

Research questions were formulated taking into account the research objectives which were introduced in Chapter 1.3.

One central research question was created which is answered through three sub research questions. Sub research questions were created by taking into account the research objectives. Each of the three sub research questions, that collectively answer to the main research question, have their own sub research questions. This results in a three level structure. All the sub research questions that are on the same level collectively answer its parent research question.

- How to replace traditional payment methods with cryptocurrencies at a large scale?
    - How are cryptocurrencies used compared to traditional payment methods?
        - What are the main use cases for cryptocurrency transactions?
        - What are the main use cases for traditional payment methods?

        - When will cryptocurrency start replacing traditional payment method use cases at a large scale?

    - How cryptocurrencies stay behind compared to traditional payment methods?

        - What are the advantages of traditional payment methods in comparison to cryptocurrencies?

        - What are the disadvantages of cryptocurrencies in the context of traditional payment methods?

    - How to increase usage of cryptocurrencies as a payment method?

        - What are the blockers for cryptocurrencies being used as a payment method?

        - What is the order of significance of the cryptocurrency blockers?

        - What can be done to overcome the blockers of cryptocurrencies?

3.2 Case and Subject Selection

Embedded case study was used as the underlying design for the research. Embedded case study is suitable when there are multiple units to analyse within a case [30]. Our objective was to link the knowledge between cryptocurrency and traditional payment methods. Thus we require subjects that must be knowledgeable in both of these domains. Hence traditional payment methods and cryptocurrencies were handled as a single case but in separate units of analysis.

Interview method was chosen which follows a semi-structured format in order to use the advantages of both structured- and unstructured interview methods.

Multiple subjects were interviewed in order to develop patterns from the resulting data. The sample size for the subjects is 8. The sample size is small because the required deep knowledge of the case is not something that is often found in the general population. Subjects were picked on the condition of having strong exposure to both the traditional

payment industry and cryptocurrency domains. Subjects that demonstrated strong knowledge in one field and lesser knowledge in the other were also considered.

We contacted universities, payment service provider companies, blockchain companies and banks to find knowledgeable subjects. Once we had established a connection to a valid subject or an organization, we asked to recommend other potential subjects who are knowledgeable in the field. With this technique the Estonian cryptocurrency specialists who were potential subjects started to recur with just two iterations. Some subjects were not from Estonia which proved very useful to forming a global perspective. Table 1 provides an overview of the interviewed subjects education and experience related to the field of finance and cryptocurrency or blockchain.

Table 1 Case education and experience

Name	Education	Finance experience	Cryptocurrency/Blockchain Experience
Subject 1	PhD degree from Tallinn University of Technology with the focus on cryptography.	-	10 years.
Subject 2	Master's degree in Theoretical Physics from University of Tartu.	30 years.	2 years.
Subject 3	PhD degree, information system, TU-Eindhoven	11 years.	11 years.
Subject 4	Tallinn Polytechnic school, IT systems	10 years.	8 years.
Subject 5	Master's degree in business and economics from The University of Edinburgh	14 years.	5 years.

Subject 6	Master’s degree in economics and management from University of Oxford, Master’s degree in art, business from Sotheby's Institute of Art in The University of Manchester	6 years.	6 years.
Subject 7	Master’s degree in Informatics from Tallinn University of Technology	-	4 years.
Subject 8	Master’s degree in Business Administration from University of Amsterdam	-	5 years.

3.3 Data Collection Procedures

Data collection was done in two steps. First, the necessary concepts and related works were analysed in order to get into a position where we could be knowledgeable to direct the interviews in the direction that the subject had insight. Secondly, the main data collection was done by interviewing the subjects.

The interview was conducted via online video call platform Google Meets [31]. Google Meets was chosen as it does not require the subject to have an account and could connect to the video conference call just by receiving a http link.

The interview followed a semi-structured format where the structured part consisted of the third level of sub research questions that were discussed in Chapter 3.1. The unstructured part consisted of questions that were asked on the go, depending on the structured questions answers.

The interviews were recorded using OBS Studio [32]. OBS was chosen since it is freeware, easy to use and was already familiar for the authors.

3.4 Analysis Procedures

Thematic analysis method was used in order to analyse the gathered data. Getting more acquainted with thematic analysis can be done here [33] and here [34].

The data analysis consists of four steps which were done in the same order: transcribing, thematic division, developing hypothesis, relating hypothesis to existing body of knowledge.

Qualitative data analysis tool NVIVO [35] was used in order to transcribe the data. NVIVO was selected because of the strong recommendation by the supervisor. Thematic division was also done with the functionality provided by the NVIVO tooling.

Thematic data analysis was done in two steps. First, the data was divided into thematic codes which relate to research questions as shown in Appendix 3. Secondly, the data corresponding to each research question was further divided into sub-codes. The sub-codes were created using thematic division as shown in Appendix 4.

Hypotheses were generated from the thematic division of the results. These hypotheses were then related to the existing body of knowledge.

3.5 Validity Procedures

In order to minimize bias, triangulation method was used which means that several interviews were conducted. Once the results start to repeat within different subjects, it means that the data is validated and exhaustive.

Some methods that were introduced by the book “Case Study Research in Software Engineering” were also used [30]. The draft case study design was reviewed by peers external to the project [30]. A pilot study was conducted to evaluate the case study design [30]. The actual progress of the case study was constantly reviewed against the planned progress in order to determine if there were any significant differences [30]. Significant differences were not found but we were flexible for changes should it been the case.

4 Results

Case study results are discussed in this chapter. First, the results are categorized and analysed in three sections. Each section corresponds to one of the sub research question of the main research question. The fourth chapter discusses the evaluation of validity of the results.

4.1 Cryptocurrency Usage Compared to Traditional Payment Methods

Results are first categorized and discussed via the sub research questions and finally a conclusion is provided as a whole.

4.1.1 What are the main use cases for cryptocurrency transactions?

Subject 1 thought that in theory it should be payments and especially automated payments due to smart contracts but in practice it seems to be mostly speculation.

Subject 2 adds that it depends on a currency. If a currency looks like a digital gold, then in this case the purpose is accumulating and saving, like Bitcoin. But in case of volatile currencies the main use case is speculation, kind of gambling.

Subject 4 mentions speculation and investment. Though he argued that this is not a problem as with conventional money over 90% of the transactions are related to Wall Street products and financial derivatives and only less than 10% are actual transactions.

Subject 3 describes that the main use case for cryptocurrencies is to make it possible for a fair banking system where free market economy transactions are possible unlike the current banking system where every step is heavily monitored and in control of the central parties.

Subject 5 explains that there is potential for utilization in the near future for larger volume transactions such as 50 000 dollars that is sent between different regulated regions internationally. This model will be competing with traditional models such as the SWIFT network which costs 35 dollars per transaction, takes 3-5 days and during this period there is no proof that the funds are transferred to the right destination. Blockchain solves for these issues. Potentially using CBDC’s if they are interoperable but that is a problem

because a lot of the CBDC's are built either on different chains or are not on the blockchain to begin with.

In addition, Subject 5 argues that over 50 % of tokens in proof of stake networks are staked and they earn rewards. Thus people are better off leaving these tokens to earn yield than spending them. Subject 5 adds that cryptocurrency transactions are used in web 3 native ecosystems. For example, NFT trading platform Opensea where it is easier to link a wallet address than it is to pay with a card network. Since the NFT that is purchased is going to be held in the same cryptocurrency wallet, this also acts as a bonus for the cryptocurrency ecosystem. Subject 5 described that the purpose of having a cryptocurrency wallet is more than just using it as a payment method. It is also meant to be a custodian of identity and a custodian of assets. In some ways the wallet should be viewed as a potential competitor to the bank. Not the end payment method that is assigned to it.

Subject 6 said that number one cryptocurrency use case is cross border settlement which is faster and cheaper than traditional payment methods. Transparency is also helpful from a compliance perspective although not all regulators and compliance people see it like that. Thirdly it enables peer to peer commerce more easily. Subject 6 added that although these are the use cases, they are currently not widely used.

Subject 7 ranks the use cases from more widely to less widely used as following: investment, peer-to-peer transactions and the purchase of goods and services.

Subject 8 describes ICO's as one of the use cases which technically require the developers to follow less regulation compared to IPO's. Subject 8 adds that for most people, the key use case is speculation where people buy and trade cryptocurrencies to get rich quickly. But in some cases also investment and diversifying assets. Subject 8 also argued that cryptocurrencies are an important use case for countries like Venezuela where there is hyperinflation and no way to send money abroad without paying 30% or more to the government. For countries where the local money is not stable and the people are not allowed to use other currencies either, cryptocurrencies are used.

4.1.2 What are the main use cases for traditional payment methods?

Subject 2 mentioned paying for services, receiving salary. Subject 6 mentioned the facilitation of ecommerce.

4.1.3 When will cryptocurrency start replacing traditional payment method use cases at a large scale?

Subject 1 described that cryptocurrencies will start replacing traditional payment methods when they are cheaper and faster. But could not specify whether it will happen the next year, after 10 years or never.

Subject 2's thinking is that cryptocurrencies will start replacing traditional currencies when governments will start to accumulate taxes in cryptocurrencies. Subject 2 argues that this is a definition of an official currency.

Subject 3 argues that it is happening already in multiple domains. For example, in the oil business a lot is moving into the crypto space and there are different types of tokens for different types of purposes. Subject 3 added that Bitcoin and Ethereum is replacing the dollar in international trade settlements although this is something that will not be heard about in mainstream media outlets which do not reflect the truth. The Iranians, transacting with their oil, soon the Russians, Chinese and many more people are getting off the dollar as an international currency of trade.

Subject 4 also agrees that the cryptocurrency is replacing traditional payment methods already in some cases such as in El Salvador where Bitcoin is a legal tender and also Venezuela. This is mostly occurring in developing countries where the local money is in a bad situation and there exists a high level of corruption. Subject 4 adds that in the remaining countries cryptocurrency will replace traditional payment methods as soon as the traditional money collapses. Subject 4 states that this is going to happen quite soon.

Subject 6 agrees that the adoption of cryptocurrencies is happening quite rapidly. The volume of transactions that went through the Ethereum network in 2021 is close to what went through the Visa network. The expectation is that the adoption curve slows over the next 18 months because of regulatory uncertainty. After that the growth curve sharpens again. Wide spread adoption is expected by the end of the decade.

Subject 5 claims that cryptocurrencies will not replace traditional payment methods. Cryptocurrencies are a store of value and act much more like a security rather than a payment method. Cryptocurrencies will succeed natively in web 3 environment where tokenomics play a key part. Potentially having the ability to earn tokens with governments and utility tokens aligned with them. Coupled with usage, loyalty or other mechanism that essentially allows those tokens to be appreciated in value or, the number of tokens issued to any individual uses it, to increase them as well. Subject 5 also argues that if a person in the United States stores a 100 000 dollars in the bank, he has the money covered even if the bank goes out of business so there is no point to store it in a stablecoin such as USDC. But for a person in Argentina, where the Peso's inflation rate is 60%, it is beneficial to store his value in USDC. It cannot be looked at purely as a global play. It has to be looked through the local environment from the regulatory and economic perspective.

Subject 8 thinks that there is less of a need to replace the existing currencies in the first world countries. There is constantly a threat on the horizon where the inflation is going up and at some point it is going to cause hyperinflation. Some libertarians are saying every year that the dollar and euro will go bust next year. So far it has not gone bust because of the experimental counter steps, such as negative interest rates, done by the central banks. As long as traditional currencies do not fail, most people are happy with dollars and euros. Currently there is not a solid reason as to why people should start using cryptocurrencies instead of regular currencies because the traditional payment methods are very well integrated and easy to use for normal people. People trust regular currencies more. Cryptocurrencies are seen as volatile. There is also the risk of losing the cryptocurrency in case of wrong usage or losing the keys. Handling the cryptographic keys properly is too much for a regular person to handle because their usual banking system works so conveniently.

4.1.4 Conclusions

The interviews clearly indicate that currently the number one use case for cryptocurrencies is speculation. Another use case is cross-border payments where larger sums are transferred as this is already cheaper and faster compared with the current traditional systems such as SWIFT. Cryptocurrencies are also used for store of value rather than a payment method. It is clear that currently cryptocurrencies are not used

primarily as a payment method although they could be if some of the problems would to be eliminated.

There were two main directions of thought as to when cryptocurrency will start replacing traditional payment methods at a large scale. One direction of thought was that this process is already happening in third world countries where the current monetary system is unreliable and also in developed countries in some domains. The second direction of thought is that cryptocurrencies will never replace traditional payment methods especially in the first world countries unless the current monetary system fails.

4.2 Cryptocurrency Shortcomings Compared to Traditional Payment Methods

Results are first categorized and discussed via the sub research questions and finally a conclusion is provided as a whole.

4.2.1 What are the advantages of traditional payment methods in comparison to cryptocurrencies?

Subject 1 described that aside from the speed and the lower cost for end users, many users do not fully appreciate the safety networks that a banking system provides. If there is a fraudulent transaction in a traditional banking system, then at some cases the end users lose their money. But usually fraud protection from the bank either blocks the transaction or if it does not block the transaction then reimburses the client for the fraudulent transaction. There is nothing like it in cryptocurrencies currently. Many people do not understand what it means that cryptocurrency transactions are final and irreversible. In the case of making a mistake in entering transaction details or having a security lapse where someone takes over the wallet and spends all the funds, there is no authority to return to complain, in order to revert those transactions.

Subject 2 said that fiat currency ratio is more stable than cryptocurrencies. The infrastructure of traditional payment methods is more advanced. Non-anonymity is a positive property of traditional payment methods. When transacting with cryptocurrencies it is not known who is doing what and this is a potential way to engage in crime. Money circulation should be transparent, meaning that it should be protected with KYC (know your customer).

According to Subject 3 “Police and military will not show up at your doorstep. That is the advantage, otherwise I do not see any advantage. These currencies would never survive in a real free market that is based on voluntarism and non-initiation of force. They would already have collapsed in 2008. This is when the global fiat currency financial system died. It has not come back to life. Ever since 2008 the central banks have been printing monopoly money out of thin air. And pushed it primarily in the derivatives bubble that had collapsed in 2008. At some point that scam does not work anymore. We are at this point where we have reached peak debt saturation. Whenever this happens you see weird things going on like suddenly Covid popped up very conveniently exactly the same time when the Interbank Trading Market collapsed overnight in 2019. Then we have more crisis’s getting worse and worse and getting more crazy conflict. In the end it is all about the money because the fiat money has gone bad. It died 2008, then they tried to prop it up with printing obscene amount of trillions out of thin air. Now even that scam does not fly anymore, it has become so dysfunctional and now you see that once it collapses the mainstream banks who are responsible for the debt are banning people right and left. Not just the banks but the media and on and on. It is all connected, a make belief system. They are trying to hide it with conflicts and epidemics that do not truthfully exist.”

Subject 4 mentioned stability and acceptance as advantages of traditional payment methods.

Subject 6 described ease of use and the fact that traditional payment methods are now very well understood and embedded in technology that enables merchants and consumers to use them very easily. Because they have been around a very long time and most are well embedded in to the consumer market today there is a high degree of trust in those payment methods which is important for consumer adoption. Many but not all traditional payment methods have sophisticated mechanisms around fraud and chargebacks that have consumer protection built into them whereas most cryptocurrency systems today do not. A lot of the advantages today for traditional payment methods lie in consumer protection and trust.

Subject 7 said that traditional payment methods are more mature, they have been around longer, they have been integrated better to the current economy. Whether a person wants to take out a loan or pay for services, it is more convenient.

Subject 8 argued that for most people traditional payment methods are familiar. They are integrated in so many places. Traditional payment methods have support mechanisms for the government in order to seize assets and do surveillance. Currently surveillance can be done on most of the cryptocurrencies as well but if the user is clever or if there is a lot of good privacy technologies then in principle blockchain can become invisible for the law makers. Another advantage is that when losing access to the funds, it can be easily recovered when the person shows up with his passport to the bank.

4.2.2 What are the disadvantages of cryptocurrencies in the context of traditional payment methods?

Subject 2 said that if a person fails to understand all the aspects of security related to cryptocurrency then probably he will be a victim of some kind of crime related to cryptocurrency.

Subject 4 thought that the disadvantages are volatility, acceptance and learning curve.

Subject 5 described that most cryptocurrencies are not actually very suited for transactions either the way that they are built on chain and the capacity of those chains. The recourse and the features for both customers and merchants are limited. For example, there is no option to do recurring transactions, there is no easy way to refund users. The other side is the incentives. Using Visa card, the customer gets 2% cashback rewards but for example when using SOL (Solana) the user loses the ability to stake that SOL and potentially earn 10% annual percentage yield. Currently the whole industry is not directed towards cryptocurrencies being used for transactional purposes. At least not in a retail sense.

Subject 6 explained that for non-stable coins there are issues around volatility and for some chains there are issues around transaction costs. For both, stablecoins and non-stablecoins, availability and choice to pay with these methods is limited as not all merchants will accept them. There are some user experience challenges with obtaining and transacting in those methods. The irreversibility of almost all cryptocurrencies today does not allow for some of the consumer protection mechanisms that other payment methods allow. For a significant proportion of the population the user experience from a digital inclusion perspective is still very challenging for cryptocurrencies.

4.2.3 Conclusions

The most often mentioned advantages of traditional payment methods were fraud protection and more advanced infrastructure. Ease of use was mentioned often together with infrastructure which indicates that infrastructure is a prerequisite for ease of use. In addition, a high level of trust against traditional payment methods was considered as an advantage. Another advantage of traditional payment methods is the low volatility of the fiat currencies that are used within these payment methods.

For non stablecoins, high volatility was mentioned as a disadvantages for cryptocurrencies compared to traditional payment methods. Another disadvantage is the extensive security related knowledge a person must possess in order to manage his wallet without any risks. Low acceptance was also mentioned as a disadvantage which can be linked again to the lack of developed infrastructure. For a regular user, transacting with cryptocurrencies is too currently too complex. The learning curve is too big which is seen as a disadvantage for cryptocurrencies. The lack of refunds and other features such as recurring payments are seen as another disadvantage for cryptocurrencies.

4.3 Increasing Usage of Cryptocurrencies as a Payment Method

Results are first categorized and discussed via the sub research questions and finally a conclusion is provided as a whole.

4.3.1 What are the blockers for cryptocurrencies being used as a payment method?

Subject 1 said that the current cryptocurrency solutions do not work well as payment tools. Transaction fees are too high, transaction delays are too long, it takes too long to get a confirmation that the payment has been accepted. Given that the transaction fee in Ethereum is in the range of 10 euros but even if it were 5 euros it would still be quite high for a one-euro payment. Subject 1 also brings out lack of consumer protection, explaining that “Most people do not know how to do information security. If all your money is information, then information security is a necessary prerequisite for financial security. Already now most people do not manage their own cryptographic keys and wallets. They use a managed wallet service like some sort of exchange. Basically as those people are concerned, they are not that different from banks. In a bank you trust that bank keeps the money well and has security measures in place and does not let anybody else access the

account and spend the money. In those hosted wallet services, you have to do the same except as long as those are not legally recognised as financial service providers all sorts of customer protection laws do not apply to them. This is something that people do not realise that there is a difference between a cryptocurrency wallet and an internet banking service from a traditional or a legacy bank."

Subject 2 argued that with cryptocurrencies by definition the user has to keep his private key by himself. Losing the private key means losing the money. This is advantageous and also disadvantageous. Keeping money on a bank account guarantees that it can be recovered in case of lost credentials. In case of cryptocurrencies it is lost forever. In addition, Subject 2 described that Bitcoin is not suitable for high throughput transactions. Cryptocurrency with a high throughput is usually not based on blockchain. It uses some other consensus mechanism that is a trade-off between a distributed system and performance. Real distributed system cannot perform actually.

Subject 3 explained as a blocker that the media and the education system has kept people extremely ignorant about how money works, what money should be, what the real purpose of money is. Adding that the central banks and the governments work in an alliance. The central banks are privately owned and the public is not officially allowed to know who owns them. The ruling politicians cannot carry out their promises as they cannot raise the taxes to realize it. Instead they take bonds which enslave their people to the central banks that are privately owned. In return the central banks print new fiat currency and trade it in exchange for the bonds that enslave the people. Put simply, central banks are engaging in counterfeiting. The media and education systems are backing them up.

Subject 4 thought that the blockers for cryptocurrency usage as a payment methods are volatility, low acceptance, but also regulatory. Subject 4 added that as cryptocurrencies become more popular, it becomes a big threat to the conventional money policies which governments are tied to. One of the blockers is that the users have not realized the benefit of cryptocurrencies. They have not realized that the inflation rate is high, the censorship is high. The pain is not yet enough to change the medium of money. Learning curve is also a blocker and also insufficient anti-money laundering technologies. Technological risks might become a blocker because the technology is growing rapidly while still young compared to banking systems.

Subject 5 said that incentives are not there for people to actually go and use their cryptocurrencies to buy traditional purchases items. Other problem lies in the regulatory side. Looking at markets like China which is the largest ecommerce market in the world: there is no way that the Chinese government is going to allow a fully decentralized form of value to be used in their country. Regulators have a huge role to play either by enabling or blocking. Cryptocurrency does not support recurring payments which is a huge problem for the merchants to even consider it.

Subject 6 mentioned high volatility, bad user experience, lack of fraud mechanisms. In addition, Subject 6 explained that one issue with wider adoption is the perception issue. There are legacy feelings where cryptocurrency has illicit relation and for customers who do not own or use cryptocurrency today, that is one of the barriers of adoption. They do not trust it, are unsure of the legal and regulatory positioning and thus it is hard for them to feel confident putting their money into it. Subject 6 also argued that for some users who use cryptocurrency today prefer it using as an asset class rather than a payment method because of the volatility. Especially looking at some of the DeFi (Decentralized Finance) solutions that make it very attractive to keep wealth in cryptocurrency in terms of the yield that can be earned versus fiat currency in a bank account. Thus for more sophisticated owners of cryptocurrency using it as a payment method is less appealing. The vast energy usage is another issue that the media particularly likes to overplay. Although it very much depends on the particular cryptocurrency, overall it still has a negative impact on adoption.

Subject 7 said that the key blocker lies in regulations. Governments and the regulatory bodies are slow to understand blockchain. There has already been a lot of adoption when looking at how much the cryptocurrencies are used. But for everyday adoption there is still too much uncertainty. Stablecoins have been existing in the cryptocurrency world for a few years. Comparing stablecoins to CBDC's the technology already exists and is used daily in the cryptocurrency space but there is not enough regulation and adoption. Visa and Mastercard are using such currencies as well but there has been a push back from the regular banking. It is obvious that the incumbent leaders withstand innovation because of their own invested interests and the desire to protect their shareholder's money.

Subject 8 explained that the blockers are high volatility, no incentive to use cryptocurrencies instead of traditional payment methods, bad reputation of

cryptocurrencies, cost of integration for merchants, high transaction cost and the “backup problem” where losing the private key means losing the asset.

4.3.2 What is the order of significance of the cryptocurrency blockers?

Subject 1 said that transaction cost and speed are the main issues. These issues are being solved by using level 2 protocols which take the technical solution closer to a traditional bank compared to the original idea of directly blockchain based solutions. When these barriers get resolved then the security issues start to be even more important. Currently big amounts of cryptocurrencies are handled by investors and it is bad when the investment is lost. But if a person would receive his monthly salary into a cryptocurrency platform and lose it and thus is not able to buy food or pay rent the next month than this is much worse. Such issues get worse as more common people start using cryptocurrency and this will happen as the speed and cost of transactions get resolved.

Subject 2 names the regulations issue as the biggest problem, Secondly throughput and thirdly the secret key vulnerability issue.

Subject 4 orders the blockers from the most important to least important as people’s usage habits, regulation issues, complexity of the learning curve, technical risks, anti-money laundering risks.

Subject 6 explains that reputation is number one cryptocurrency blocker. Within reputation can be included legal regulatory, climate aspects and energy usage aspects as these are the ones that the media tends to talk about. Secondly comes the user experience as obtaining and transacting in cryptocurrency is too complicated. Thirdly the volatility and the preference to consider cryptocurrency as an asset class instead of a transaction mechanism.

Subject 7 said that regulation issues are the most critical blocker.

Subject 8 ranks the blockers from the most important to least important as service fee (not a case for layer 2 technologies or sufficiently big purchases), no incentive to use cryptocurrencies instead of traditional payment methods and currencies, volatility, bad reputation, cost of integration for merchants, backup problem (lose private key, lose asset).

4.3.3 What can be done to overcome the blockers of cryptocurrencies?

In the case of insufficient regulations, Subject 2 said that as soon as governments start collecting taxes in cryptocurrency then this is a good sign that regulation is in place. Subject 4 described that cooperation and education with policy makers and lobby work would help to accelerate to fix the issues with regulations. Subject 6 adds that There is a big role for public affair teams, non-governmental organizations and trade bodies to play in educating the government, policy makers and also regulators to guide the importance of it. Subject 7 proposes that having continuous and more intense collaboration within the private sector and the public sector would greatly benefit the situation and not produce so much uncertainty years later. Subject 8 brings out that in the case of Estonia, requirement to pay too much taxes because of missing investment account opportunity is a regulation problem which needs to be fixed. Governments could simplify the tax systems. Platforms that are used for buying and selling cryptocurrencies could automatically integrate with the government systems so that the users do not need to report their taxes manually.

Subject 1 commented about the transaction fees and throughput problem that there are cryptocurrencies that claim to provide better response time but most of them are in development and experimental stage. Most of them are not used widely. So it is hard to tell if any of them will be able to deliver if they get more popular and whether the transaction fees will indeed stay low in the face of more pressure to process more transactions. Subject 2 thought that the solution is some kind of different technology which will not be based on proof of work. It is necessary to make compromise with the proof of work consensus mechanism. Subject 8 said that in principal systems like the Lightning network in the case of Bitcoin should fix the scaling issue and thus the service fee issue.

Subject 1 believes that the answer in resolving security issues lies in social or economic, not so much technical domain. In security purely technical solutions hardly ever work. It always has to go together with either a legal framework or at least user education. Pretty much any security that is based on user education is largely doomed because majority of users do not want to be educated. As cryptocurrency gets more mainstream it will be regulated one way or another and be under the same consumer protection laws as the banks are currently and have to charge service fees to cover their costs of protection services or insurances, however it gets resolved from the service provider side. In the end

cryptocurrencies become more and more like traditional banks at least as far as payment processing goes. Subject 2 thought that a solution to lower the risk of losing the private key is to open a cryptocurrency account on a bank but in this case using cryptocurrency is exactly the same as using a normal bank account for the client which defeats the whole purpose of cryptocurrency. Subject 8 said that the most decentralized solution is where you make your key into multiple shares and where you would need only three shares from the total five to recreate the key. The easier solution for most people is to keep their cryptocurrencies in a bank or an exchange. But in principle this is against the idea of cryptocurrencies.

Subject 1 thought that the safety mechanisms to fix lacking consumer protection can technically be implemented. The question is whether those people who like cryptocurrencies because of the lack of intermediation and lack of censorship would like it. There is going to be some religious war around this. If an existing cryptocurrency platform starts doing something like that then some people who are fundamentalist might leave the platform because for many people, the purpose of using cryptocurrencies is that they cannot be censored and transactions cannot be reversed. It will involve adding some sort of intermediaries into the transaction processing chain which currently lacking is the primary selling point of cryptocurrencies. Subject 5 had a similar point of view and said that The European Union is trying to normalise and bring cryptocurrencies towards normal payments by having every cryptocurrency transaction to go through KYC. That is an asset test for the industry. Because either the purists who like the idea of self-custody will comply and cryptocurrencies will suddenly move a lot closer to traditional payment systems such as Visa or they will push back and the cryptocurrency will start moving back towards the dark web. These ecosystems might end up existing both side by side, but the key point is that one will be a very regulated environment using the payment methods we are familiar with and the other one will be unregulated, uncontrolled, unbacked way to store value. Subject 4 thinks that regulation can help this issue to be resolved.

Subject 8 mentioned about the issue of volatility that once a cryptocurrency such as Bitcoin becomes sufficiently large the volatility should go down automatically. Other option is that to suppress volatility there is in need for a central bank to systematically buy and sell the cryptocurrency. Subject 6 also said that there is a possibility that some

cryptocurrencies themselves will reach sufficient size and scale that their price volatility significantly reduces.

Subject 4 thought that the blocker of insufficient incentives to use cryptocurrencies is related to the pain or struggle of using a conventional money has to become bigger for people to change their habits to using cryptocurrencies. Subject 6 said that the media and particularly government policy media relations have done quite a lot to damage the reputation of cryptocurrencies. Creating a more positive media image is helpful to dispel some of the myths why people do not perceive cryptocurrencies as being beneficial. Better education for consumers around why there are benefits with transacting with cryptocurrencies would help as well. Subject 8 thought that the issue around cryptocurrencies reputation is getting better over time. In addition, press campaigns would help such as articles online and famous people like Elon Musk talking about cryptocurrencies in a positive tone.

4.3.4 Conclusions

The most important blocker lies in insufficient regulations. The reason why these regulations are slow to evolve is because for the banks and governments there is a conflict of interest. Traditional domains that currently are in power do not want to lose their control over the monetary system. Continuous collaboration and lobby work between the public and private sector is the only hope for this issue to be resolved.

Once the problem with regulations is solved, the second most important blockers are transaction fees and throughput. These issues are currently being actively solved. The key is to have a Multi-layer hybrid architecture where validation of individual transactions can be parallelized. Individual transactions can be validated or verified independently and then the validation results would be collected by validator nodes who would form partial blocks and those partial blocks could be united into the blockchain blocks by consensus mechanism where the number of participants do not have to be so big. This kind of architecture where you aggregate individual transactions into groups can scale.

The third blocker, security issues, intensifies after the first two are solved. It involves the necessary knowledge of handling the cryptographic keys and the steep learning curve for the user. Both of these can be improved with infrastructural advancements.

The fourth blocker, lacking consumer protection, which involves the necessity for refunds, chargebacks and KYC, are also tied to the infrastructural advancements. Infrastructural advancements are in turn blocked by the insufficient regulations.

Although the security issues and lacking consumer protection blockers can be solved with infrastructural and protocol advancements, these advancements would effectively mean that the cryptocurrency would start acting a lot more like traditional payment methods and thus some of the inherent features which are currently the primary selling point for cryptocurrencies such as lacking intermediaries will be lost.

Volatility is the least important blocker. In the case that a cryptocurrency will reach at a certain scale the volatility issue will probably diminish automatically.

All of the before mentioned blockers are in part enablers for another blocker, which is a compilation of reputation, people's habits of using traditional payment methods and insufficient incentives into using cryptocurrencies as payment methods.

In the case of first world countries where the current monetary system works well, all of the previously mentioned steps might still not be enough incentive for people to start using the cryptocurrencies. In this case the enabler would probably be some features that are not available in traditional payment methods such as the native web 3 wallet integration that is already currently working with NFT's (Non Fungible Tokens) better than traditional payment methods. Another scenario is the collapse of the traditional monetary system which would enable cryptocurrencies to thrive.

4.4 Evaluation of Validity

Construct validity was achieved by using the third level sub research questions as the backbone of the interview questions. Research questions were developed based on existing knowledge. Thus we can be sure that the interview questions cover all the topics that are relevant to the issue.

Internal validity was reached by taking into account only codes that were mentioned by multiple subjects as valid results. There were a few codes that needed to be left out because of this limitation. This might indicate that because of the limited sample size possibly some issues might have not been covered in this research. Regarding

cryptocurrency blockers, the validity of sequence of the first three blockers (regulations, transaction speed & cost, security issues) were strongly indicated from the results. The sequence of the last two (lacking consumer protection, volatility) were less strongly indicative from the results.

Regarding external validity, the results cannot be generalized across all the world. The results are applicable only to the western society.

Conclusions were made only by relying on the thematic codes that emerged from the interview results. Thus the validity of conclusions relies on the unbiasedness of the interviewees.

5 Conclusion and Future Work

The main research objective of this thesis was to understand how to increase decentralized cryptocurrency usage as a payment method at a large scale. The main objective was divided into sub research objectives which can be found in Section 1.3. In order to reach these objectives, research questions that correspond to the objectives were created. Thus answering the research questions means fulfilling the research objectives.

This chapter consists of answers to research questions which are then related to existing evidence. Furthermore, the impact and implications are discussed, as well as limitations. Finally, possibility of future work is discussed.

5.1 Answers to Research Questions

In order to answer the main research question "How to replace traditional payment methods with cryptocurrencies at a large scale?" three sub research questions were answered.

The first sub research question was "How are cryptocurrencies used compared to traditional payment methods?" The answer is that currently the number one use case for cryptocurrencies is speculation in order to get rich fast. Another use case is cross-border payments which is currently the only use case that can compete with traditional payment methods offering the same service such as the SWIFT network. Overall, currently cryptocurrencies are much more used as a store of value rather than a payment method. There were two directions of thought on whether this situation will improve in the future. The first direction of thought was that in third world countries where the current monetary system is unreliable, the switch to cryptocurrencies as a payment method is already happening. Whereas the second direction of thought is that cryptocurrencies will never replace traditional payment methods, especially in the first world countries unless the current monetary system fails.

The second sub research question was "How cryptocurrencies stay behind compared to traditional payment methods?" The answer is that the advantages of traditional payment

methods currently are fraud protection, which does not exist in cryptocurrencies, more advanced infrastructure, ease of use which is tied to the more advanced infrastructure. But also high level of trust against traditional payment methods and low volatility. The disadvantages of cryptocurrencies also include the extensive security related knowledge that is necessary for a person to know in order to manage his/her wallet without risks. In addition, it is too hard for a regular user to transact with cryptocurrencies as the learning curve is too complex. Lack of features such as refunds and recurring payments are also a disadvantage for the cryptocurrencies.

The third sub research question was "How to increase usage of cryptocurrencies as a payment method?" The answer is that there are blockers that need to be solved in order to increase cryptocurrency usage as a payment method. The blockers rank from more important to less important: insufficient regulations, high transaction fees and low throughput, security issues where it is too hard for a regular user to handle his/her cryptographic keys, lacking consumer protection which includes missing refunds and chargebacks, volatility issue.

The main research question was "How to replace traditional payment methods with cryptocurrencies at a large scale?" In order to improve the current situation where cryptocurrencies are being used mainly for speculation and store of value there are specific blockers which must be solved in a specific order so that cryptocurrency usage as a payment method would increase and eventually start replacing traditional payment methods. The proposed sequence of events is shown in Figure 5.

We propose the following hypothesis: "Cryptocurrencies will start replacing traditional payment methods at a large scale when regulatory blockers are resolved"

Which encompasses several sub-hypotheses:

- "High transaction fees and low throughput will become the main blockers for cryptocurrency usage as a payment method when regulatory blockers are resolved."
- "High transaction fees and low throughput issues will be resolved with layer 2 solutions."

- “Security issues will become the main blockers for cryptocurrency usage as a payment method when transaction fees and low throughput issues will be resolved.”
- “Security issues will be resolved with infrastructural advancements.”
- “Lacking consumer protection will be resolved with infrastructural and protocol advancements.”
- “Once cryptocurrency consumer protection is sufficiently implemented, the cryptocurrency size and scale will rise significantly large.”
- “Volatility issue diminishes by itself once the size and scale of a cryptocurrency is significantly large.”

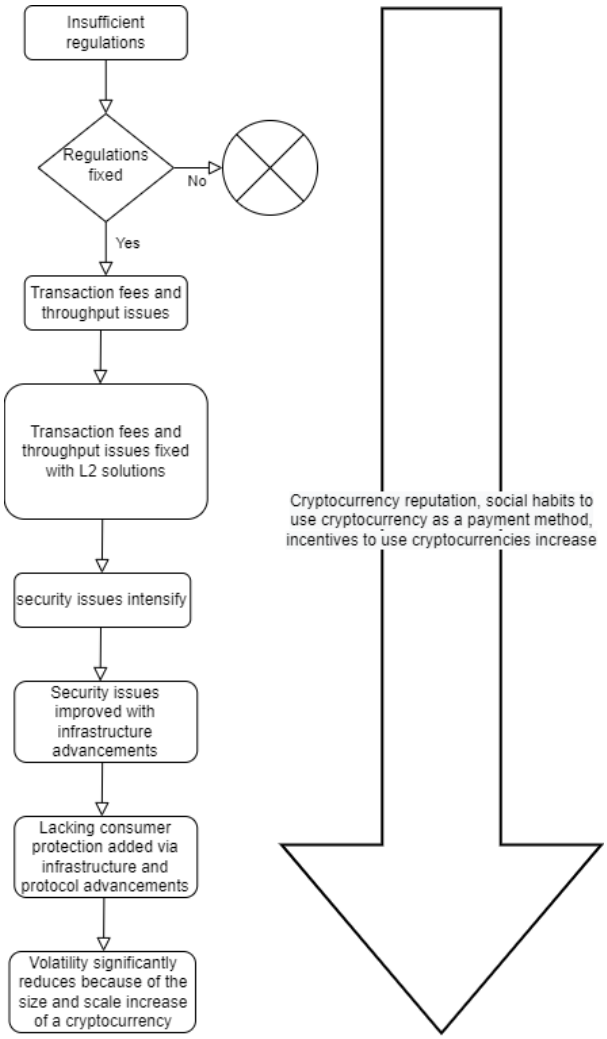


Figure 5 How cryptocurrencies will start replacing traditional payment methods at a large scale

Layer 2 technologies are based on a multi-layer hybrid architecture where validation of individual transactions can be parallelized. Individual transactions can be validated or verified independently. These kind of solutions are already being developed and tested currently.

Security issues in this context means that for a normal user the necessary knowledge of handling the cryptographic keys and the steep learning curve is too big. Both of these can be improved with infrastructural advancements meaning that exchange sites such as Coinbase [36] and Binance [37] will hold the wallet and hide the complexity for the user.

Lacking consumer protection in this context means that there are no features such as refunds, chargebacks and KYC. KYC is already implemented within some of the exchange sites. In the end, with the help of intermediaries, cryptocurrencies from the perspective of an end-user will be used like regular banks currently.

In conclusion, there are solutions to all blockers except for the enabler which is insufficient regulations. The problem is that entities who are currently in control of the fiat monetary system do not want to lose their power and thus are not incentivised to advance the cryptocurrency regulations.

5.2 Relation to existing evidence

Existing evidence show that Bitcoins are mainly used as a speculative investment and not a medium of exchange [38]. This was further confirmed within our research. Third world countries that have an unhealthy local fiat currency and have enabled cryptocurrency regulation are existing evidence that imply that the most important blocker for cryptocurrency adoption lies in insufficient cryptocurrency regulations [39]. The solution for high transaction fees and slow transaction speed in the form of layer two technologies which include performing transactions off chain is confirmed as the dominant solution to the scalability problem [40]. We proposed that the solution to fix the problems of lacking consumer protection lie within the infrastructural and protocol advancements. But this would mean introducing intermediaries or violating the principle of immutability. Violating principle of immutability opens the door to entirely new risks [41].

5.3 Impact

This work confirmed that cryptocurrencies are currently used mainly as a store of value and for speculative purposes but not as a payment mechanism. In addition, gathered all the current issues and possible solutions that act as blockers for cryptocurrency to be used as a payment method. Furthermore, it proposed hypotheses and a flow diagram which connects the blockers to each other and describes their lifecycle.

5.4 Limitations

In order for our hypotheses which rely on the proposed sequence of events that were shown in Figure 5 to be valid, some conditions must be met. The country that fixes the regulatory blockers and starts the snowball effect must be a first world country with sufficiently large economy so that in case of a technological or infrastructural blocker there is enough resource to overcome the blocker. Secondly, the cryptocurrency must be market dominant such as currently is Bitcoin which has the potential to be big enough so that the volatility issue resolves by itself. Thirdly, even when all the blockers get solved there still might not be sufficient incentive for people to start using cryptocurrencies as a payment method.

5.5 Future Work

This work gathered all the relevant issues that act as blockers to the rise of using cryptocurrency as a payment method. Furthermore, the discovered issues were sorted by order of relevance and their most viable solutions were presented.

While some of the proposed issues are already confirmed in existing body of work, others are not. The importance of insufficient regulations acting as the dominant blocker is reflected in our work and the current body of work [39]. Nevertheless, no viable solution is yet proposed as to how to fix this problem. Fixing the issue of insufficient regulations is the most important direction for future work as it acts as the blocker for all the rest of the proposed issues.

The second most relevant issue, high transaction fees and low throughput, are being actively solved and already have indications of real world solutions. Although being an

important issue, it does not lack existing research to finding solutions such as is the case with insufficient regulations.

Security issues have the most likely solution in the hands of intermediary wallet exchanges that act similarly as a bank. There are two possible directions of future research in this aspect.

- Focus on how to better the current wallet exchanges in terms of security and usability.
- Focus on design of a solution that does rely on intermediary wallet exchanges.

Lacking consumer protection is currently not a relevant issue. Although in theory it is solvable with infrastructural and protocol advancement, it is not proven. When a cryptocurrency reaches to the point where lacking consumer protection will become the main issue, future research is necessary on how to implement these solutions.

References

[1] M. H. Joo, Y. Nishikawa and K. Dandapani, “Cryptocurrency, a successful application of blockchain technology,” *Managerial Finance,* vol. 46, no. 6, pp. 715-733, 2020.

[2] “CoinMarketCap,” [Online]. Available: https://coinmarketcap.com/. [Accessed 10 05 2022].

[3] A. Joshi, M. Han and Y. Wang, “A survey on security and privacy issues of blockchain technology,” *Mathematical Foundations of Computing,* vol. 1, pp. 121-147, 2018.

[4] D. E. Sorkin, “Payment Methods for Consumer-to-Consumer Online Transactions,” *Arkon Law Review,* vol. 35, no. 1, 2001.

[5] K. Zīle and R. Strazdiņa, “Blockchain Use Cases and Their Feasibility,” *De Gruyter,* vol. 23, no. 1, pp. 12-20, 2018.

[6] D. Walsh, “Paying with Bitcoin: These are the major companies that accept crypto as payment,” 12 04 2021. [Online]. Available: https://www.euronews.com/next/2021/12/04/paying-with-cryptocurrencies-these-are-the-major-companies-that-accept-cryptos-as-payment. [Accessed 10 05 2022].

[7] R. Dhamodharan, “Why Mastercard is bringing crypto onto its network,” 10 02 2021. [Online]. Available: https://www.mastercard.com/news/perspectives/2021/why-mastercard-is-bringing-crypto-onto-our-network/. [Accessed 10 05 2022].

[8] B. Luthi, “Visa Adds Cryptocurrency to Its Settlement Platform,” 30 04 2021. [Online]. Available: https://www.investopedia.com/visa-adds-cryptocurrency-to-its-settlement-platform-5181149. [Accessed 10 05 2022].

[9] C. Orji, “Bitcoin ban: These are the countries where crypto is restricted or illegal,” 11 01 2022. [Online]. Available: https://www.euronews.com/next/2022/01/11/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2. [Accessed 10 05 2022].

[10] N. N. N. Conde, A. A. Ibrahim, N. Idris and H. B. M. Mohadis, “Cryptocurrency Adoption in E-payment: Barrier of its Implementation”.

[11] P. Gomber, J.-A. Koch and M. Siering, “Digital Finance and FinTech: current research and future research directions,” *J Bus Econ,* vol. 87, pp. 537-580, 2017.

[12] L. Coppolino, S. Antonio, L. Romano, G. Papale, L. Sgaglione and F. Campanile, “Direct Debit Transactions: a comprehensive analysis of emerging attack patterns,” in *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2015.

[13] L. Moumeni, M. Saber, I. Slimani, I. Elfarissi and Z. Bougroum, “Machine Learning for Credit Card Fraud Detection,” in *Proceedings of the 6th International Conference on Wireless Technologies, Embedded, and Intelligent Systems*, 2022, pp. 211-221.

[14] D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain Technology Overview,” National Institute of Standards and Technology, 2018.

[15] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque and A. Colman, “Blockchain Consensus Algorithms: A Survey,” 2020. [Online]. Available: https://arxiv.org/abs/2001.07091#. [Accessed 10 05 2022].

[16] C. Zhang, C. WU and X. Wang, “Overview of Blockchain Consensus Mechanism,” in *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, Shanghai, China, 2020.

[17] N. Chaudhry and M. M. Yousaf, “Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities,” in *International Conference on Open Source Systems and Technologies (ICOSST)*, 2018.

[18] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang and L. He, “A Comparative Study of Blockchain Consensus Algorithms,” *Journal of Physics: Conference Series,* vol. 1437, 2020.

[19] F. Ginez, “Bitcoin Versus Traidtional Payment Systems: Is One More Effective Than The Other?,” WisdomTree, 2019.

[20] D. Maček and D. Alagić, “Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique,” *JIOS,* vol. 41, no. 1, pp. 69-87, 2017.

[21] U. Rahardja, Q. Aini, E. P. Harahap and Raihan, “Good, Bad and Dark Bitcoin: A Systematic Literature Review,” *Aptisi Transactions on Technopreneurship,* vol. 3, no. 2, pp. 115-119, 2021.

[22] L. A. Smales, “Bitcoin as a safe haven: Is it even worth considering?,” *Finance Research Letters 30,* 2018.

[23] D. G. Baur, K. Hong and A. D. Lee, “Bitcoin: Medium of exchange or speculative assets?,” *Journal of International Financial Markets, Institutions & Money,* vol. 54, pp. 177-189, 2018.

[24] L. P. d. l. Horra, G. d. l. Fuente and J. Perote, “The drivers of Bitcoin demand: A short and long-run analysis,” *International Review of Financial Analysis,* vol. 62, pp. 21-34, 2019.

[25] A. Spurr and M. Ausloos, “Challenging Practical Features of Bitcoin by the Main Altcoins,” *Quality & Quantity,* vol. 55, pp. 1541-1559, 2020.

[26] F. Allen, X. Gu and J. Jagtiani, “A Survey of Fintech Research and Policy Discussion,” 2020.

[27] F. Hampl and L. Gyönyörová, “Can Fiat-backed Stablecoins Be Considered Cash or Cash Equivalents Under International Financial Reporting Standards Rules?,” *Australian Accounting Review,* vol. 31, no. 98, pp. 233-255, 2021.

[28] B. N. Thanh, T. N. V. Hong, H. Pham, T. N. Cong and T. P. T. Anh, “Are the stabilities of stablecoins connected?,” *Journal of Industrial and Business Economics,* 2022.

[29] A. Islam, S. Hoosen, M. Hossain, J. Nime, S. Hossain and M. Dutta, “An Online E-Cash Scheme with Digital Signature Authentication Cryptosystem,” in *Sustainable Communication Networks and Application,* Springer, 2021, pp. 29-39.

[30] P. Runeson, M. Höst, A. Rainer and B. Regnell, Case Study Research in Software Engineering, John Wiley & Sons, Inc., 2012.

[31] “Google Meets,” [Online]. Available: https://meet.google.com/?pli=1. [Accessed 10 05 2022].

[32] “https://obsproject.com/,” OBS, [Online]. Available: https://obsproject.com/. [Accessed 10 05 2022].

[33] J. Saldana, The Coding Manual for Qualitative Researchers, SAGE Publications Ltd, 2015.

[34] V. Braun and V. Clarke, Successful Qualitative Research, SAGE Publications Ltd, 2013.

[35] “alfasoft.com,” Alfasoft.com, 2022. [Online]. Available: https://www.alfasoft.com/en/products/statistics-and-analysis/nvivo.html?gclid=CjwKCAiAyPyQBhB6EiwAFUuakqvlPHWZu5GsDnxFjQS3ZT8RFvzFYoQqGWxThJZ4Xl3CI6o_f7j-MBoCMYEQAvD_BwE. [Accessed 10 05 2022].

[36] “Coinbase,” [Online]. Available: https://www.coinbase.com/. [Accessed 10 05 2022].

[37] “Binance,” [Online]. Available: https://www.binance.com/en. [Accessed 10 05 2022].

[38] D. G. Baur, K. Hong and A. D. Lee, “Bitcoin: Medium of exchange or speculative asset?,” *Journal of International Financial Markets, Institutions and Money,* vol. 54, pp. 177-189, 2018.

[39] E. A. Mosakova, “National Cryptocurrency as Venezuela's economic development factor in the 21th century,” 2019.

[40] J. Khamis, S. Schmid and O. Rottenstreich, “Demand Matrix Optimization for Offchain Payments in Blockchain,” in *IEEE International Conference on Blockchain and Cryptocurrency*, 2021.

[41] M. Zachariadis, G. Hileman and S. V. Scott, “Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services,” *Information and Organization,* vol. 29, pp. 105-117, 2019.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Cryptocurrency as a Replacement for Traditional Payment Methods”, supervised by Alexander Norta
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

16.05.2022

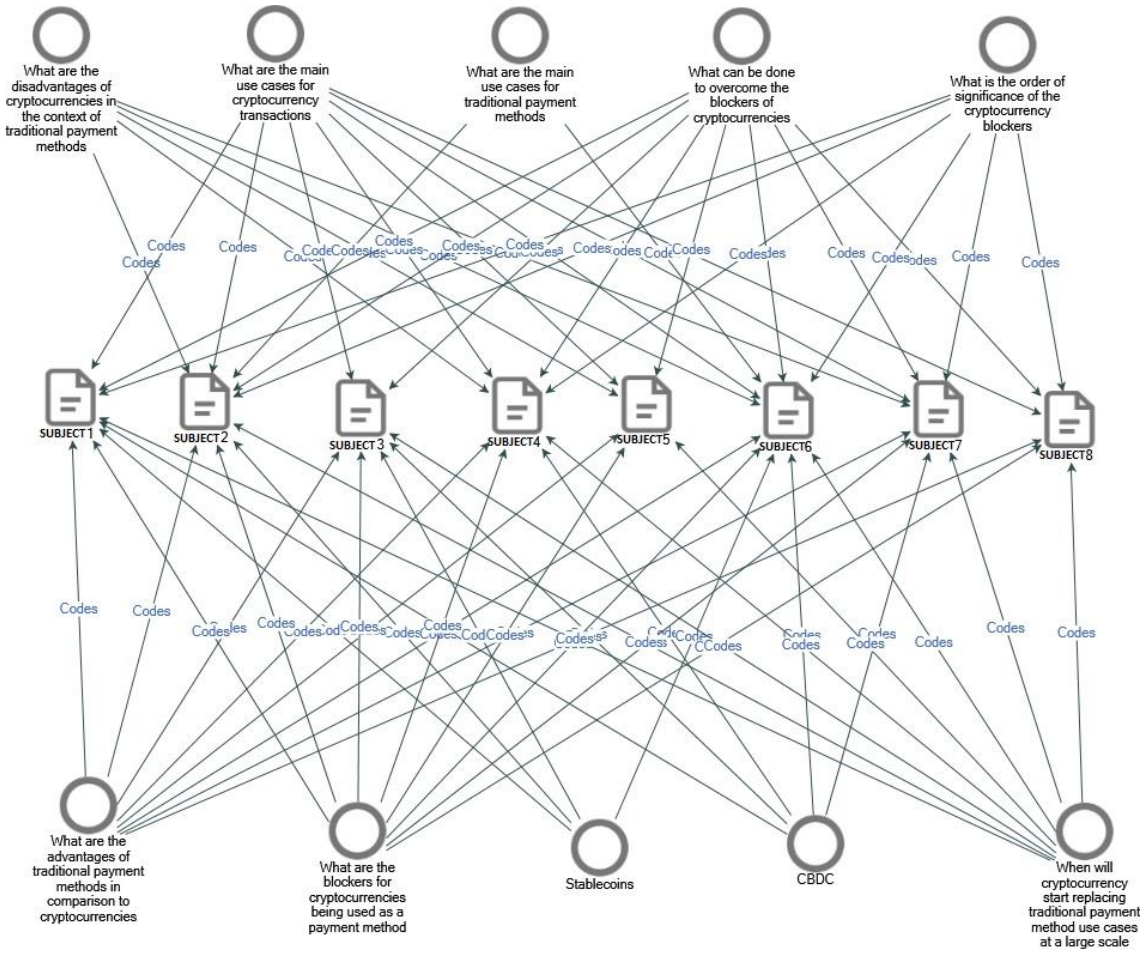
1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview questions cheat sheet

Questions:

- What is your name?
- What kind of education do you have?
- How many years of experience in the field of finance and/or cryptocurrency?
- What are the main use cases for cryptocurrency transactions?
- What are the main use cases for traditional payment methods?
- When will cryptocurrency start replacing traditional payment method use cases at a large scale?
- What are the advantages of traditional payment methods in comparison to cryptocurrencies?
- What are the disadvantages of cryptocurrencies in the context of traditional payment methods?
- What are the blockers for cryptocurrencies being used as a payment method?
- What is the order of significance of the cryptocurrency blockers?
- What can be done to overcome the blockers of cryptocurrencies?

Appendix 3 – Thematic Map of all Subjects and Main Codes



Appendix 4 – Thematic Map of all Main Codes and Sub Codes