Proceedings of the 3rd International Conference on Financial Technology and Business Analysis
DOI: 10.54254/2754-1169/149/2024.19259

# *Analysis of the Realization for Trading Security of Cryptocurrency*

**Tianyu Zhang**[1,a,*]

*[1]Department of Computer Science, Carleton University, Ottawa, Canada*
*a. TianyuZhang7@cmail.carleton.ca*
**corresponding author*

***Abstract:*** With the advancement of digital economy as well as network technology, blockchain was gradually becoming an important driving force for development of different areas. Data on blockchain is stored in a way which is transparent, cannot be changed easily, and does not need to rely on centralized control. Cryptocurrency, which works through blockchain, was showing broad prospects for its use in finance, supply chains, healthcare, and other sectors. Blockchain's application in cryptocurrency is one of the more significant ones. The financial system that existed before faced many problems, and cryptocurrency introduced a new financial service model. While cryptocurrency development has created opportunities, challenges related to transaction security also have been brought along. Researchers work to find algorithms that are new, consensus methods and other protection strategies, to deal with security risks like hacker activity, transaction fraud, and manipulation of the market. These security risks were being addressed through these efforts which, by improving the safety of cryptocurrency itself, would give protection to enable its more widespread use in future. The significance of this paper is found in how it systematically looks at cryptocurrency transaction security, analyzing its safety as well as demonstration of the ways current security measures work and what cost comes with ensuring such safety. This will help dig deeper into the security of cryptocurrencies, and offer references for stable growth of cryptocurrency markets in the future.

***Keywords:*** Cryptocurrency transaction security, blockchain technology, consensus mechanisms, security challenges and costs, regulation and future outlook.

## 1. Introduction

The historical development of blockchain technology and research history of blockchain starts from late 1980s. Leslie Lamport, in 1989, made the Paxos protocol, which is about achieving agreement in unstable networks. Afterward, somewhere in the 1900s, Bayer and others proposed the signed chain of information, contributing to further development of electronic ledger systems and establishing groundwork for the immutability of data [1]. This research from Bayer et al. laid the groundwork for data security technology and what later became known as distributed ledgers and blockchain technology. Later, three main optimizations were made to the electronic ledger's data structure, like using hash functions instead of signatures for links, grouping documents in blocks to lessen complexity, and using binary Merkle tree structure within blocks to link transaction hash pointers [1].

Following these developments, some forms of electronic currencies like ecash, bmonie, and Bit gold were created but none saw wide adoption [1].

The field saw major change only in 2008, when Satoshi Nakamoto introduced Bitcoin’s white paper, based on a refined electronic ledger system that used proof-of-work (PoW) for network security [2]. This PoW method, a cryptographic method originating from Cynthia Dwork and Moni Naor in 1992, was used to secure networks [1]. Bitcoin and blockchain's main advantage over earlier electronic money systems was that it was decentralized and had no single control point [1]. Even though, proof-of-work has been criticized because of high power consumption, leading to introduction of proof-of-stake (PoS) and delegated proof-of-stake (DPoS) mechanisms as improvements [3]. Eventually, smart contracts came into play in blockchain, allowing decentralized apps to be created [3]. Bitcoin’s success showed that blockchains had feasible real-world uses, making developers and researchers more interested in exploring blockchain. This expanded blockchain research beyond cryptocurrency into new areas. This shift wasn’t just about moving from cryptocurrencies but also showed researchers were focusing on inefficiencies and challenges of blockchain tech [4]. These problems included technical architecture, security, privacy, and network safety concerns [3]. Moreover, research focus also started including service provision and how to apply technology in various areas [3].

Current research on cryptocurrencies is showing a steady growth. This growth is reflected in the breadth of cryptocurrency research. Literature indicates that cryptocurrency-related research covers qualitative, quantitative, and mixed research methods [5]. The variety of research approaches demonstrates the broad interest in cryptocurrencies among academics. In addition, cryptocurrencies are an important financial innovation. This is because cryptocurrencies enable decentralized financial transaction management through blockchain technology and verify the validity of transactions without the control of a single institution [6]. Cryptocurrencies can also be used as an investment vehicle. Despite the volatile nature of the cryptocurrency market, cryptocurrencies show great investment potential as a safe-haven asset in an environment of global economic uncertainty [7].

Cryptocurrencies have become widely noticed from the time they came up as a type of digital money. The thing that makes cryptocurrencies run is blockchain technology. With this technology, what cryptocurrencies do is bring decentralization and make things more open for everyone. Though as cryptocurrencies grew more used by people, what happens is transaction safety has become one big problem. In recent times, studies on cryptocurrency and blockchains have leaned towards security matters. That change in research focus has made transactions safer to an extent, but hacking attempts and fraud still give problems, and people can lose their cryptocurrency money. What most research does is talk about the basic structure of blockchain and how encryption techniques are made. But how to make things more secure when there are so many transactions happening and attacks are getting harder to handle is still something to look at more. This research aims at talking about security-related algorithms for cryptocurrency and figuring out how to make use of them. Risks that are left in cryptocurrency trades and the expense of putting security in place are also looked at. Discussing the ways to use algorithms and looking into risks can give something to think about for the future when trying to make cryptocurrency transactions safer. The subsequent sections will explain blockchain and technologies. Some uses of them are talked about. Blockchain has been used in different areas, some examples are given for those. What blockchain can do has been described in different fields with applications. Afterward, cryptocurrency security algorithms are introduced, and then how these algorithms work is discussed. The usage of algorithms in securing crypto transactions is important and examples of such uses have been provided. Cryptocurrency transaction risks are still there, some of them remain. Costs that come with securing the transactions are talked about, which make sure the transactions are safe, but at a certain price. Lastly, the findings are summarized and also what these mean for future security of crypto transactions is mentioned. How research can affect the future of security in crypto transactions is discussed.

## 2. Basic Descriptions of Blockchain Techniques

Blockchain is defined as a decentralized distributed ledger technology. The basic principle of a blockchain is that a series of transactions are connected to each other in chronological order and form a chain that cannot be tampered with. The transaction records kept in a blockchain can also be understood as blocks [8]. Blockchain includes a variety of related technologies, including, but not limited to, blockchain types, cryptography, consensus mechanisms, data structures, P2P network technologies, smart contract technologies, privacy-preserving algorithms, and interoperability protocols [9]. With the development of technology, blockchain has been widely used in many fields, including but not limited to chained financial systems, supply chain management, Internet of Things (IoT), energy management, education, and healthcare.

Blockchain is divided into three types, i.e., public blockchain, private blockchain, and federated blockchain. Public blockchain refers to a type of blockchain that is completely open and can be participated by anyone. A public blockchain is decentralized and transparent. However, public blockchains have the disadvantages of slow transaction speeds and the high energy consumption of public blockchains. This makes public blockchains suitable for deploying cryptocurrencies like Bitcoin and Ether and for deploying decentralized applications on the blockchain [8, 9]. Private blockchain refers to a blockchain that can be accessed only by authorized members. A private blockchain is an efficient and controlled system and is often used within an organization. The advantages of private blockchain are efficiency and scalability. However, because private blockchains are intelligently accessed by authorized members, the security and trust of private blockchains depend on centralized management. The general application scenarios of private blockchain are internal enterprise systems, supply chain management, and settlement systems of financial institutions. A federated blockchain refers to a blockchain that is jointly managed by multiple organizations. This blockchain supports collaborative contracts between different organizations and is decentralized and transparent between public and private blockchains. This blockchain is used in supply chain management, cross-organizational financial transactions and joint data auditing systems [8, 9].

Cryptography is used in blockchain to ensure the security of transactions and data privacy. The part of cryptography that is used to secure transactions is asymmetric encryption algorithms such as RSA, ECC. Asymmetric encryption algorithms are used to encrypt transaction data on the blockchain. The encrypted transaction data can be decrypted with maximum assurance that only the recipient with the private key can decrypt the transaction data [9]. Furthermore, asymmetric encryption gives authenticity and traceability to blockchain transactions. Another application of cryptography in blockchain is hash functions, such as SHA-256 and SHA-3, which are used to generate a unique identifier for each block to ensure that the block data has not been tampered with [8]. In order to ensure the security and consistency of the de-intermediated blockchain, blockchains also use consensus mechanisms. Currently, mainstream blockchains use three consensus mechanisms. The three consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Data structure is one of the core components of a blockchain. Each block in a blockchain contains a block header and block data. The block header records the hash value and timestamp of the previous block. The block data is used to record transactions within the block. The combination of the two ensures that the blocks are organized according to time. (Using this hash-tree-like structure, each transaction in a block can be quickly verified, thus increasing the efficiency of data verification [9].

Smart contracts are one of the key innovations of the blockchain. Smart contracts allow the blockchain to automatically execute contracts based on predefined conditions [9]. Smart contracts act as a computer program that can execute transactions without the need for a third party to manage them [8]. Smart contracts in Ether are written in the solidity language [9]. Meanwhile, Vype, an alternative language to Solidity, focuses more on simplicity and security than Solidity [9]. This technology extends the use of the blockchain [8].

Blockchain relies on peer-to-peer network technology to disseminate data. Through P2P networking technology, the ability to verify transactions and generate new blocks is given to each node on the blockchain [9]. This means that the blockchain can use peer-to-peer network technology to ensure decentralization [9]. Privacy-preserving algorithms are also one of the important techniques in blockchain in order to avoid information leakage. Blockchains use zero-knowledge proofs (zk-SNARKs) to ensure that users can verify their knowledge of information without revealing specific identity information [9]. Subsequently, an upgraded version of zero-knowledge proofs (zk-STARKs) has emerged. This upgraded version is more scalable and transparent [9].

With the development of blockchain technology, blockchain technology has been extensively researched in the healthcare field. Blockchain technology has shown advantages in medical data management, health information exchange, insurance claims, clinical research, etc. [8]. Traditional medical data usually faces privacy issues such as data loss. Blockchain can rely on decentralized features and encryption algorithms to ensure data security and privacy issues [8]. This means that patients can securely share their health information with their doctors and can trace the use of the information in a timely manner [8]. Blockchain, as a distributed ledger, allows data to flow seamlessly between different organizations [8]. The blockchain can automate insurance claims by writing and executing contracts [8]. This means that the use of blockchain can reduce manual operations and increase the efficiency of claims processing. Blockchain facilitates global research collaboration through secure and efficient data sharing, privacy protection, and data validation [8].

## 3. Algorithms for Trading Security of Cryptocurrency

The underlying technology of cryptocurrencies is the blockchain [10]. This means that the security of cryptocurrencies is based on the blockchain technology platform and the support of the blockchain technology [10]. For the blockchain technology platform, the components related to the security of cryptocurrencies are the fundraising, the duration, the employees, and the consensus algorithm (seen from Fig. 1) [10]. The algorithmic component is the consensus algorithm in the blockchain. The main consensus protocols in blockchain include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (pBFT), and Stellar Consensus Protocol (Stellar). Stellar Consensus Protocol (SCP) [11, 12].

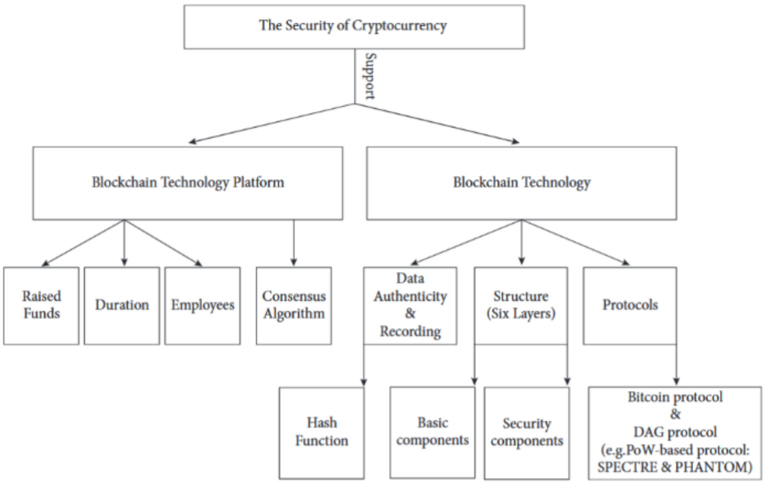
The Security of Cryptocurrency
Support
Blockchain Technology Platform
Blockchain Technology
Raised Funds
Duration
Employees
Consensus Algorithm
Data Authenticity & Recording
Structure (Six Layers)
Protocols
Hash Function
Basic components
Security components
Bitcoin protocol & DAG protocol (e.g.PoW-based protocol: SPECTRE & PHANTOM)

Figure 1: Framework for security of cryptocurrency [10].

Proof of workload works by having miners solve complex mathematical problems to validate transactions and generate new blocks [12]. Complex mathematical problems are usually hash calculations [10]. This consensus protocol forces an attack which requires the use of huge network resources in order to control the blockchain [10]. This means that proof of workload ensures decentralization and security of the blockchain [12]. The disadvantage of this consensus method is that it can be slow to transact, consumes a lot of energy and can be subjected to 51% attacks [12]. Proof of workload is used in the Bitcoin network [12]. Proof of stake works by determining whether a node can validate transactions and generate new blocks based on the number of tokens it holds [10]. This consensus protocol emerged as a replacement for proof-of-workload because it increases the efficiency of blockchain transactions by reducing the amount of energy consumed in verifying transactions [10]. In addition to increased efficiency, proof-of-work is characterized by fast block generation and high attack costs [12]. The disadvantage of this consensus protocol is that it concentrates the wealth on a few individuals [12]. This consensus protocol is used in Ether, Peercoin and NXT [12]. Delegated Proof of Equity is a consensus protocol similar to Proof of Equity pairs. The principle of this consensus protocol is that participants in the blockchain use voting to select nodes. The chosen node is responsible for new block generation and transaction validation [11]. The advantage of this consensus protocol is that it increases the speed of transaction processing. However, the selection of new nodes by voting may lead to over-centralization of power. Too much concentration of power represents the risk of centralization [11].

Practical Byzantine Fault Tolerance is characterized by allowing information to be agreed upon between the wrong node and the right node [12]. This consensus protocol is suitable for use in permission networks [12]. This consensus protocol is characterized by fast block generation and fast transaction processing [12]. However, Practical Byzantine Fault Tolerance prefers a centralized blockchain with a limited scope [12]. This consensus protocol is widely used in private and enterprise blockchains such as Hyperledger Fabric [11]. The Stellar Consensus Protocol is an open membership consensus protocol based on the Byzantine protocol [12]. Based on this protocol, participants in a blockchain choose which other participants to trust and form a trust list [12]. The trust list is called a quorum slice. Overlapping of different quorum slices in the blockchain will eventually lead to the formation of a quorum within the blockchain [12]. Consensus is formed when most of the members of the quorum agree [12]. This consensus protocol is characterized by prioritizing security [12]. This means that this consensus protocol can continue to operate in the presence of bad nodes [12]. To achieve this, the consensus mechanism sacrifices response time for security to ensure that more trusted nodes are involved in the decision [12]. For blockchain technology, the parts involved are data authenticity, blockchain structure and protocol. Among them, data authenticity and protocols have an impact on blockchain security. The technology used in blockchain to confirm the authenticity of data to ensure the security of blockchain is hash function. The hash function usually uses SHA-256 as the hash algorithm. Any data entering the SHA256 hash algorithm is mapped into a hash of 256 bits in length. The core value of the entire algorithm in ensuring authenticity is that no one can deduce the original number from the hash value. By generating a hash value for each block in the blockchain and concatenating each block, it is guaranteed that the data in the block cannot be tampered with. In addition, SHA256 is also used as a tool for generating digital signatures that can confirm the legitimacy of blockchain transactions [10].

Another key element of blockchain technology that impacts security is discussed next. There are two dominant protocols that secure blockchain transactions. The SPECTRE protocol is a proof-of-work (POW)-based directed acyclic graph (DAG) protocol, which is a blockchain data structure that guarantees that multiple blocks can be run and processed simultaneously. This data structure avoids the limitations of the traditional Bitcoin structure. This data structure allows for faster processing of transactions that occur on the blockchain. The combination of SPECTRE and the new data structure allows SPECTRE to be used to increase the maximum frequency of transactions, and SPECTRE can be used not only to increase the maximum speed of transactions, but also to handle forks in the blockchain. Finally, blockchain security and stability are further enhanced by the adoption of the SPECTRE protocol, which improves the resistance to double payment attacks and censorship attacks [10]. Similarly, the PHANTOM protocol is a DAG-based protocol. Unlike the SPECTRE protocol, the PHANTOM protocol is mainly used to solve the problem of smart contract execution, and it ensures the execution of smart contracts by allowing all blocks to be sorted linearly [10].

## 4. Risks and Costs for Trading Security of Cryptocurrency

Cryptocurrencies have received a lot of attention in recent years, but there are still many problems with the security of cryptocurrencies. In order to address cryptocurrency security issues, the industry has proposed a number of solutions to cryptocurrency problems. This paragraph discusses cryptocurrency security issues in the order of technical security challenges, transaction and market challenges, adoption challenges, and regulatory challenges. This is followed by a discussion of the costs of implementing cryptocurrency security. A framework diagram is shown in Fig. 2 [11].

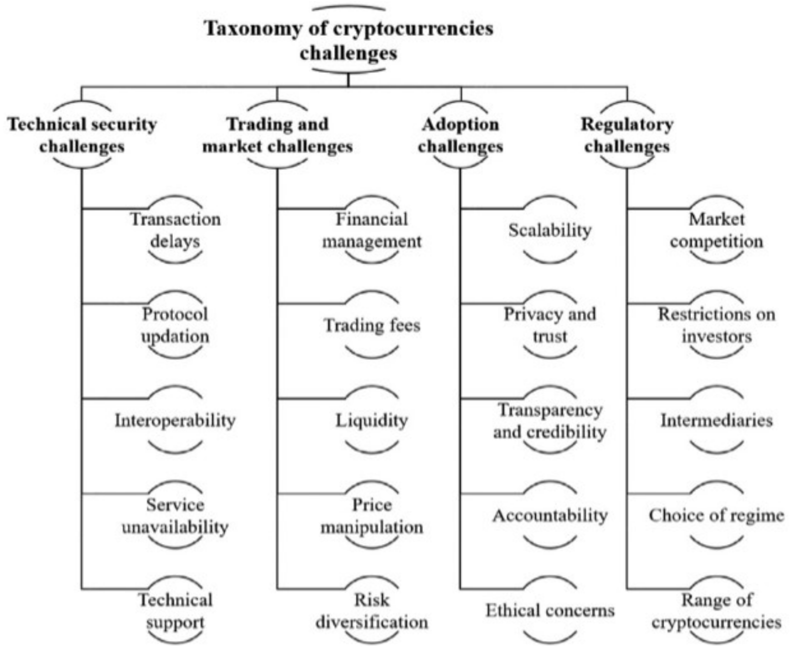

Figure 2: Challenges and risks for cryptocurrency [11].

Transaction latency is a key issue that cryptocurrencies in the network need to face. Because the block size of the blockchain in which cryptocurrencies are deployed is not infinite, the size of the blocks, and the congestion in the network are not always sufficient. The size of the blocks, the level of congestion in the network and the delay in the propagation of data through the blockchain all contribute to longer transaction confirmation times for cryptocurrencies. The increase in transaction times will not only inconvenience customers trading cryptocurrencies but will also lead to double-costing of the blockchain [11]. Another technical security issue for cryptocurrencies is the updating of the blockchain protocol. Inconsistent blockchain protocols across different network nodes may lead to a fork of the blockchain network. Forks in the blockchain network may lead to security vulnerabilities. Security vulnerabilities can be exploited by attackers to cause security problems in cryptocurrencies [11]. Blockchain interoperability can also lead to cryptocurrency security issues. As noted in Article, cryptocurrencies cannot circulate on blockchains other than the one in which they are deployed [11]. This complicates the management of multiple cryptocurrencies deployed on different blockchains. The complexity of managing cryptocurrencies increases the chance of errors and security breaches. Service unavailability can also lead to security issues for cryptocurrencies. The network services of a cryptocurrency service provider may be interrupted due to hardware failures, cyberattacks, or high transaction volumes. Termination of the network service may in turn prevent users from accessing cryptocurrency wallets and executing cryptocurrency transactions. The unavailability of such services can lead to property damage and reduce users' trust in the service provider [11]. Another security issue regarding cryptocurrency platforms is that the lack of support provided by cryptocurrency platforms to their customers contributes to cryptocurrency security problems. According to Article, users are vulnerable to security threats related to cryptocurrencies in the absence of adequate technical support [11, 12].

Cryptocurrencies are highly volatile in trading markets. Market volatility of cryptocurrencies poses a significant risk to the financial management of cryptocurrencies. Rapid fluctuations in cryptocurrency market sentiment, discussed in Article, can lead to large losses for investors [13]. This trend is significant among traders who use leverage [13]. Blockchain's transaction procedures can impede trading. Due to the nature of the blockchain, which requires miners to keep track of accounts, trading cryptocurrencies on the blockchain requires payment to miners. Transaction fees during peak times on the blockchain network can increase dramatically. This could result in the transaction fees for microtransactions and microtransactions being a significant portion of the transaction amount itself, or the amount of the fee being greater than the transaction itself. This makes micro- and micro-transactions economically impossible [11]. Some cryptocurrencies are less actively traded than others. This means that cryptocurrencies with low activity have low trading activity, fewer purchases, less trading volume, and less market depth. Cryptocurrency markets with low activity are susceptible to market manipulation. Market manipulation includes, but is not limited to, buying large quantities of cryptocurrencies to drive up the price and then selling large quantities of cryptocurrencies when the price is high [13]. The decentralized nature of cryptocurrencies has resulted in the lack of a regulator for cryptocurrencies. The lack of a regulator allows malicious traders to disrupt the cryptocurrency market. Malicious traders can manipulate the market price by using activities such as false pending orders. Cryptocurrency traders and investors can be misled by false market prices [13]. Some cryptocurrencies are highly correlated. The price of one cryptocurrency may affect the price of other related cryptocurrencies. The interplay between cryptocurrencies concentrates the risk of cryptocurrencies. Concentrated investment risk can magnify investment risk during market downturns [13].

Cryptocurrencies cannot be widely adopted due to the low scalability of the technology. The low scalability of cryptocurrencies is reflected in the fact that cryptocurrencies are not able to cope with the same scale of transactions as traditional payment systems by relying on the existing blockchain infrastructure. This makes it difficult to popularize cryptocurrency transactions in everyday life [11]. Transactions using cryptocurrencies on the blockchain require that the transaction information be broadcast to all nodes in the blockchain, which means that while the blockchain provides transparency of information and transactions, it also leads to privacy issues. In Articl, it is mentioned that cryptocurrency transactions that are made public on the blockchain result in information that is no longer anonymous [11]. Transparency of transaction information can lead to the exposure of important financial information. Transparency in the blockchain not only leads to the potential exposure of transaction information, but also allows malicious attackers to find weaknesses in the transaction system through transparent information [11]. For example, the code of smart contracts is publicly available on the blockchain. This allows an attacker to find vulnerabilities in the code to attack the transaction program running the smart contract. The irreversible nature of transactions in the blockchain leads to liability issues. As mentioned in Article, irreversible cryptocurrency transaction errors leave the user alone to bear the consequences [11]. Transaction errors include entering the wrong transaction address or being scammed. The public image of cryptocurrencies is associated with illegal activities, including but not limited to money laundering and the financing of illegal acts. These images are largely negative. These ethical and legal issues may cause the public image of cryptocurrencies to suffer. They may also be subject to stricter regulation [11].

Cryptocurrencies are in an unregulated environment due to their decentralized nature. The lack of proper regulation can lead to severe volatility in the cryptocurrency market. Severe volatility in the trading market can lead to loss of revenue for investors and the development of the cryptocurrency financial system [11]. Cryptocurrencies are viewed and regulated differently in different countries and regions. Different regulations may limit the participation of cryptocurrency investors. In some countries and regions, strict laws and restrictions are imposed on cryptocurrencies. This has resulted in the development of cryptocurrencies being hindered in areas where strict laws are in place [13]. Some investors use third-party intermediaries to manage their cryptocurrencies. These intermediaries may have security vulnerabilities. Security breaches can lead to risk and fraud. They may also be insolvent in the event of financial problems, which could result in significant financial losses for investors [14]. Cryptocurrencies lack a harmonized regulatory framework due to the different laws governing cryptocurrencies in different jurisdictions. Multiple regulations and regulatory frameworks lead to regulatory uncertainty. Uncertainty complicates the operations of different individuals and businesses using cryptocurrencies around the world [11]. The lack of cryptocurrency regulation has also led to the emergence of many cryptocurrencies in the market. Most cryptocurrencies are not exposed to regulation. This has resulted in investors being unable to recognize the legitimacy of cryptocurrencies in the market. This leads to an increased risk of scams and financial losses for consumers [11].

To address the security of cryptocurrencies, there are significant costs to traders. The costs to consumers include, but are not limited to, increased complexity, increased financial costs, decreased performance, increased energy costs, decreased user experience, increased education costs, and increased legal fees. The use of self-managed wallets, such as hardware wallets, increases the security of the keys, but the use of such wallets requires skill on the part of the user. There is also the possibility of losing cryptocurrency after using such wallets, such as losing private keys and mishandling backups [14]. This means that even if users have more relevant skills, they may still be at risk of losing cryptocurrencies due to complex operations. The use of self-managed wallets, as mentioned above, not only requires users to be technologically savvy, but also represents an increase in the amount of money that users need to invest in self-managed wallets. This investment is not only in the purchase of a self-managed wallet, but also includes, but is not limited to, secure storage solutions and advanced exchange services. Higher standards of storage and exchange services require more money [13]. This means that cryptocurrency security issues can significantly increase the cost of managing cryptocurrency assets for users. To increase the security of cryptocurrency transactions, users will use more advanced security protocols to secure their transactions. While more advanced security protocols will provide better security, more advanced security protocols also have their drawbacks. However, more advanced security protocols also have the potential to increase the computational overhead [11]. This means that more advanced security protocols will result in slower transactions for the same amount of computing hardware. In proof-of-work-based cryptocurrencies, a large amount of energy is used to secure the cryptocurrency. This means that there is a relationship between the security of a cryptocurrency and the amount of energy consumed. Producing large amounts of energy by consuming large amounts of energy has an impact on the environment. At the same time, the economic value of this energy-intensive approach is a concern [11]. For the security of cryptocurrencies, security and convenience cannot exist at the same time. Cryptocurrency security procedures include, but are not limited to, multiple authentication and key management mechanisms.

These complex applications can be difficult for users to understand in a short period of time. This leads users to choose less secure but easier to use security programs [15]. Attacks on cryptocurrencies can be approached not only from a computer technology perspective, but also from a human perspective. Social engineering attacks can be used from a human perspective. This attack uses the behavior of the user as a starting point. Attacks include, but are not limited to, phishing and fraud. To mitigate social engineering attacks, additional resources and time are required for user education [15]. Faced with different regulations for cryptocurrencies in different regions, companies developing cryptocurrencies need to pay an additional fee for legal advice. As mentioned in Article, meeting different regional regulations can lead to significant cost increases and the need to adjust operational strategies [13]. This means that not only will there be more costs associated with meeting regional regulations, but there will also be more costs associated with adjusting operational strategies. Adjusting operational strategies can also lead to changes in revenue. Cryptocurrencies face multiple risks in terms of technology, market, adoption, and regulation. At the same time, mitigating these risks can be costly and time-consuming. These risks need to be balanced against security, convenience, and performance.

## 5. Limitations and Prospects

Cryptocurrency as an emerging technology has attracted a lot of attention in the past few years. However, there are still some limitations in the research on the security of cryptocurrencies. These security research limitations have restricted the development of cryptocurrencies. First, one of the security limitations is the lack of in-depth academic research on the security factors of cryptocurrency use. Existing research has not explored the key factors of trust, security, and risk in cryptocurrency security [5]. These cryptocurrency security factors are important for users to use cryptocurrencies. The second point is that the existing research on cryptocurrencies uses a single model. Most of the research on cryptocurrency security uses models that focus on technology acceptance models, but these models fail to address financial risk and transaction security factors [5]. Third, the sample sizes used in cryptocurrency research are too small. Some studies have small sample sizes and lack research on a wider range of people [5]. The narrow scope of the study's results in findings that do not properly represent the current state of cryptocurrency security. Fourth, the network of collaboration between different researchers is sparse. Collaboration in cryptocurrency security research has not been fully exploited and this lack of collaboration has been manifested at both the individual and organizational levels [16]. This means that there are fewer citations and collaborations between different disciplines. Finally, cryptocurrencies currently suffer from a lack of regulation and legislation. Due to the rapid development of cryptocurrencies, the regulation of cryptocurrencies often lags the current stage of technology [6]. This represents an increased risk of criminal activity or fraudulent behavior towards cryptocurrencies.

To address the limitations of cryptocurrency security-related research mentioned above, the first step should be to use more options in research modeling. For example, a comprehensive technology adoption model should be used. This is because a comprehensive technology adoption model includes both risk and security factors. For example, the security of cryptocurrencies can be analyzed more comprehensively by the diffusion of innovations theory and the theory of planned behavior [5]. Second, interdisciplinary and transnational cooperation should be strengthened. Collaboration between different countries and disciplines can contribute to the deeper development of cryptocurrency security. Adding additional disciplines between finance, law, and technology could increase the research angle and advance comprehensive research [16]. Third, a comprehensive legal and regulatory system should be established. The government should enforce cryptocurrency-specific regulations to protect cryptocurrency traders and the trading market [6]. Establishing a reasonable regulatory framework can better promote the development of cryptocurrencies. Similarly, improving the technological capabilities of government regulators can enhance their ability to stop criminal activities related to cryptocurrencies [6].

## 6. Conclusion

To sum up, this study looks at and talks about how cryptocurrency transaction security has grown and where it is right now. The main idea of cryptocurrency started in the late 1980s. After that, cryptocurrency technology went through development and changes. Bitcoin came out in 2008, which was a big moment for cryptocurrency technology. Cryptocurrencies like Bitcoin use a proof-of-work system to make transactions happen. Later, people started using cryptocurrencies in different kinds of things. But as cryptocurrencies became more successful, people found problems with security. Security problems in cryptocurrency made researchers study algorithms, consensus systems, transaction risks, and regulations for cryptocurrency security. While progress has been made in researching cryptocurrency security, there are still many risks that cryptocurrencies face in terms of technology, markets, how they are used, and rules around them. Looking at the future of cryptocurrency security, it's important to make research models bigger, get more cooperation across fields and borders, and build a full legal system with rules. Researching cryptocurrency security from different angles can help cryptocurrencies grow. The importance of this paper is to show research about cryptocurrency security and the risks involved. This is meant to help guide research in the future about cryptocurrency security and support blockchain development continuing forward.

## References

*[1] Paulavičius, R., Grigaitis, S., Igumenov, A. and Filatovas, E. (2019) A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions. Informatica, 30(4), 729-748.*

*[2] Nakamoto, S. (2019) Bitcoin: A Peer-to-Peer Electronic Cash System (Unabridged.). BN Publishing.*

*[3] Zou, Y., Meng, T., Zhang, P., Zhang, W. and Li, H. (2020) Focus on Blockchain: A Comprehensive Survey on Academic and Application. IEEE Access, 8, 187182–187201*

*[4] Wang, G., Zhang, S., Yu, T. and Ning, Y. (2021) A Systematic Overview of Blockchain Research. Journal of Systems Science and Information, 9(3), 205-238.*

*[5] Al-Amri, R., Zakaria, N.H., Habbal, A. and Hassan, S. (2019) Cryptocurrency adoption: current stage, opportunities, and open challenges. International Journal of Advanced Computer Research, 9(44), 293–307.*

*[6] Gunarso, G. and Stephanie. (2022) Cryptocurrency and Its State of Research. International Dialogues on Education, 9(1), 151–175*

*[7] Hossain, M.S. (2021. What do we know about cryptocurrency? Past, present, future. China Finance Review International, 11(4), 552–572.*

*[8] Kuo, T.T., Kim, H.E. and Ohno-Machado, L. (2017) Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220.*

*[9] Dong, S., Abbas, K., Li, M. and Kamruzzaman, J. (2023) Blockchain technology and application: an overview. PeerJ. Computer Science, 9, e1705–e1705.*

*[10] Yu, C., Yang, W., Xie, F. and He, J. (2022) Technology and Security Analysis of Cryptocurrency Based on Blockchain. Complexity, 2022(1).*

*[11] Quamara, S. and Singh, A.K. (2022) A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives. Computers & Security, 113, 102548.*

*[12] Yousuf, R., Jeelani, Z., Khan, D.A., Bhat, O. and Teli, T.A. (2021) Consensus Algorithms in Blockchain-Based Cryptocurrencies. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 1–6.*

*[13] Mikhaylov, A. (2023) Understanding the risks associated with wallets, depository services, trading, lending, and borrowing in the crypto space. Journal of Infrastructure, Policy and Development, 7(3).*

*[14] Fröhlich, M., Gutjahr, F. and Alt, F. (2020) Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. Proceedings of the 2020 ACM Designing Interactive Systems Conference, 1751–1763.*

*[15] Weichbroth, P., Wereszko, K., Anacka, H. and Kowal, J. (2023) Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. Sensors, 23(6), 3155.*

*[16] Corbet, S. and Lucey, B. (2020) An analysis of the development of cryptocurrency research. In Cryptocurrency and Blockchain Technology (Vol. 1, pp. 23–54). Walter de Gruyter GmbH.*