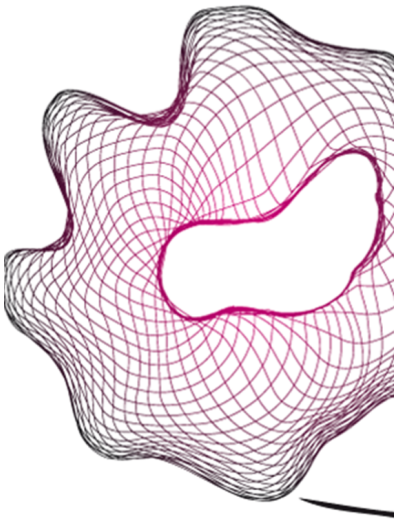
UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering,
Mathematics & Computer Science (EEMCS)
Services, Cybersecurity and Safety (SCS)



Security Risks Surrounding Cryptocurrency Usage: A Study on the Security Risks of Cryptocurrencies and How Security Perception Affects Usage

Janina Roppelt
M.Sc. Thesis
August 2019

Graduation Committee:
dr. A Peter
prof.dr. M.D.T. de Jong
S. Barth, M.Sc.
S.R. Jansma, M.Sc.

Telecommunication Engineering Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Security Risks Surrounding Cryptocurrency Usage: A Study on the Security Risks of Cryptocurrencies and How Security Perception Affects Usage

Janina Roppelt
University of Twente
EEMCS

***Abstract*—Since 2017, cryptocurrencies are known to nearly everyone. Their popularity, vast variety, and financial nature raise questions about the security risks that surround them. Just as important as the actual risks are risk awareness of people and to which extent their security risk perception does influence the decision to use cryptocurrencies. In this paper, two studies are conducted to identify security risks associated with cryptocurrencies, their perception by (possible) users and the effect this perception has on the decision to use cryptocurrencies. Conducting these studies will identify risks to address in cryptocurrencies and help to understand hurdles in the adoption process. Study one is a literature study that describes cryptocurrency vulnerabilities and their associated risks. Results show that risks for users are especially found in the cryptocurrency environment. Study two focuses on how a persons' security perception influences their cryptocurrency usage through a questionnaire. It is found that participants who own cryptocurrencies perceive them as less risky, have more trust in them and higher knowledge. The results show that the largest threat to cryptocurrency usage is the environment around cryptocurrencies, as it does not only hold technical risks but is also perceived as highly impacting. We conclude that (1) security risk perception does play a role in the adaption of cryptocurrencies and that (2) the involvement of unregulated third parties in the environment hinders widespread cryptocurrency usage.**

1. Introduction

In 2014, five years after the launch of Bitcoin, private users, as well as the management of important stakeholders in the financial field, believed cryptocurrencies to be a possible disruption through easier and quicker payment possibilities around the globe, possibly leading to cryptocurrencies as the only method of payment [1], [2]. More recent research has shown, that the shift into a broadly used currency has not happened yet, but that cryptocurrencies are still mainly used for investment purposes [3].

Nevertheless, cryptocurrencies gained a lot of popularity especially in late 2017. The market price of Bitcoin went from €1,000 per Bitcoin to nearly €20,000 within six months, before falling back to €3,000 within ten months. Alternative cryptocurrencies (altcoins) also followed the trends observed in Bitcoin, especially when values fell [4]. After the value decrease in 2018, media attention around cryptocurrencies decreased; the hype was over. Nevertheless, the market price of Bitcoin is recovering and rising again in 2019.

A technology hype is typically a marketing tool utilized to further a user basis. Although there is no one company behind cryptocurrencies, the quick value developments in 2017/2018 followed the hype cycle quite well. Broad media coverage and issued warnings for consumers indicate that the user basis indeed grew in the critical month. One of the most pressing questions from a security point of view is whether this hype led to less security risk considerations before using cryptocurrencies. In a broader sense, the question arises to what extent the individual perception of security influences the decision to use cryptocurrencies. While foremost being interested in the effect of security risk awareness, this research will also include the concepts of knowledge, trust, and attitude and their effect on the decision to use cryptocurrencies.

Knowing how security influences users is relevant, as the concept of a blockchain as the basis of a currency is just around ten years old and might impose new, unknown security concerns. The security of a specific cryptocurrency is not only dependent on the security of the blockchain technology, but also on its developers and algorithms used. Flaws once in the source code are hard to rectify, which makes cryptocurrencies more vulnerable than normal software when flaws are discovered. Therefore, it is important to know which vulnerabilities exist. For users, it is just as important to know how vulnerabilities translate to risks for them personally. Additionally to risks originating from a specific cryptocurrency, trading and using cryptocurrencies cannot be done without a third party, which is not bound to the blockchain and therefore does not have the security standards a user might expect when handling cryptocurrencies. We call these parties the *environment* of cryptocurrencies.

This paper sets out to research possible attacks on cryptocurrencies and their environment as well as the risks attached to these attacks. Another research goal is to investigate how people are perceiving the security around cryptocurrencies and if this perception influences their usage of the technical currency. Furthermore, we are interested in the effects the hype had on security risk

awareness. The research will be split into two parts. The first part is a technical literature study that establishes which vulnerabilities can be found in cryptocurrencies and which risks these vulnerabilities hold for users. The second part is a questionnaire study on the use of cryptocurrencies and how security perception affects the usage decision. We formulate the overall research question and subquestions per study:

What are the security risks of cryptocurrencies and how does their perception influence usage of the technology?

Study 1 - Security risks in cryptocurrencies.

T1: *Which cryptocurrency vulnerabilities do exist?*
T2: *How big are the risks associated with the found vulnerabilities?*

Study 2 - Cryptocurrency usage and security risk perception.

S1: *How do people use cryptocurrencies?*
S2: *To which extent does security risk perception influence the usage decisions?*
S3: *To which extent did the hype influence security risk awareness?*

By conducting these two studies, we can extract the biggest risks to cryptocurrencies, both technical and in people's perceptions. Knowing these risks is essential from a technical point of view to mitigate them according to the risk they pose. On the other hand, knowing which risks are perceived as the highest threats by (possible) users helps to understand the adoption of cryptocurrencies. We also include further concepts of security perception that might have an impact on the usage of cryptocurrencies, such as knowledge and trust. These results can be used to address the critical points to further widespread adaption of the technology.

On the other hand, knowing the influence a hype has on the risk considerations before using a technology can help to protect consumers from impulsive decisions, by using warnings that address the right issues.

Finally, we will give an overview of the population of people that use, used or considered using cryptocurrencies. This is not helpful to better understand the results of this study but can also serve as a basis for further studies.

2. Theoretical Framework / Related Work

This section starts with an overview of how cryptocurrency works technically and which components are needed to use them. This part furthers understanding of the results of study one. Second, we discuss security risk awareness, as well as other concepts related to how a person perceives the security around cryptocurrencies. This part will form the theoretical basis for the user study.

2.1. The Cryptocurrency Technology

Cryptocurrencies are built on blockchain technology. A blockchain is a series of data records (called blocks) tied to each other by incorporating a unique identification code (hash) of the previous block in the following one. By doing so, it is impossible to delete or change a block in the chain, without changing every block thereafter as well. Consequently, blocks that are added to the blockchain last are least secure, as an attacker would only have to change a few consecutive blocks. Changing a block is not trivial, as the majority of the distributed network has to agree on the creation of a new block [5]–[7].

In the following subsections, the cryptocurrency technology is described, starting with the technological components of the blockchain: hashes, blocks, and the consensus protocol, and how they help to establish a distributed ledger. Afterward, differences between cryptocurrencies are discussed. Finally, the environment around cryptocurrencies and its role in risks associated with using cryptocurrencies is introduced.

2.1.1. Hashes. Hashes are used to ensure the integrity of the data in the blockchain. Generally, they are digests of an unspecified amount of data. Most cryptocurrencies hashes are calculated with the SHA-256 algorithm which gives back a hash of 256 bits. Hashes are easily computed from any data, but it is computationally infeasible to compute the reverse of the hash (the data). Another characteristic is that even a small change in the original data will result in a completely different hash value. Furthermore, the possibility of two hashes from different data to be the same when produced with a secure hash function of bit-length 256 is $1/2^{128}$. This gives a negligible chance of collision and is called *uniqueness*. All these properties are important to secure the data integrity in the blockchain.

2.1.2. Blocks. The data of a block holds all transaction details and is the part that must be kept secure. Secure in this case means that the integrity of the data is ensured. A block contains metadata and actual data, which is normally one or more asset (coins) transactions done on the blockchain. Every transaction has a number, two addresses (sender and receiver), and the number of assets to be transferred. In contrast to conventional money, cryptocurrency coins can be split into very small pieces. Addresses are the digital counterparts to a bank account with the difference that they do not correspond to a person but to a public/private key pair. Every transaction is made to a receiver's address which is his public key. A transaction also has to be signed by the sender with his private key. After an assembled block is proposed to the network, it is verified. During this process, the correctness of the signature will be checked with the public key and the receiver's address on existence. Note that the verification in this case only checks technical correctness. There is no validation of any kind to check whether a transaction is legal or should not be made because of other reasons.

2.1.3. Consensus protocols. A consensus protocol is used to reach consensus about new blocks in the network, and to slow down the creation of new blocks. The most common consensus protocol is the Proof of Work (PoW). As the name states, someone aspiring to publish a new block must proof that he put work, in this case computation power, into it. This is done by solving a computationally difficult 'puzzle'. A common puzzle is to lay restrictions on the hash value that is calculated as a fingerprint for each block. Since even a small change in the hashed data results in a completely different hash, producing a valid hash will take trial and error. The difficulty of a puzzle can be seen as the number of hashes one would be expected to try before finding a valid one. It can be adjusted to increase or decrease the average time in which a new block is published. At the moment, a Bitcoin proof of work will take around ten minutes, while an Ethereum proof of work takes around 15 seconds. As an incentive, a reward is given for each correct solution. The processing of blocks to receive a reward is called *mining*.

There are alternatives to the PoW. The most common alternative is the proof of stake (PoS). In a proof of stake, one has to have a certain amount of resources in a specific cryptocurrency. Based on the amount and time the amount is held, users gain more right to vote for new blocks. Other alternatives are proof of elapsed time (PoeT), a byzantine fault-tolerance protocol, and hybrids of different proofs.

2.1.4. Distributed ledger. The distributed ledger ensures that the blockchain ledger is available and consistent throughout the network. That means that there is a network of nodes that all have the latest version of the blockchain. This adds extra security in terms of availability as even when a big part of the network fails, no data will be lost. Every node can publish a new block like described above. It then broadcasts that block and the rest of the network verifies it. If more than 50% agree, the block is added to the blockchain. Dependent on the underlying protocol the local chain might only be permanently updated after a specific amount of consecutive blocks are collected. In some cases, two blocks may be published at the same time. In this case, a fork is created. The forking continues until one of the branches becomes bigger than the other, as the main blockchain is always defined as the longest branch from the root note.

2.1.5. Differences between cryptocurrencies. The main technical differences between popular cryptocurrencies is whether a cryptocurrency is based on a *fixed* vs. a *programmable* blockchain. Bitcoin, Litecoin, and Monero are examples for fixed blockchains. These blockchains can only be used for the creation and exchange of the coin connected to it.

The first and most popular programmable blockchain is used by Ethereum. Programmable blockchains are also called *platforms*. In contrast to Bitcoin, Ehtereum can not only be used for money transactions and token creation but also to execute code. This creates new opportunities like running distributed applications or the implementation of smart contracts. Smart contracts are intended to digitally verify or enforce actions that should be done according to a contract. By using such a computer protocol, a trusted third party is omitted without raising insecurity for the contract parties. A programmable blockchain can be seen as a distributed supercomputer. To use the computation power of the Ethereum blockchain, you have to pay with the Ethereum currency *Ether*.

Another difference is based on whether a cryptocurrency uses its own *native* blockchain, or is built on a platform and therefore uses a *non-native* blockchain. A native blockchain means that there is a dedicated blockchain for this one cryptocurrency. When a cryptocurrency is non-native, it is built on a platform like Ethereum. The advantages of such a currency are quick set-up time and no need for their own network and contributors. Disadvantages are little freedom in implementation and no self-sufficiency. For such a currency, a fixed amount of tokens is created before it is launched. This is useful for purposes like crypto securities and real-world asset tokens, that should not be awarded for computational effort, but only to a limited amount of people or when a specific event happens.

2.1.6. The broader cryptocurrency environment. Each cryptocurrency has an environment around its source code and network, which provides information and the utilities to acquire, sell and store coins. We include the environment in this research as previous research suggests that there are significant risks for users in them, as they add an (unregulated) third party [8], [9].

Acquiring a cryptocurrency can be done in different ways. Besides mining, cryptocurrencies can also be acquired through online exchanges. These exchanges sell cryptocurrencies for real money or other cryptocurrencies based on the market value of the moment. This is the way an investor would choose, while mining is mostly done by tech-enthusiasts.

When someone owns a cryptocurrency he owns a private and public key. The public key can be seen as the address to an account on which cryptocurrencies are sent to, stored at, and paid from. The private key is proof that someone owns the amount of cryptocurrency stored at a specific address. Consequently, the private key should be kept a secret while the public key can be disclosed to anyone. The keys are usually kept secure in so-called *wallets*.

A wallet is a piece of hardware or software that holds the key data. Hardware wallets are usually USB sticks or custom made cryptocurrency solutions. The most common forms of software wallets are programs running on a personal device and online wallets. When running a software wallet on a device, both keys are stored on this device and there is no third party that has to be trusted. With online wallets, key management is delegated to a third party. To retrieve a private key the user has to log-in to the service with a password.

Besides the possibility of having a personal wallet, users can also choose to be part of an exchanges' wallet. The difference is that all users of the exchange gain access to one

or more shared wallets that are managed by the exchange. So rather than receiving a private key, they will only have a password for the exchange. Exchanges act as a trusted third party and have their own backlog ledger independent of cryptocurrency blockchains. This, in turn, means that transaction made between users of the exchange will not appear in a cryptocurrency ledger, but only in the exchanges' administration. Real blockchain actions are only made when cryptocurrencies are transferred in or out of the exchange. As every third party involvement, this adds new risks to cryptocurrency trading.

2.2. Cryptocurrency users

Although we know about the possibilities cryptocurrencies offer, there is little literature about how people use them. In the following, we will discuss social aspects of cryptocurrencies. Security perception will be defined and discussed based on its components. As cryptocurrencies are primarily financial, we will also investigate investment research, combined with possible explanations of demographic aspects. For every discussed concept we give the hypothesis at the end of the paragraph. They are marked with Hx.

2.2.1. Security perception. We define the construct of security perception as a combination of knowledge, attitude, trust, and risk awareness. These concepts have either already shown to have some effect on (intended) cryptocurrency usage or were relevant in general investment research.

Knowledge. In finances, higher knowledge was found to be related to higher risk tolerance [10]. In fintech research, knowledge was found to have a significant influence on the participants' security perception. Participants with higher levels of financial knowledge perceived fintech technologies as more secure [11].

There is one study [12] about knowledge in the context of cryptocurrencies in the United States. They focus on the gender gap they found in cryptocurrency knowledge, but their results can also be used as a basis for present knowledge around cryptocurrencies. The study consisted of six questions about knowledge, which had to be answered on a true/false scale. Participants scored a 3.013 of 6, with men scoring slightly higher, and women slightly less high. Interesting is that the overall score is not much better than a score we would expect from blind guessing. There also is a clear separation between correct answers to the questions. While participants were good in answering questions about third parties, government insurance and the existence of a central repository, they were bad at answering questions on the existence of a public ledger, whether or not the supply of coins is fixed and if transactions are reversible. It seems that questions which got media attention and are more political get answered correctly, while knowledge of primarily technical subjects is not present. In this research, we will focus on technical knowledge.

H0: *High knowledge is expected to result in higher cryptocurrency usage.*

Attitude. Attitude is the way one thinks or feels about something [13]. In this research, we choose to define attitude as the way people classify cryptocurrencies in financial terms. Using money to create value without precise knowledge of the outcome can be divided into three actions: investment, speculation, and gambling. A conceptual and empirical study found the concepts of gambling and investment to be different, for example on the risk of loss, time frame, and winning margin. Speculation has conceptual similarities to both gambling and investment. The empirical part of that study focused on cognitive, motivational and personality attributes. They found that all three concepts have users with similar attributes, with the strongest relationship between gambling and speculating [14].

Because of the high volatility of cryptocurrencies, it is hard to distinctly classify them in one of the categories. Therefore, people might have different perceptions of what they are dealing with and might act differently from each other. Several studies [2], [14] [15] showed that people use cryptocurrencies both for long term investment and short term speculation. Regarding the findings on similar attributes in gambling and speculating as well as news coverage on cryptocurrencies, it seems that gambling motivations are also relevant when it comes to cryptocurrencies. The five motivation dimensions of gambling are: hitting the jackpot, social rewards, intellectual challenges, mood change, and winning [16]. Most, if not all of these dimensions can be seen in media reports on cryptocurrencies. In conclusion, the classification of cryptocurrency into one of the three concepts is not clear, and they are used in all contexts. This is why we include a users' attitude as part of security perception. A positive attitude is defined as the classification into an investment, while a negative attitude is a classification of cryptocurrencies as gambling.

H1: *A positive attitude is expected to result in higher cryptocurrency usage.*

Trust. The ecosystem of cryptocurrencies is established to decentralize trust (in third parties). But at least the components around the actual currency like exchanges and information website still involve third parties into the cryptocurrency trading. From the developer of a cryptocurrency over the exchanges' employees to the trading parties, essentially all actions that have a connection to the physical world bare risks and could, therefore, raise trust issues.

In [15], characteristics of the blockchain technology impacting trust are extracted from an interview study. The characteristics are Decentralized Blockchain, Unregulated Blockchain, Blockchain's Embedded Expertise, Blockchain's Reputation, Transparent Transactions, Easy and Quick Transactions, and Low-Cost Transactions. In the article, the only characteristic negatively influencing trust in cryptocurrencies was the blockchain's reputation which took a hit in 2013 when the Silk Road anonymous online market was shut down. But as the crash at the beginning of 2018, the utilization of criminal activities didn't impact the reputation for long. The article also named participants where the reputation had positive impacts due to big com-

pany involvement in cryptocurrencies.

The characteristics found in [15] hint that there is more trust in technology than in institutions. This is more explicitly stated in a 2015 study [17] that focuses on algorithmic authorities. The main findings were that people prefer to trust a decentralized algorithm over conventional institutions. These institutions lost trust in the 2008 financial crisis and the actions in Greece during the Euro-crisis. Although trust in technology is high in comparison, the authors argue that there is no blind trust in algorithms, but that most users also want human judgment to be involved. In relation to this, the participants of the study were divided in their answers to the question of whether or not cryptocurrencies should be regulated.

Trust seems to be one of the key concepts of why cryptocurrencies might be chosen over traditional money. This is especially interesting when looking into security risks because trust in technology might lead to a less critical view of possible flaws.

H2: *Higher trust is expected to result in higher cryptocurrency usage.*

Risk awareness. Awareness is knowing something exists and seeing it as important [13]. Therefore, we define risk awareness as a combination of knowledge about risks and the importance a user gives to it. Previous research intended to find a negative effect of perceived security risks on intended cryptocurrency usage were not able to find such an effect [18]–[20]. Nevertheless, they agree that risk awareness should play an important role in cryptocurrency usage and the negative findings might be due to methodological choices. Walton and Johnston [20] found an effect of risks that related to trust rather than security, which means that people were hesitant to adopt cryptocurrencies as the elimination of the trusted third party also means the elimination of a party to take the risk. In this research, we aim to include risk awareness, both on security and trust, in a different way. By using technical understanding and a scenario approach to measure risk awareness, rather than questionnaires, we hope to overcome the problems of previous researches. Another difference will be that all discussed articles only looked at the intention to use cryptocurrencies, rather than to actual behavior. In our study, we will research actual behavior.

H3: *A higher risk awareness is expected to result in less cryptocurrency usage.*

Amongst others, one reason to study cryptocurrencies was the high attention in 2017/2018, which was called a hype. One of the reactions to the hype was issued warnings from consumer protection institutions about the dangers of cryptocurrencies. This is why, for the question of whether the hype did influence risk awareness to a point that people disregard their security concerns, we formulate the following hypothesis:

H4: *We expect to find a difference in risk awareness based on cryptocurrency acquisition time.*

2.2.2. Demographics and general investment research. Research on investment and personality agree that there is a significant effect of demographics on investment. [21]–[24].

Men generally invest more capital, while women invest more successful, meaning that they lose less money. This is explained by the fact that men are generally more trusting than their female counterparts [25]. Although, the difference found between genders might be less significant than thought due to the proportion of men that are highly optimistic and therefore invest a lot [26]. The effect of gender on investment was also found in the context of trading cryptocurrencies. Women are less likely to engage in cryptocurrency trading, are less active, but do get higher returns [27].

H5a: *We expect a higher prevalence of male cryptocurrency users.*

Hasso et. al. [27] found an effect of age on cryptocurrency trading. Contrary to gender, the age effect was not a consistent finding. It was only found to have a positive effect in some phases of the developments in late 2017. Age is also found to have an influence on other financial concepts, like expectations about inflation [28].

H5b: *Higher age is expected to result in higher cryptocurrency usage.*

Although there is not yet an indication that education also has an impact on cryptocurrency usage, Grable et. al [10] found that higher education is connected to higher risk tolerance. As cryptocurrencies are generally seen as risky [18], education is also included in this research.

H5c: *Higher education is expected to result in higher cryptocurrency usage.*

Figure 1 shows a model of the expected effects extracted from the literature.

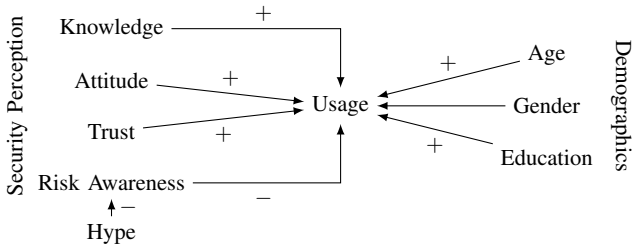


Figure 1. Model of the security perception construct and the expected effect of its dimensions on cryptocurrency usage

3. Study 1 - Method

The goal of this study was to identify vulnerabilities connected to cryptocurrency usage and classify their risks. The first step of study one was a literature study to find weaknesses in cryptocurrencies. The search term used in Scopus and Google Scholar was: (Cryptocurrenc* OR Bitcoin) AND Security. From useful studies ([5], [8], [29]),

vulnerabilities were selected for further analysis based on their effect on users. Similar attacks were grouped. Attacks concerning the environment rather than the blockchain technology were added based on technical blog posts and media articles.

In the next step, risks were allocated to different attacks. Risk was defined as:

$$\text{risk} = \text{likelihood} \times \text{impact}$$

Likelihood and impact were scored from low to high. Likelihood was determined by past events and theoretical likelihood/ease of attack. We chose three main impacts to analyze:

- Impact on finances
- Impact on reputation
- Impact on trust

As trust is a more complex concept, it was split into dimensions, based on the findings of Sas et. al. [3] [15]. They found seven dimensions impacting a cryptocurrency users' trust: *blockchain's embedded expertise*, *decentralized blockchain*, *unregulated blockchain*, *easy and quick transactions*, *low-cost transactions*, *transparent transactions*, and *blockchain's reputation*. In our analysis, we combined them into four dimensions:

- Trust in technology
- Trust in decentralization (decentralized blockchain, unregulated blockchain)
- Trust in transactions (Easy and quick transactions, low-cost transactions, transparent transactions)
- Reputation of the blockchain

The scoring was visualized with a heat map as seen in table 1. As risk was defined as likelihood times impact, the darker the color of a cell, the higher the risk for a user.

TABLE 1. HEATMAP FOR RISK CODING

LH \ IM	Low	Medium	High
Low			
Medium			
High			

LH = Likelihood, IM = Impact

4. Study 1 - Results

4.1. Cryptocurrency vulnerabilities

The literature study yielded ten direct and one environmental vulnerability for users. Three vulnerabilities of the cryptocurrency environment were added through further research. An overview of the resulting 14 vulnerabilities is given in table 2. The >50% hash power attack is the only mayor attack affecting users. A major attack means it directly uses a vulnerability in the technology rather than misusing protocols.

Seven out of ten attacks on cryptocurrencies itself are issues related to the distributed network, making the network the biggest attack vector. Most of these attacks harm the user by isolating him or controlling his traffic in different ways. Those attacks are sybil, tampering, eclipse or netsplit, and routing attacks. The other two attacks on the network are DDoS attacks which prevent usage of the network by overloading it, and deanonymization of users.

The remaining three attacks are wallet theft, refund attacks, and punitive feather forking. Wallet theft and punitive feather forking are both attacks that are aimed at a specific user. A refund attack is mainly targeting sellers of products, but also harm users in their reputation.

There were four vulnerabilities found in the environment: the closing of an exchange, a data leak or breach of an exchange, misinformation on the value a cryptocurrency should be exchanged at, and scams which sell new cryptocurrencies that will never exist. Out of these four vulnerabilities found in the environment of cryptocurrencies, three were possible because of no regulations.

4.2. Associated risk

The risks defined in this research can be found in table 3, 4 and 5. In the first two tables, likelihood, as well as impacts on finances, reputation, and overall trust, were defined per attack. The overall impact on trust was derived from table 5, where all four dimensions of trust and the impact of an attack on them were explored.

The two attacks associated with the most risks for a user were wallet theft and initial coin offering (ICO) scams. Refund attacks, on the other hand, are the least harmful for a private cryptocurrency owner. Punitive and feather forking, sybil, eclipse, tampering, and routing attacks are grouped into 'attacks that concentrate on the isolation of a user in any way'. These attacks had similar impacts, as well as likelihoods. All risks associated with the environment around cryptocurrencies also form a group. This group was left out of the detailed trust analysis, as it had no direct impact on trust. This is because attacks in this domain affect a third party, rather than a cryptocurrency itself.

We found that direct attacks on cryptocurrencies have a high impact on finances when they are targeted at a specific user. Targeted attacks are isolation attacks and wallet theft. Impact on finances for attacks on the environment was high throughout. This is not surprising, as attacks on the infrastructure around cryptocurrencies would be expected to be primarily financial in motive.

Impact on reputation had the lowest impact in total. Compared to other impacts, reputation is almost only at risk when actively using cryptocurrencies as a payment method.

Impact on trust was highest for attacks that use vulnerabilities in the cryptocurrency network. Trust in technology and the blockchain's reputation were the more vulnerable trust dimensions, as they are affected by nearly every attack. Trust in decentralization is theoretically the least impacted by the found vulnerabilities. Except for DDoS attacks, all network attacks can affect trust in decentralization, but other attacks are no threat. Trust in transactions was impacted by all network attacks, which makes it slightly more vulnerable.

TABLE 2. SECURITY VULNERABILITIES

Security issue	Primarily affected party	Description	Type	Possible because of (problems in)
>50% hashpower or Goldfinger	Bitcoin network, miners, Bitcoin exchange centers, and users	A malicious entity holds more than half of the hash power in the network	Major attack	Cryptocurrency network
Refund attack	Sellers or merchants, users	The refund policies of sellers/merchants are misused, users can suffer reputation losses	Misbehaviour attack	Refund policies
Punitive and Feather forking	users	Dishonest miners blacklist transaction coming from specific addresses	Misbehaviour attack	Dishonest miners
Wallet theft	individual users or businesses	The private key gets stolen which gives the thief control over the wallet	Misbehaviour attack	Wallet (private key loss)
DDoS	Bitcoin network, miners, businesses, and users	The network cannot be used anymore because the attack exhausts the available resources	Misbehaviour attack	Cryptocurrency network
Sybil	Bitcoin network, miners, users	Adversary creates multiple virtual identities	Misbehaviour attack	Cryptocurrency network
Eclipse or netsplit	miners, users	Adversary controls in- and outgoing traffic of the victim	Misbehaviour attack	Cryptocurrency network
Tampering	miners, users	Delay network communication about transactions and blocks to specific nodes	Misbehaviour attack	Cryptocurrency network
Routing attacks	miners, users	Isolate nodes from the network	Misbehaviour attack	Cryptocurrency network
Deanonymization	users	Link IP-addresses to coin addresses	Misbehaviour attack	Cryptocurrency network
Exchange closing	users	An exchange where users stored cryptocurrencies decides to close	Misbehaviour attack	No regulation
Exchange (data) leak/breach	users, exchanges	An exchange where users store cryptocurrencies or have an account gets hacked/breached	Misbehaviour attack	Exchanges vulnerabilities
Misinformation on value	Bitcoin network, miners, businesses, users	A community page on which values are stored is not correct/up to date	Misbehaviour attack	No regulation and no official tap in values
Scams	Cryptocurrency reputation, users	A new cryptocurrency that raised money via an initial coin offering (ICO) does not actually deliver a cryptocurrency	Misbehaviour attack	No regulation

TABLE 3. ANALYSIS OF RISKS ASSOCIATED WITH ATTACKS

Security Issue	Likelihood	Impact on Finances	Impact on Reputation	Impact on Trust in Cryptocurrencies
Uncategorized Attacks				
>50% hashpower or Goldfinger	Medium: In 2018 and the beginning of 2019, there have been at least 3 successful 51% attacks in different cryptocurrencies. (Bitcoin gold, Zenchash, Ethereum classic). Taking earlier attacks into account, there have been 1-2 attacks per year. The risk is bigger for smaller crypotocurrencies	Medium: The last attack on Ehtereum classic had an impact of over 1 million dollar. Financial impact for the users is less than for merchants. The greatest threat for financial losses is a loss in value of the attacked cryptocurrency	Low: There is little to no impact in reputation of users, as the attack will be known and merchants can attribute other attacks to this one	High: No currency can be relied on if attackers can take over the network
Refund attack	Low: There are no numbers for this attack. Also, the reward is much less than with other attacks	Low: the user will have no knowledge of the attack	High: The merchant will think the user claimed a refund while not giving back the product	Medium: If your money has unexplained behaviour which can impact your reputation, you might not trust is completely
Wallet theft	High	High: Getting a private key stolen (or loosing it) is equal to loosing all assets connected to this key	Medium: Having to tell people you got your private key stolen might lead to reputational losses	Low: Theft is not unique to cryptocurrencies and therefore has low impact on its validity
DDoS	Medium: In 2017, cryptocurrencies were the 5th most attacked industry by DDoS. There was no information about anything for 2018 that indicates that this trend continued	Medium: The user will temporarily have no access to his money and will not be able to make transactions	Low: As DDoS attacks will become known, there is little impact to personal reputation	High: DDoS attacks are a threat to every payment system. If you can't rely on your money to work 24/7, it is not a good system
Deanonymization	Medium: Deanonymization is possible, but not feasible/economical in most cases	Low	High: Especially when using cryptocurrency for illegal or sensitive purposes, reputational impacts can be high	Medium
Attacks that focus on a kind of isolation (isolation/blacklisting/control of addresses)				
Punitive and Feather forking Sybil Eclipse or netsplit Tampering Routing attacks	Medium: There are no numbers on how often this happens, but a punitive fork attack can be done with 20% of the network power, which is achieved by the biggest mining pool. Feather forking is even easier to achieve	High: A user who gets blacklisted will have little chance on his transactions to come through without paying high transaction fees. If it does not come through, the assets will be frozen forever	High: If your transactions are not working, you will most likely be categorized as untrustworthy	High: When blacklisted, isolated or controlled, the user is essentially banned from using the cryptocurrency, which will have high impact in trust

TABLE 4. CONTINUED ANALYSIS OF RISKS ASSOCIATED WITH ATTACKS

Security Issue	Likelihood	Impact on Finances	Impact on Reputation	Impact on Trust in Cryptocurrencies
Attacks on the Cryptocurrency Environment				
Exchange closing	Medium: In 2013 18 of 40 researched exchanges closed in the last three years [8]. There are also reports of that happening in 2019 (Liqui.io), but it does not seem to be occurring every other day	High: When an exchange closes, there is a high possibility of users to lose their whole investment	Low	As these attacks do not attack on the blockchain technology level, they have no direct impact on the trust in cryptocurrencies
Exchange (data) leak/breach	Medium: In 2013, Moore et al. [8] Found that 25% of all researched exchanges had a breach in the last 3 years.	High: In the research breaches, only 50% compensated for losses of the users	Medium: Data leaks and possible credential leaks can have impact on reputation through other websites	
Misinformation on value	Medium: There is still no regulation on prices of a cryptocurrency. There are reports from early 2019 where misinformation was given	High: People payed 1000 dollar per Bitocin too much because of 'wrong' pricing of a particular exchange	Low: There might be reputation losses as investor, but no major impacts	
ICO Scams	High: Scams became so common that authorities in the EU warned users about that kind of investment	A user will loose his whole investment	Low: As above, a user might look foolish for supporting a scam	

TABLE 5. THE DETAILED ANALYSIS OF ATTACK IMPACT ON TRUST

Security Issue	Likelihood	Trust in Technology	Trust in Decentralization	Trust in Transactions	Blockchain reputation
Uncategorized Attacks					
>50% hashpower or Goldfinger	Medium	Medium	High: When attackers take over the network, decentralization is lost	High: With a 51% attack, other attacks focused on transaction are facilitated	High: This attack is one of the most discussed problems with distributed PoW networks. They will therefore have a high impact on the blockchains reputation
Refund attack	Low	Low: It's not the technology but the protocols that make this possible	Low	Medium: Transactions on behalf of the customer can be made which should not be possible	Medium: If this happens more often the user might switch to another currency
Wallet theft	High	Medium: Although the technology of cryptocurrencies has nothing to do with getting your key stolen, victims might associate the two	Low	Low	Low
DDoS	Medium	High: The technology itself is unable to fend of a DDoS attack	Low	High: Under a DDoS attack, payments will be dropped or take longer than expected	Medium: One DDoS attack will not have major impacts on reputation, but recurring attacks will
Deanonymization	Medium	High: If a cryptocurrency promised anonymity but people get deanonymized, the technology cannot be 100% anonymous	Low	Low	High: If a cryptocurrency promised anonymity but people get deanonymized, they essentially lied
Attacks that focus on a kind of isolation (isolation/blacklisting/control of addresses)					
Punitive and Feather forking Sybil Eclipse or netsplit Tampering Routing attacks	Medium	Medium: The technology facilitates this attack, but it is mainly misbehaviour of humans, which is why we only categorize the impact on technology as medium	High: The idea of the decentralization is that there is no more power in one hand than the other, which is not what happens here	High: If you can only make transaction through paying horrendous fees, or not at all trust in transactions will be lost	High: A cryptocurrency that I cannot use when I want to I will not use

5. Study 2 - Method

5.1. Design

The goal of study 2 is to research security risk perception of (possible) cryptocurrency users, how these translate into usage decisions, and if risk awareness was influenced by the hype-like value developments. To do so, a questionnaire on cryptocurrency usage and the different aspects of security risk perception is conducted and analyzed. In the following section, we discuss the instrumentalization of the concepts as well as the means of analysis used on the resulting data.

5.2. Instruments

The questionnaire consisted of three parts displayed in this order: Demographics, cryptocurrency usage, and questions about security risk perception.

5.2.1. Demographics. Besides the age, nationality, and gender, subjects are asked for their education level and field of study/profession.

5.2.2. Cryptocurrency usage and motives. This part of the survey was used to gain an overview of how and why people use cryptocurrencies. The first question evaluated the current cryptocurrency status of the participant. The status was either *I own cryptocurrencies*, *I owned cryptocurrencies*, *I considered owning cryptocurrencies*, or *I never considered owning cryptocurrencies*. The grouping based on the first three answers was later used as the dependent variable. If the participant stated to never have considered owning cryptocurrencies, the survey ended. Based on the other three options, participants were asked questions on

- which cryptocurrencies they own(ed)
- how they store(d) them
- when they bought/sold their cryptocurrencies
- how much money they used to buy cryptocurrencies
- why they own or do not own cryptocurrencies (anymore)

5.2.3. Security risk perception. In the following, we will discuss the measurements of security risk perception per concept, as introduced in the theory section.

Knowledge

Three questions were asked to establish basic cryptocurrency knowledge:

- All cryptocurrencies use the same blockchain technology - yes/no/I don't know
- All cryptocurrencies have their own blockchain - yes/no/I don't know
- Which consensus protocols do you know? - 6 options, one false

When answering 'Yes' on the first question, the remaining questions were skipped. The third question was only displayed to a participant if he answered at least one of the first two questions correctly. The reason this was done was to prevent participants to get frustrated when confronted with questions they do not understand.

Attitude/Classification

Classification of cryptocurrencies was measured with one slider from zero to 100. A score of zero is a classification into pure gambling, a score of 100 a pure investment classification. We chose not to explicitly include speculation, as it has characteristics of both gambling and investment.

Trust

General trust in cryptocurrencies was also measured with one slider from zero to 100, zero meaning *no trust at all* and 100 *complete trust*.

Risk awareness

To measure the risk awareness construct, seven scenarios are established from the attacks found in study one (see table 2). Isolation attacks were bundled into one attack and only the two environment attacks *Scams* and *Exchange closing* were chosen. From the uncategorized attacks, the *Refund attack* was excluded, which leaves the *50% attack*, *Wallet theft*, *DDoS*, and *Deanonymization*. Excluding the refund attack was done because it mainly impacts reputation, but the questionnaire only measured impacts on finances and trust to reduce complexity. Because of the same reason, trust was reduced from 4 to 2 dimensions (impact on trust in the cryptocurrency technology and impact on trust in cryptocurrencies as a functioning currency.). This was possible as 3 dimensions were close to each other in impacts (see table 5.

Risk awareness was measured on matrix questions. As risk is defined by likelihood $\times$ trust, participants had to score likelihood and impact of different attacks on a *none* - *low* - *medium* - *high* scale. Scenarios which were perceived as easy in the pretest were displayed first to prevent discouragement of participants with less technical knowledge.

5.3. Procedure

After a pretest, participants were recruited via snowball sampling. The researcher asked people who were known to own cryptocurrencies or expressed interest in them to take part in the study. While recruiting, participants were also asked to forward the survey to any other people they knew who at least showed an interest in cryptocurrencies. Additionally, the link to the survey was posted on LinkedIn and Reddit (r/samplesize).

The questionnaire was published via the online survey tool Qualtrics. Participants could use computers or mobile devices to fill in the questionnaire. Before answering the 51 questions, participants accepted the informed consent form and state that they were older than 18 years. After completing the questionnaire, they were thanked for their time.

TABLE 6. DEMOGRAPHICS OF THE PARTICIPANTS

Characteristic	Count	Percentage
Gender (n=81)		
Male	66	81.5%
Female	12	14.8%
Prefer not to say	3	3.7%
Nationality (n=80)		
Dutch	53	66.3%
German	8	10.0%
Other European	9	11.3%
American	7	8.8%
Other	3	3.8%
Level of Education (n=81)		
High School or less	20	24.7%
Bachelor's or Professional Degree	35	43.2%
Master's Degree or higher	26	32.1%
Field of study (n=76)		
Computer Science	33	43.4%
Engineering	19	25%
Other STEM study	9	11.8%
HASS	15	19.7%
Age (n=80)	Mean	SD. Deviation
	28.63	8.98

5.4. Participants

The target audience of this study was everybody that owns, owned or considered owning cryptocurrencies at some point in time. There were no restrictions on gender or nationality. The only restriction for age was that the participant had to be older than 18 for reasons of consent. The survey reached around 100 people, 91 participants filled in the survey past the informed consent. More than 50% of the responses came from people that were approached personally. The majority of participants were male. The age of the participants ranged from 18 to 66 years. There were 12 distinct nationalities. Most participants were Dutch, followed by German. The majority studied and/or worked in computer science or another technical field. For an overview of the demographics see table 6.

5.5. Analysis

The data conducted from the questionnaire was analyzed with SPSS. After data sanitation, scores were calculated where necessary. After that, we used descriptive analyses to explore cryptocurrency usage. Security risk perception is analyzed on the differences between the three usage decision groups via ANOVA. Risk awareness is analyzed as a whole, but also in its dimensions: likelihood, impact on finances, and impacts on trust. The hypothesis on the effect of security risk perception and demographics are tested via a multinomial logistic regression. To check whether the hype affected security risk awareness, a MANOVA is used. In the following sections, the steps are described in detail.

5.5.1. Data sanitation. There were 91 responses to the survey that were filled in past the informed consent form. From these 91 responses, 73 are finished. Finished and unfinished Responses were kept if the participant either completed at least 4 of the 7 scenarios (2 responses) or everything but the security perception block (6 responses). The latter responses were only used for the analysis of cryptocurrency usage and motives, not for the analysis of security perception on the usage decision. Furthermore, 8 responses were discarded from the sample as the participants stated to have never considered owning cryptocurrencies. This left 81 valid responses for the descriptive analysis of cryptocurrency usage and 75 valid responses for the whole analysis.

5.5.2. Score calculation. While the scores for trust and classification could be used without further work, knowledge and risk awareness needed calculation.

Knowledge Knowledge was measured with the three questions stated above. For the first two questions, one point was given for the right answer (*No*). *Yes* and *I don't know* both were awarded no points. For the consensus protocols, one point per checked protocol was awarded. If a participant checked the false protocol (proof of transparency), she received no points for this question. With this scoring, the minimum knowledge score is 0, and the maximum score 7.

Risk awareness We calculated two scores for risk awareness. One for accuracy, which related to knowing something exists, and one for over-/underestimation of risks to measure the importance a participant gave to a risk. Both scores compared the participants' answers to the results of study one as can be seen in table 3, 4 and 5.

For accuracy, the closer the participant reached this baseline, the better her awareness. A participant got 0 points when she reached the baseline, and the number of steps she was off for other answers. For example, a participant that filled in *low* on an item that was *high* in study 1 was given two points. This means that 0 points stand for a perfect score, while the maximum offset can be 71. Missing values were filled with the expected values (1.5 for *none* and *high*, 1 for *low* and *medium*).

To see if participants over- or underestimate risks, a second score (estimation direction) with positive as well as negative points was calculated. Positive points were given for overestimating, negative points for underestimating. For example, if a participant filled in *none*, while the baseline value is *high*, she was given -3 points. The other way round, she would have been given 3 points. Based on the scoring, the lowest score one could achieve was -55 (extremely underestimating risk), the highest 30 (extremely overestimating risks). To have equal intervals, the positive scores were scaled to have a maximum of 55. Perfect estimation had a score of 0. Missing values were filled with the expected values (1.5 for *none*, 0.5 for *low*, -0.5 for *medium*, and -1.5 for *high*).

Besides the overall score, we explored differences between likelihood, impact on finances, and the two impacts on trust (in the technology and in cryptocurrencies as a functioning currency). This gave a better insight into which impacts are most pressing for the participants. To do so, we calculated the 4 dimension scores for both accuracy and estimation direction as described above. As, due to different baselines established in study one, all accuracy scores have different maximum scores per dimension they were scaled to 100. The same is true for the estimation direction dimensions. They were scaled to a scale ranging from -10 to 10. The ranges of the scales were arbitrary and chosen based on ease of understanding.

5.5.3. Logistic regression. To answer the main research question, we used a multinomial logistic regression model. The dependent variable was cryptocurrency usage, which was separated into three groups: *present*, *past*, and *considered*. The independent variables came from two constructs: demographics, and security perception. The following variables will be used per construct:

Demographics

- Age
- Gender (nominal)
- Level of education (ordinal)

Security perception

- Cryptocurrency knowledge
- Attitude (classification)
- Trust in cryptocurrencies
- Risk awareness scores (accuracy, estimation direction)

5.5.4. MANOVA. A MANOVA was used to test whether the hype around cryptocurrencies influenced risk awareness. Two groups were established as the independent variable. Present and past cryptocurrency users were classified as either hype users (18) or non-hype users (30). As a hype is not a scientific concept, we chose to use the coin value of Bitcoin as a hype indicator. The classification was done by median value in a month. The cut value was set to €5000 for one Bitcoin, as this is approximately the value at which the steep incline in October 2017 started. The independent variables are the two dimensions of security risk awareness: accuracy and estimation direction.

6. Study 2 - Results

6.1. Cryptocurrency usage

From the 81 participants, 40 own cryptocurrencies, 14 owned cryptocurrencies in the past, and 27 considered owning cryptocurrencies at some point in time. Current users are grouped under the word *present*, past users under the word *past*, and people that considered owning cryptocurrencies under the word *considered*.

As expected, the most common cryptocurrency was Bitcoin, followed by Etherium. Table 7 shows the preferred cryptocurrencies. The *other* category only holds cryptocurrencies that were named exactly once. The number of different cryptocurrencies owned per participant ranged from one to more than 57 with a mean of 3.8 (SD=6.53).

TABLE 7. DISTRIBUTION OF DIFFERENT CRYPTOCURRENCIES

Bitcoin	Etherium	XRP	Bitcoin Cash	Litecoin	Cardano	EOS	Stellar	IOTA
72	42	20	11	21	3	9	8	5
Monero	NEO	Nano	Dodge coin	Stratis	TRON	GAS	other	
3	3	3	3	2	2	2	24	

TABLE 8. DISTRIBUTION OF DIFFERENT STORAGE METHODS

Online exchange	Online wallet	Offline (software) wallet	Hardware wallet	Paper wallet
29	19	21	18	2

6.1.1. Acquisition and storage. From the 54 participants that own or owned cryptocurrencies, 30 bought them, 3 mined for them and 18 did both. The remaining three earned them for work they did.

Table 8 shows the different storage methods used by the participants. It is interesting to see, that offline methods are nearly as popular as online methods (48 vs. 41). Out of the 51 participants, 26 used one storage methods, while 21 used two and 6 more than two. From the 21 people using two methods, 85% used both an online as well as an offline storage. The distribution between methods for people who only used one is 50/50 for online/offline wallets.

6.1.2. Motives. Participants checked more than one motive on average. Because of this is it was not possible to assign one major motive to a participant. The main reason to own cryptocurrencies was *making profit*, which was named by 36 of the 53 people that answered this question. From the remaining 17 responses, five also had financial motives. Only nine people had a purely financial motive, four owned cryptocurrencies for fun only, and one for idealistic reasons. In general, idealistic reasons were the third most important motive to own cryptocurrencies.

Participants that own or owned cryptocurrencies were asked their motives to choose a specific currency. The main motives were the specific technology behind a cryptocurrency and popularity, followed by more financial motivation like coin value. The developers' vision was more important than security and privacy together, showing that idealism was also a theme when choosing a currency.

Motives to not own cryptocurrencies anymore were filled in by past users. They were mostly financial ones, like reaching a set goal or needing the money. The most common non-financial motive was the lack in a cryptocurrencies usefulness as actual currency.

TABLE 9. MOTIVES OF CRYPTOCURRENCY USAGE

Motives to own cryptocurrencies	Count
For profit	36
For fun	30
Idealistic reasons	14
As a security	6
To use as currency	5
For work/research	3
Other	2
Motives to own a specific cryptocurrency	
Technology	27
Popularity	23
Coin value	18
Previous value developments	16
Developers vision	14
Market Cap	13
Security	6
Privacy	5
Other	9
Motives not to earn cryptocurrencies anymore	
Reached required profit	6
Not useful enough as currency	5
I spent them	4
I needed money	3
Too much value loss	2
Sold at break even point	1
Too little value gain	1
I lost them	1
Time commitment	1
Motives to never own cryptocurrencies	
Too much risk	15
Too much knowledge required	8
Too much effort	8
Not enough money	5
Not useful as currency	4
Too technical	2
Not allowed to	1

The primary motive of the participants that only considered cryptocurrencies, but never bought them, was the risk involved with the usage of cryptocurrencies. Other important reasons were restrictions like *too little knowledge*, *too little money*, or *too much effort* needed to be able to own cryptocurrencies. All motives can be seen in table 9.

6.1.3. Timing. Contrary to the expectation that the media hype around cryptocurrencies led to new users, a significant amount of people (25, 46.3%) acquired cryptocurrencies before July 2017. In figure 2 we can see only a small rise at the end of 2017 and the beginning of 2018. At this point, cryptocurrencies were at their highest value.

Four of the people not owning cryptocurrencies anymore (n = 14) bought and sold them before July 2017. The rest sold, lost, or spend their cryptocurrencies between October 2017 and October 2018. There was a slight indication of more activity at the end of 2017 and the beginning of 2018. Interestingly, the trend became more clear when also including users who still have cryptocurrencies on the question when they spent their cryptocurrencies. This is possible as

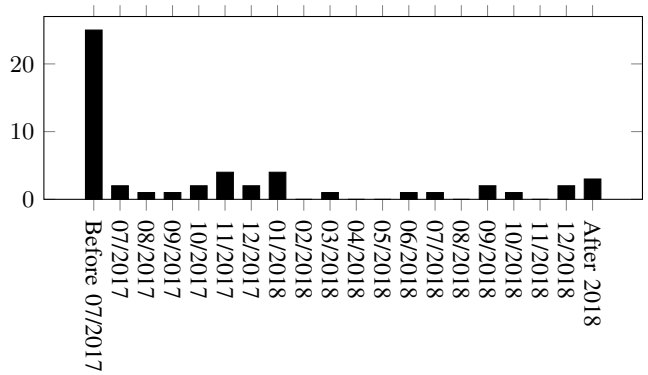


Figure 2. When respondents bought their cryptocurrencies (n = 49)

the question was mistakenly also shown to users who did not yet sell all of their cryptocurrencies. We also observed that the total amount invested in cryptocurrencies was higher when cryptocurrencies were bought while the coin value was high.

6.2. Security perception

In the following, the parts of the security perception construct are described and analyzed for differences between the cryptocurrency usage groups *present*, *past*, and *considered* (dependent variable).

6.2.1. General cryptocurrency knowledge. Knowledge was measured on a scale from 0 to 7. The maximum score achieved by a participant was 6. The mean score was 2.36 (SD=1.94). The more technical the question, the worst participants performed. In the third question, eleven people chose the fake consensus protocol (proof of transparency), which is 17% of all people who answered the question. Three of these ten only checked the fake consensus protocol. Also, more people chose the false protocol than the existing 'proof of elapsed time', which was only checked by two people with valid answers. An ANOVA on the means between groups showed that the present group scored significantly better in knowledge compared to the considered group (see table 10).

6.2.2. Classification into gambling/investment. The classification score had a mean value of 44.01 (SD=24.79), meaning participants were slightly leaning towards the gambling classification (mean difference= -5.99; t=-2.13 *P<.04). There was a significant difference between groups in the ANOVA analysis (see table 10). The present group scored significantly higher than the considered group.

6.2.3. Trust. Trust in cryptocurrencies was measured on a scale from 0 to 100. The range of trust was as big as the scale, with a mean of 51.17 and a standard deviation of 26.47. This data suggested that the sample did not lean to either trust nor distrust of cryptocurrencies. People who own or have owned cryptocurrencies had higher trust than

TABLE 10. ANOVA RESULTS FOR THE SECURITY PERCEPTION DIMENSIONS

Dimension	F-value	Mean difference	SD	Sig.
Knowledge	8.39**			.00
present-considered		1.78***	0.44	.00
Classification	3.25*			.04
present-considered		15.54*	6.01	.03
Trust	7.82**			.00
present-considered		24.26**	6.15	.00
Accuracy	1.41			.25
Estimation Direction	8.08**			.00
present-considered		-17.75***	4.44	.00

TABLE 11. MEANS AND RANGE OF ALL ACCURACY AND ESTIMATION DIRECTION DIMENSIONS

Dimension	Mean	SD
Accuracy (0 to 100)		
Likelihood	38.04	10.91
Financial Impact	42.88	22.14
Impact on Trust in Technology	42.19	11.14
Impact on Trust in Cryptocurrencies as a Currency	47.66	15.19
Estimation direction (-10 to 10)		
Likelihood	-1.94	2.50
Financial Impact	-2.88	4.12
Impact on Trust in Technology	0.15	5.06
Impact on Trust in Cryptocurrencies as a Currency	1.39	5.06

those who never owned them, although only the difference between the present and considered group was statistically significant (see table 10).

6.2.4. Risk awareness. In this part, the results for two dimensions of risk awareness are given.

Accuracy On the 0-71 accuracy score, the mean score for all participants was 31.01 (SD=7.17). This mean was slightly better than the expected value for guessing (35.5), with a mean difference of -4.38 (t=-5.29; ***P<.001). There were no significant difference in the accuracy score between groups (see table 10).

Estimation Direction On the scale reaching from -55 to 55 participants scored a mean of -5.88 (sd=18.26). The highest score was 44, the lowest -47. The whole sample underestimated risks (mean difference=-5.88; t=-2.19; **P<.01). People who own cryptocurrencies, as well as those who owned them tended to underestimate risks while people who only considered them slightly overestimated the risks. A comparison of means per group can be found in table 10. Contrary to the accuracy score, the differences between the present and the considered group were significant.

Detailed analysis of the risk awareness dimension Next to the overall risk awareness scores the four dimensions of it were invested to gain detailed insight in which impacts weigh most for users. The dimensions were: likelihood, impact on finances, impact on trust in the technology, and impact on trust in cryptocurrencies as a functioning currency.

Table 11 shows the mean scores per dimension. Accuracy of likelihood was best and accuracy for impact on cryptocurrencies as a currency worst. At the estimated directions, likelihood and financial impacts were underestimated and the impact on trust as cryptocurrencies as a currency overestimated. The impact on trust in the cryptocurrency technology was the only one not significantly different from 0 (P=.68), which means that it was estimated correctly on average.

Next, a dependent sample t-test was used to check whether the different accuracy dimensions and estimation directions are scored significantly different per subject. This is done to check whether the likelihood and different impacts were perceived as different concepts. This is the case for all comparisons but the one between accuracy of financial impact and accuracy of impact on trust in the cryptocurrency technology.

An ANOVA for differences between groups showed that the dimensions mostly behave like the global scores. Only the accuracy scores of impact on fiances were significant (F=3.20; *P<.05). The difference is between the present and considered group (mean difference=14.21; SD=5.71; *P=.04). While all other estimate direction scores were lowest for the present group and highest for the considered group, likelihood was underestimated worst by the considered group. It was the only estimation direction dimension that did not show a significant difference between the present and considered users. The differences of the other groups were significant for impact on finances (mean difference: -3.25; SD=1.04; *P=0.01), impact on trust in the technology (mean difference: -5.19; SD=1.21; ***P<.001) and trust in cryptocurrencies as a functioning currency (mean difference: -4.70; SD=1.24; **P=.001).

6.3. Multinomial Logistic Regression

A multinomial logistic regression was run to test the effects of security risk perception and demographics on the decision to use cryptocurrencies. All variables were entered at the same time. The regression model fitted the data with a significance of ***P<.001. 57.7% of the variance was explained by the model. There were three univariate outliers in estimation direction and one in accuracy. As removing these outliers did only slightly better the significances of the already significant variables as reported in table 13, they are not removed from the dataset. There were no multivariate outliers.

With the proposed model, 78% of all cases classified correctly. The present and considered group were distin-

TABLE 12. CLASSIFICATION TABLE OF THE LOGISTIC REGRESSION (N=69)

Observed	Predicted			
	Present	Past	Considered	Correct
Present	33	0	3	91.7%
Past	3	5	4	41.7%
Considered	2	3	16	76.2%
Overall	55.1%	11.6%	33.3%	78.3%

guished nearly perfect, while the past group in between was not classified very well. See table 12.

The results of the regression are shown in table 13. Between the present and past group, knowledge was the only significant contributor, with higher knowledge in the present group. There were more significant differences between the present and the considered group. The only demographic variable that contributed significantly to the model was age. Participants that were older decided to use cryptocurrency more often than younger participants. From the five security risk perception variables knowledge, trust, and risk estimation direction were significant. Current cryptocurrency users tended to have higher knowledge, more trust in cryptocurrencies, and are underestimating risks compared to participants that only considered owning them. The contributions of risk accuracy and classification were not significant.

Because of the earlier indications that classification influenced cryptocurrency usage, its high significance value in the regression was surprising. Further analysis showed that classification was significantly correlated with trust (.68; ***P<.001). Rerunning the regression without trust, changed the effect of classification into a significant one (B=-0.31; *P=.03; Exp(B)=0.96), meaning that participants that had cryptocurrencies during the study were more likely to classify them as an investment than those participants that did never own cryptocurrencies. The significance of the other variables remained unchanged, but correct classification into the three groups dropped to 70.4%.

6.4. MANOVA on the influence of the hype on security risk awareness

A MANOVA was run to see whether the hype around cryptocurrencies did have an impact on security risk awareness. There was a statistically significant difference in security risk awareness based on the acquisition time, F (2, 44) = 3.27, *P<.05; Wilk's $\lambda = 0.87$, partial $\eta^2 = .13$. The hype groups were the only groups in the analysis that had a significant difference on accuracy. The mean score of participants that bought cryptocurrencies during the hype was 3.43 (SD=2,02; t=-1.71, *P<0.05) points higher than the score of participants who bought them before or after the hype.

6.5. Revisiting Hypothesis and Model

After the analysis of the influences of security perception and demographics on cryptocurrency usage, we reject the hypothesis that gender (H5a) and level of education (H5c) affect cryptocurrency usage. We found indications for effects of classification (H1), so we accept their influence with the remark that their effect also seems to be explained by general trust. We accept the hypothesis that knowledge (H0), trust (H2), risk estimation (H3), and age (H5b) influence cryptocurrency usage. The hypothesis that the hype affected security risk awareness (H4) is also accepted. See table 14 for an overview. Figure 3 shows the revised model based on our findings. Gender and education are no longer included in the model. Attitude based on classification is still present, but they are affected by trust and therefore their own effect on the usage decision can be omitted in favor of trust. Risk awareness is split into its two dimensions. Estimation direction which does have an effect on usage, and accuracy which was impacted by the hype.

TABLE 13. VARIABLE EFFECTS OF THE LOGISTIC REGRESSION (N=69)

Group[1]	Parameter	B	Sig.	Exp(B)
'Past'	Intercept	3.93	.25	
	Knowledge*	-0.45	.05	0.64
	Classification	-0.01	.47	0.99
	Trust	-0.02	.48	0.99
	Accuracy	-0.07	.38	0.93
	Estimation direction	0.03	.46	1.03
	Age	-0.16	.13	0.85
	Gender (male)	1.52	.21	4.57
	Gender (female)	0[2]	.	.
	Education (less than High School)	0.99	.49	2.71
	Education (Bachelors' or Professional Degree)	-0.33	.77	0.72
	Education (Masters' Degree or higher)	0[2]	.	.
'Considered'	Intercept	5.04	.11	
	Knowledge**	-0.65	.01	0.52
	Classification	-0.01	.64	0.99
	Trust*	-0.06	.02	0.95
	Accuracy	0.02	.83	1.02
	Estimation direction*	0.07	.04	1.08
	Age*	-0.14	.02	0.87
	Gender (male)	0.97	.32	2.64
	Gender (female)	0[2]	.	.
	Education (less than High School)	-0.38	.79	0.69
	Education (Bachelors' or Professional Degree)	-1.56	.11	0.21
	Education (Masters' Degree or higher)	0[2]	.	.

[1]The reference group is: 'Present'
[2]This parameter is set to zero because it is redundant

7. Discussion

This research set out to shed light on the security risks concerning the usage of cryptocurrencies, both from a technical point of view as well as their perception by (intended) cryptocurrency users. Two studies were conducted to establish security risks, to see how the hype around

TABLE 14. HYPOTHESIS

Hypothesis	Accept/Reject
H0: *High knowledge is expected to result in higher cryptocurrency usage.*	Accept
H1: *A positive attitude is expected to result in higher cryptocurrency usage.*	(Accept)
H2: *Higher trust is expected to result in higher cryptocurrency usage.*	Accept
H3: *A higher risk awareness is expected to result in less cryptocurrency usage.*	Accept
H4: *We expect to find a difference in risk awareness based on cryptocurrency acquisition time.*	Accept
H5: *Demographics*	
H5a: *We expect a higher prevalence of male cryptocurrency users.*	Reject
H5b: *Higher age is expected to result in higher cryptocurrency usage.*	Accept
H5c: *Higher education is expected to result in higher cryptocurrency usage.*	Reject

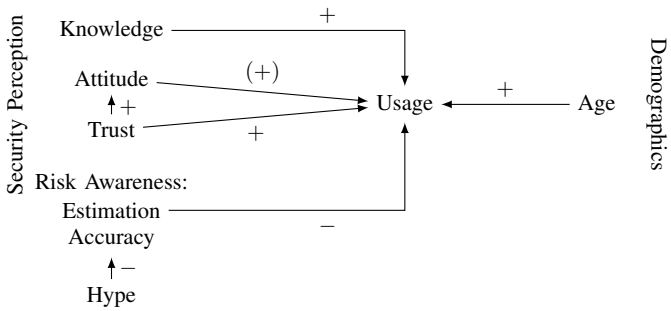


Figure 3. Revised Model of the security perception construct and the measured effect of its dimensions on cryptocurrency usage

cryptocurrencies influenced security risk awareness, and to research how security perception influences the decision to use cryptocurrencies. In the following section, we will discuss the results.

The most pressing (financial) risks were found in the environment of cryptocurrencies. This is not surprising, as every exchange or other external service adds a third party, which is not bound by the blockchain, to the equation. The necessity of a third party which lies outside the trusted blockchain [9], combined with no regulations and the irrevocable nature of cryptocurrencies, is an attractive state for criminals [8].

Besides the environment, the difference between impacts is noteworthy, too. Although the impact on trust in cryptocurrencies should be low theoretically, this was not the case for the participants. The participants in this study did not seem to make a difference between the cryptocurrency itself and the other technologies they utilize to use them. They rather had a single concept of cryptocurrencies which included all components.

The fact that the trust-related impacts were estimated higher than impacts on finances and likelihood is in line with the findings of Walton et. al. [20], that trust-related risks affect the intention to use cryptocurrencies. The combination of high risk estimation in trust, high risk estimation in the environment, and the conceptualization of cryptocurrency and its environment as one, shows the importance of the lack of safety stemming from the added third parties needed to use cryptocurrencies.

Risks in the environment are primarily possible because of missing regulations of cryptocurrencies. This is a positive problem on the one hand, as regulations are flexible and can be added without changes to a blockchain. On the other hand, regulations are slow, especially with new technologies. Furthermore, regulations are against the unregulated, decentralized character of cryptocurrencies. Sas et. al. [3] found that people were undecided about the regulation of cryptocurrencies. They also found that cryptocurrencies are still used as an investment tool rather than a currency. Our results show that this is not surprising, given the high estimation of risks related to the environment.

Following and based on the risk study, we set out to research how differences in perception and risk awareness in particular influence the decision to use cryptocurrencies. We found significant effects for risk estimation, knowledge, trust, classification, and age. Risk accuracy, gender, and education did not prove to have significant effects on usage in this study.

While we expected to find the other effects, the risk awareness estimation effect was less obvious to find as it had not yet happened in the literature, although being hypothesized. Reasons for the findings might be that we measured actual usage instead of intended usage, as well as the difference in our methodology. Arias et. al. [18] stated that participants perceived the risks around cryptocurrencies as high throughout which led to little distinctive power. Our study focused on concrete technical scenarios rather than questionnaires about general risk perception. Using technical scenarios instead of general questions on the risk perception of cryptocurrencies gives more nuance to risk perception and mitigates the problem that all risks are perceived as high.

Knowledge was the only factor that had a significant effect between the present and past group added to the effect between the present and considered group. One explanation for this might be the time of acquisition. Many past users bought cryptocurrencies early when they still were cheap and therefore more of a game than a financial investment. Because of this, there was no need to build knowledge of the technology before purchasing. Knowledge is of interest when wanting to further cryptocurrency usage, as it might be raised rather easily since it is less complex and dependent on general character than trust.

Participants scored high impacts on their trust in cryptocurrencies, especially for their use as a payment method for attacks on the environment. This is noteworthy as logically, these impacts should not exist. We argue that cryptocurrencies will not be widely adopted as a real currency unless the environment is changed to be more trustworthy and less prone to attacks.

Classification had a significant effect on cryptocurrency usage when omitting trust from the model. This, as well

as the strong correlation of the two concepts, indicated that they measure a similar concept. Trust is vital in forming an attitude towards products [30]. Because of these findings and the fact that trust is the stronger one of the two variables, we argue that classification is a facet of trust rather than a distinct concept.

There was no significant effect of gender in this study when comparing the decision to use cryptocurrencies. This means that men were not more likely to use cryptocurrencies compared to women. One of the reasons for this could be that this study investigated the decision to invest, rather than the amounts invested and won/lost. Another reason could be the small fraction of female participants.

As with gender, the expected effects of education could not be found. We attribute this to the explanatory power of age, as well as the generally young age of the participants. With a mean age of around 28, the sample had a lot of current students in it, which means that a degree is pursued but not yet obtained by many of the participants. With a broader sample across the population, the effects of education might be present.

The effect of age on the decision to use cryptocurrencies is likely due to financial stability. While students and young adults have to be careful about their expenses, older participants have the financial stability and freedom to take more risks.

Another question this paper addressed is whether the attention around cryptocurrencies has an effect of risk awareness of (possible) users. The results showed that there is indeed a difference in risk awareness based on time of acquisition. This effect is found on accuracy, the risk awareness dimension that did not have a significant impact on the decision of whether or not to use cryptocurrencies. In turn, estimation direction predicted cryptocurrency usage but was not significantly influenced by the hype. The reason for these findings might be that the hype was the deciding factor for some people that were already considering cryptocurrencies for a while. If their risk awareness accuracy was lower, to begin with, the hype could be enough to motivate them to make the decision. People with higher risk awareness accuracy, on the other hand, might be less affected by external attention on cryptocurrencies and make their decision independent of those factors.

We see the reason why risk estimation is not significantly affected by the hype but affects the usage decision in the fact that accuracy is about knowing risks exist, while estimation is about how much importance you give to them. From this, it seems logical that importance weighs more in deciding to use a specific technology. Knowing something, on the other hand, costs more (mental) effort, for example through researching. Therefore, it is a metric that has to be established actively. This might not happen when time is a crucial factor because of extreme changes in market value. Based on the different grouping for cryptocurrency usage and hype groups, it is not possible to know whether the hype influenced the decision to use cryptocurrencies.

Next to discussing risks and security perception, this research also gave an overview of the use of cryptocurrencies in general. First of all, our overall sample in this research did not fit the profile of hype followers. Half of all participants purchased cryptocurrencies before July 2017. In the other half, we observed only a slight increase in months with high coin-values. Furthermore, most of the participants in this study used more than one wallet. They preferred one online and one offline wallet. This indicates tech-savviness and security considerations on a non-trivial level.

Based on the demographic trends in education and age as well as motives for cryptocurrency usage we argue that cryptocurrency usage is still in the early adoption phase of Rogers' innovation adoption curve [31]. It is not yet perceived as safe enough for users without financial security, specific knowledge, and a high risk tolerance. As long as the use of cryptocurrencies is dependent on technical knowledge and can only be used in a (perceived) risky environment, majority adoption is unlikely.

8. Limitations and Future Work

There was little differentiation between the likelihoods of attacks, as they were nearly all classified into *medium*. One reason for this is that there were no real numbers on attack prevalence present. The reliance on theoretical possibility and media attention of a specific attack might skew the results. Further research into security risks on cryptocurrencies should focus on a better understanding of the likelihood of attacks.

Although we were able to make some remarks about the influence of the hype on security risk awareness, there were some limitations in this study regarding these findings. The first was that the sample mostly included participants that had cryptocurrencies before the growth in attention and value. Second, our definition of hype users had no solid basis as the concept is not defined scientifically. Further research in this direction should try to recruit more users joining during the rapid value developments. The classification if someone did join because of the hype could be improved by not only querying the month of acquisition but also a day or coin value. With this data, there is much more basis for the analysis, and it would also be possible to see whether the value was increasing or decreasing at the time of purchase. This study decided against a detailed question on acquisition time/value because of the already elaborate questionnaire that had other main focuses. Finally, there was no possibility to measure whether the hype influenced cryptocurrency usage. To do this, either pre- and post measures would be needed, or participants would have to answer retrospective questions on this influence.

Another limitation of this study was the methodology used for users' classification of cryptocurrencies. The classification into gambling and investment left out the third possible classification which is speculation. Speculation is conceptual between gambling and investment and shares characteristics of both [14]. Especially as the sample was only slightly leaning to gambling, the addition of speculation might add to the explanatory power of classification on usage. However, the results of this study showed that

classification does not have added explanatory power when trust is measured, too. Consequently, if classification is not of interest on its own it can be omitted in favor of trust.

Furthermore, there was a high overlap in possible motives to own cryptocurrencies, which made it impossible to include them in any meaningful analysis. To be able to include them, motives would either need to be collected by only asking for the most important one, or by scoring the different motives on their importance.

9. Conclusion

This study researched vulnerabilities in cryptocurrencies, the corresponding risks, how a person's security risk perception influences the decision of whether to use cryptocurrencies or not and how the hype influenced security risk awareness.

We found that most risks were in the environment around cryptocurrencies which is composed of trusted third parties. This might be a cause for slow adaption, as the environment is not regulated - and some people also do not want it to be - but problems in the environment will influence the users' trust in the cryptocurrency itself as they see both as one concept.

Security did play a role in the decision to own cryptocurrencies. Besides estimating risks as less severe, cryptocurrency users tended to have more trust and knowledge of cryptocurrencies. Especially the effect of risk estimation is noteworthy, as previous studies were not able to find a significant influence of risk perception on intended cryptocurrency usage. The reasons for the different results are seen in the technical way of measuring risk perception, as well as the test on actual rather than intended usage.

The hype around cryptocurrencies had some influence on security risk awareness. From this research, it is not to say whether it also influenced the usage decision.

Additional to these findings, we reported how people use cryptocurrencies, which can be used as a basis for further research.

Acknowledgments

The author would like to thank the supervisors of this Master's thesis, all participants that took the time to take the survey, and everyone who gave feedback on the draft versions.

References

[1] H. Spenkelink, "The adoption process of cryptocurrencies-identifying factors that influence the adoption of cryptocurrencies from a multiple stakeholder perspective," Master's thesis, University of Twente, 2014.

[2] A. W. Baur, J. Bühler, M. Bick, and C. S. Bonorden, "Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co," in *Conference on e-Business, e-Services and e-Society*, Springer, 2015, pp. 63–80.

[3] C. Sas and I. E. Khairuddin, "Exploring trust in bitcoin technology: A framework for hci research," in *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, ACM, 2015, pp. 338–342.

[4] P. V. J. da Gama Silva, M. C. Klotzle, A. C. F. Pinto, and L. L. Gomes, "Herding behavior and contagion in the cryptocurrency market," *Journal of Behavioral and Experimental Finance*, vol. 22, pp. 41–50, 2019.

[5] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th annual conference on privacy, security and trust (PST)*, IEEE, 2016, pp. 745–752.

[6] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[7] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, IEEE, 2015, pp. 104–121.

[8] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of bitcoin-exchange risk," in *International Conference on Financial Cryptography and Data Security*, Springer, 2013, pp. 25–33.

[9] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electronic commerce research and applications*, vol. 29, pp. 50–63, 2018.

[10] J. E. Grable, "Financial risk tolerance and additional factors that affect risk taking in everyday money matters," *Journal of business and psychology*, vol. 14, no. 4, pp. 625–630, 2000.

[11] S. H. Lim, D. J. Kim, Y. Hur, and K. Park, "An empirical study of the impacts of perceived security and knowledge on continuous intention to use mobile fintech payment services," *International Journal of Human–Computer Interaction*, vol. 35, no. 10, pp. 886–898, 2019.

[12] C. Bannier, T. Meyll, F. Röder, and A. Walter, "The gender gap in 'bitcoin literacy'," *Journal of Behavioral and Experimental Finance*, vol. 22, pp. 129–134, 2019.

[13] A. S. Hornsby, *Oxford advanced learner's dictionary*. Oxford University Press, 2005, vol. 7, p. 85.

[14] J. N. Arthur, R. J. Williams, and P. H. Delfabbro, "The conceptual and empirical relationship between gambling, investing, and speculation," *Journal of behavioral addictions*, vol. 5, no. 4, pp. 580–591, 2016.

[15] C. Sas and I. E. Khairuddin, "Design for trust: An exploration of the challenges and opportunities of bitcoin users," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, 2017, pp. 6499–6510.

[16] P. Binde, "Why people gamble: A model with five motivational dimensions," *International Gambling Studies*, vol. 13, no. 1, pp. 81–97, 2013.

[17] C. Lustig and B. Nardi, "Algorithmic authority: The case of bitcoin," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, IEEE, 2015, pp. 743–752.

[18] M. Arias-Oliva, J. Pelegrín-Borondo, and G. Matías-Clavero, "Variables influencing cryptocurrency use: A technology acceptance model in spain," *Frontiers in Psychology*, vol. 10, 2019.

[19] J. C. Mendoza-Tello, H. Mora, F. A. Pujol-López, and M. D. Lytras, "Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments," *IEEE Access*, vol. 6, pp. 50 737–50 751, 2018.

[20] A. Walton and K. Johnston, "Exploring perceptions of bitcoin adoption: The south african virtual community perspective.," *Interdisciplinary Journal of Information, Knowledge & Management*, vol. 13, 2018.

[21] J. F. Graham, E. J. Stendardi Jr, J. K. Myers, and M. J. Graham, "Gender differences in investment strategies: An information processing perspective," *International journal of bank marketing*, vol. 20, no. 1, pp. 17–26, 2002.

[22] N. Nicholson, E. Soane, M. Fenton-O'Creevy, and P. Willman, "Personality and domain-specific risk taking," *Journal of Risk Research*, vol. 8, no. 2, pp. 157–176, 2005.

[23] C. C. Eckel and P. J. Grossman, "Sex differences and statistical stereotyping in attitudes toward financial risk," *Evolution and human behavior*, vol. 23, no. 4, pp. 281–295, 2002.

[24] N. Parashar, "An empirical study on personality variation and investment choice of retail investors," *Journal of Management and Information Technology*, vol. 2, no. 1, pp. 33–42, 2010.

[25] A. Chaudhuri and L. Gangadharan, "Gender differences in trust and reciprocity," 2003.

[26] J. Felton, B. Gibson, and D. M. Sanbonmatsu, "Preference for risk in investing as a function of trait optimism and gender," *The journal of behavioral finance*, vol. 4, no. 1, pp. 33–40, 2003.

[27] T. Hasso, M. Pelster, and B. Breitmayer, "Who trades cryptocurrencies, how do they trade it, and how do they perform? evidence from brokerage accounts," *Journal of Behavioral and Experimental Finance*, vol. 23, pp. 64–74, 2019.

[28] W. Bruine de Bruin, W. VanderKlaauw, J. S. Downs, B. Fischhoff, G. Topa, and O. Armantier, "Expectations of inflation: The role of demographic variables, expectation formation, and financial literacy," *Journal of Consumer Affairs*, vol. 44, no. 2, pp. 381–402, 2010.

[29] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, 2018.

[30] B. Hultén, "Customer segmentation: The concepts of trust, commitment and relationships," *Journal of Targeting, Measurement and Analysis for Marketing*, vol. 15, no. 4, pp. 256–269, 2007.

[31] E. M. Rogers, *Diffusion of innovations*. Simon and Schuster, 2010.