Hindawi
Complexity
Volume 2022, Article ID 5835457, 15 pages
https://doi.org/10.1155/2022/5835457

Research Article

Technology and Security Analysis of Cryptocurrency Based on Blockchain

Chao Yu,[1] Wenke Yang ,[2,3] Feiyu Xie,[1] and Jianmin He[2]

[1]School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China
[2]School of Economics and Management, Southeast University, Nanjing 211189, China
[3]Department of Management, Strategy and Innovation, Faculty of Economics and Business, KU Leuven, Warmoesberg 26, Brussels 1000, Belgium

Correspondence should be addressed to Wenke Yang; wenkedyang@gmail.com

Received 26 April 2022; Accepted 4 July 2022; Published 21 July 2022

Academic Editor: Yi Su

Blockchain technology applied to cryptocurrencies is the dominant factor in maintaining the security of cryptocurrencies. This article reviews the technological implementation of cryptocurrency and the security and stability of cryptocurrency and analyzes the security support from blockchain technology and its platforms based on empirical case studies. Our results show that the security support from blockchain technology platforms is significantly insufficient and immature. In addition, we further Zyskind and Nathan (2015) and Choi (2019) and find that the top ten platforms play critical roles in security support and have significant advantages in terms of funds, duration, and human resources. Moreover, these platforms provide computational resources and benefits to the consensus algorithm selection for blockchain practitioners. Second, encryption ensures the security of cryptocurrencies. On the one hand, the digital signatures identify the identity of the signatory and the transaction. However, the principle of the hash algorithm (SHA256) confirms ownership. Meanwhile, SHA256 is infeasible to compute in the reverse direction and is difficult to attack. Furthermore, the records in the blockchain can be queried by every participant, making the system information transparent and open reliable. Third, compared to the study of Fu and Fang 2016, we find that the blockchain structure is composed of security components and basic components of six layers that are independent and cannot be extended completely and have a certain coupling among them. Fourth, the underlying ledger structures of Bitcoin and DAG are highly correlated to their security. Specifically, we follow Sompolinsky et al. (2016) and detect that the structure of SPECTRE ensures network security and robustness from its block production, conflict resolution, and generated trusted transaction sets. Meanwhile, the voting algorithm of SPECTRE makes resolving conflicting transactions by calculating votes and ensuring the transaction information that is virtually unable to be tampered with possible. In particular, the security calculation power of SPECTRE can reach 51% and resist “double-spend attacks” and “censorship attacks” effectively. In addition, the RDL framework of SPECTRE achieves security confirmation of transferring funds. Moreover, PHANTOM identifies evil blocks by employing block connectivity analysis and ensures its security. Eventually, we also expand the studies of (Sompolinsky et al., 2016 and Sompolinsky et al., 2017) and compare the basic characteristics of the protocols of Bitcoin, SPECTRE, and PHANTOM and find that protocols play imperative roles throughout the implementation process of cryptocurrency. In addition, the underlying ledger structure and consensus mechanism make up a blockchain while the confirmation time, throughput limit, and ordering are prerequisites for smart contracts.

1. Introduction

Cryptocurrency, owing to its rarity and ability to prevent overabundance and inflation, has drawn a large number of speculators, including those with trading experience and novices in trading operations, and has gradually been applied in the financial sector [1–3]. Cryptocurrencies are diverse owing to various distinct cryptocurrency protocols [4]. In 2021, the market contains over five thousand tokens of different cryptocurrencies, even though most of them are not in demand because of their poor capitalization and the same technic as their predecessors. Specifically, consider that the first five cryptocurrencies, Bitcoin (BTC), Ethereum (ETH), Tether (USDT), Cardano (ADA), and Binance Coin (BNB), hold 45.81%, 17.11%, 4.16%, 3%, and 2.9% of the global cryptocurrency market capitalization, respectively, adding up to approximately 81.5%, which can be used as proxies for cryptocurrencies. It is noteworthy that Tether (USDT) and Cardano (ADA) have replaced the status of Ripple (XRP) and Litecoin (LTC). In addition, the application fields of cryptocurrencies generate differences [4, 5]. However, their application fields are mainly determined by protocols for cryptocurrency. Additionally, the majority of these cryptocurrencies exploit protocols, even though there are other database structures.

The underlying technology behind cryptocurrencies is blockchain, which is treated as an immutable distributed ledger. Blockchain technology has been portrayed as the "next-generation Internet" and "new foundational technology" [6]. In addition, compared to traditional state-sponsored currencies, cryptocurrency may have the ability to perform microtransactions and then solve the economic gap. However, the application of blockchain technology, such as many cryptocurrencies that are distributed autonomous organizations (DAOs) and based on the top of blockchain infrastructures, is characterized as "Ponzi schemes." Blockchain technology is the single most disruptive to financial and economic systems [1]. Therefore, future blockchain applications and technology adoption will be wildly jeopardized [7].

Additionally, current blockchain technology platforms are chaotic and have difficulties in achieving consensus, coordinating actions, and resolving differences [8]. As shown in Figure 1, although the overall growth trend of blockchain technology platforms is exponential and grows rapidly from 2012 to 2019 with an average growth rate of 55.08%, the growth rate has dropped significantly from 2019 to 2021. Blockchain infrastructures have not been operated by an official organization or a physical and legal entity [9].

Blockchain is generally regarded as a distributed database system and managed by a peer-to-peer network of computing devices, which helps provide a shared, yet accurate record [10]. For instance, blockchain-inspired technology was recently adopted to describe distributed ledger technology, such as Corda, which was developed by R3. According to Nakamoto [11], blockchain can be defined as a peer-to-peer electronic cash system. In particular, traditional organizational functions are replaced by encoded and executed on the blockchain through distributed autonomous organizations (DAOs). Blockchains contain different governing principles and parameters, and they have similar data structures and distributed architectures. Blockchains secure the database and protect it from external attacks or malicious behaviors by cryptography, such as public or private key infrastructure and hash functions [7]. On the one hand, the public key plays the role of receiving the address of cryptocurrency to participate in address exchange. Meanwhile, the public key can be used to verify transaction information and prevent transaction messages from being maliciously forged. On the other hand, the private key can generate a signature of messages that cannot be denied by the signer. In addition, the private key is devoted to managing and protecting cryptocurrencies. Nevertheless, most cryptocurrency users are unable to execute with technical enterprises on complex plans, which makes them over-extended and underachieved on technical execution, and even have a higher probability of losing their private keys than external adversaries. Furthermore, the role of the hash function was limited.

Hence, we may conclude that cryptocurrencies and blockchain technology have developed rapidly in the past 13 years. However, their development has also generated various kinds of security issues, such as the trust, risk, and efficiency of cryptocurrency, which has not been fully considered to maintain robust functioning financial systems. Therefore, making a detailed analysis of the technology and security of cryptocurrency is increasingly indispensable for the development of financial systems. The main reasons are indicated as follows: first, trust cannot solely rely on the code base for the loophole in the code, which can turn it to be a legitimate action and allowable within the code [7]. Meanwhile, the trust and acceptance of users are generated by the value of cryptocurrencies such as Bitcoin continue to exist, which indicates that trust and acceptance may diminish when their values are gone [1]. Second, significant risks can be generated by all encoded contractual agreements and organizational relationships on the blockchain. Therefore, trust issues in transactions generate risks. Third, cryptocurrency improves financial efficiency and makes digital transactions widespread [6, 7]. For international transactions, cryptocurrencies can quickly respond to emergency transaction needs through peer-to-peer systems. Then, the efficiency of cryptocurrency would be greatly enhanced once trust issues are resolved. For example, cryptocurrency markets have high liquidity and are evolving [12]. Thus, three research questions are addressed in this study:

(a) What is the status quo of the security and stability of cryptocurrencies in terms of support from blockchain technology platforms and blockchain technology?

(b) What is the relationship between blockchain technology and the security of cryptocurrency?

(c) How do maintain and what are the differences between the security and stability of cryptocurrencies?

In this article, we present a detailed analysis of the security and stability of cryptocurrencies in terms of support from blockchain technology platforms and blockchain technology. As many of the presented issues are related to the financial market, this work falls in the more general security area in data authenticity and recording, and the structure and protocols of blockchain technology. The contributions of this article are as follows: we outline the security of cryptocurrencies based on blockchain technology from multiple perspectives according to our proposed framework. First, we expand the study of Choi [13] and

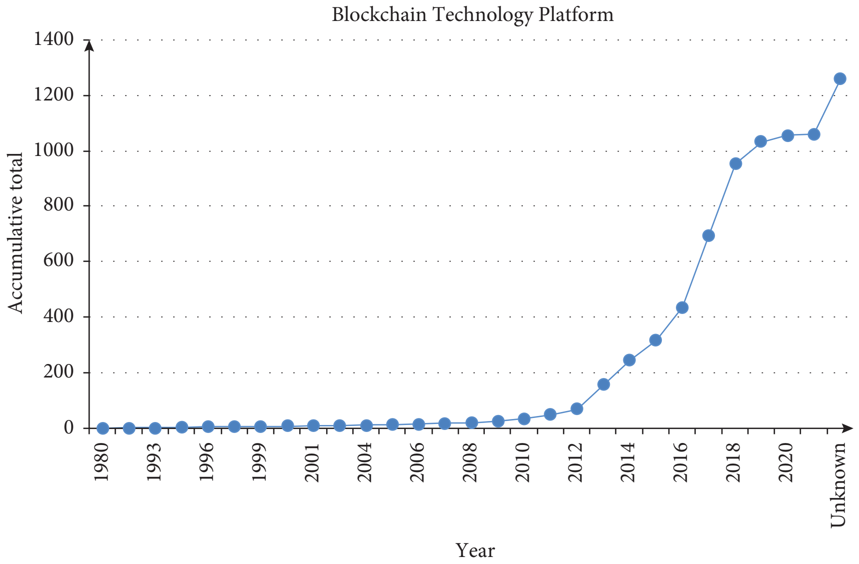

Figure 1: Accumulative total of blockchain technology platform (note that the unknown means that the founded year of block chain technology platforms is not clear).

consider the technical support from blockchain technology platforms by adopting empirical evidence to analyze their shortcomings. Second, it is noteworthy that prior studies, from the perspective of users, focus on the basic security requirements for cryptocurrencies, but these studies fail to formally take the basic principle of the secure hash algorithm (SHA256) as an example of blockchain technology to describe the security of data authenticity and the recording of cryptocurrency in an intuitive manner. Third, we further study Fu and Fang [14] to discuss the structure of blockchain and define the security components of different layers. Moreover, our results show that these security components have certain connections or joint effects in the blockchain. Fourth, we emphasize the importance of protocols and their frameworks to maintain the security of cryptocurrencies by comparing the underlying ledger structure of Bitcoin and DAG. Additionally, we further compare 2 classic protocols of the DAG blockchain including the difference between SPECTRE and PHANTOM.

The remainder of this article is organized as follows. Section 2 presents a literature review. Section 3 introduces the research methodology. Section 4 presents an analysis of the technology and security of cryptocurrencies. Section 5 concludes.

2. Literature Review

This section presents an overview of the current studies on the technological implementation of cryptocurrency and the security and stability of cryptocurrency, a discussion of the relationship between blockchain technology and the security of cryptocurrency, and the factors that facilitate risk and build trust.

2.1. The Technological Implementation of Cryptocurrency. As technology innovation is increasingly indispensable in financial sectors, technologies based on blockchain in cryptocurrency have fundamentally changed the notion and mode of perceiving virtual currencies of users, enterprises, financial intermediaries, and governments [15–17]. First, a finite number of cryptocurrencies will ever be generated, preventing overabundance and ensuring its rarity. Specifically, mining pools may constrain the sustainability of a cryptocurrency ecosystem. Because of this, cryptocurrency has become a transformative technology and has attracted a growing and supportive community of developers and users [1]. Second, it is programmers and math instead of the government that undertakes the technical control of cryptocurrency [18]. Specifically, the operating principle of cryptocurrency is to solve encryption algorithms that aim at creating unique hashes. Third, blockchain technology adopted in cryptocurrency can recognize users as owners of their personal data, which decreases the cost of securing and compartmentalizing data [19]. Hence, the adopted technologies enable cryptocurrencies to perform the same monetary functions as traditional currencies, as well as significantly higher security and lower cost, and to play a decentralized role.

Blockchain is composed of individual blocks. Each block contains collections of transactions that are included in the ledger. All transactions were recorded and stored in each block [20]. In addition, cryptocurrency is referred to as an open and distributed ledger technology (DLT) that can verify records and process requests in parallel but cannot modify them [21, 22]. Nevertheless, the storage devices of DLTs are connected from one to another and form a mesh [22]. These storage devices can then be expressed as nodes. Physically, different nodes were separated. However, the CRUD operations return the same results even though the nodes that operate are different. Additionally, every node in a platform or network can access authorized information for the same permissions and obligations [21]. Moreover, nodes in the network transfer data do not require mutual trust. To conclude, the DLT is architecturally distributed but logically centralized [23]. Generally speaking, there is no significant distinction between blockchain, Bitcoin, cryptocurrency protocol, and distributed database structure [11, 24]. Nevertheless, blockchain, back to the narrow sense of its definition, is regarded as a chained data structure that combines information and data blocks in chronological order, and then encrypts records as a distributed ledger that cannot be forged or tampered with [21].

In addition, most cryptocurrency protocols widely adopt blockchain technology. These protocols involve cryptocurrency incentives, cryptography, and consensus mechanisms. In particular, cryptocurrency protocols are regarded as rules that regulate applications that can be performed within a set environment [4]. For instance, the Nakamoto protocol in Bitcoin decides the full order of blocks and then confirms the full order of transactions [25]. Leading companies can implement their proprietary authentication software using the OAuth protocol, which enables them to serve as centralized trusted authorities [26, 27]. To guarantee the targets of final security, a modular analysis benefits the exploration of the security properties of subprotocols [26]. For instance, the proof of solvency can be proved by a secure cryptographic coprocessor, such as a trusted platform module (TPM). Cryptocurrency also employs asymmetric encryption technology to safeguard the blockchain. In particular, the public and private keys constitute asymmetric encryption. First, public key cryptography makes no other user transfer other account values possible through digital signatures. In addition, the private key is regarded as the sole basis for legally controlling cryptocurrency accounts for users, ensuring the security of account assets [21]. Specifically, the private key can be encrypted and stored in its wallet unless the user exports it manually and then decrypted to sign the transaction record upon request. For instance, armory is used to manage private keys (see Figure 2). Nevertheless, cryptocurrency technology is unable to solve the account key theft and trading parameter tampering caused by a lack of security awareness [28]. In addition, privacy information is always stolen by attackers despite permissions through the desktop cryptocurrency wallet remote procedure call (RPC) interface, even though the asymmetric encryption techniques safeguard the privacy and security of the participants [20, 29]. Furthermore, a shared consensus mechanism benefits the benign nodes to achieve agreement on an almost immutable record of transactions by DLT. Above all, similar to bank transfers, transactions committed to the ledger make digital assets transfer from the asset owner to another available user.

2.2. *The Security and Stability of the Cryptocurrency.*

The binding between the state and international security is changing due to the emergence of the Fourth Industrial Revolution because of the progress of information technologies [30]. It is noteworthy that the information technology of blockchain, which is adopted in Bitcoin and other cryptocurrencies and has security features, has drawn our attention. According to Febrero and Pereira [4], security mainly includes the aspects of fault tolerance, network resilience, scalability, and immutability when facing attacks. For example, security is achieved by a technology intersection that generates different cryptocurrency protocols [4]. Cryptocurrency protocols can simultaneously display technological components, including cryptography, DLT, consensus mechanisms, and cryptocurrency incentives. Nevertheless, stability is expected to be drawn attention to financial systems [31]. Particularly, stability is highly correlated to public blockchain mining owing to the existence of a motivation that destroys cryptocurrency.

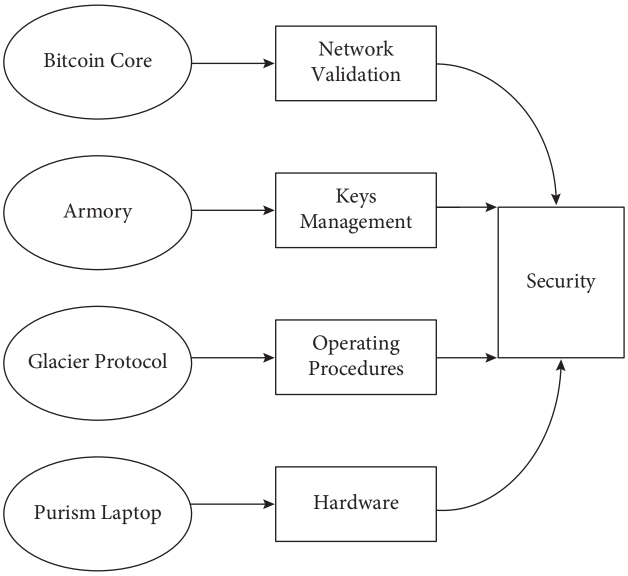

Figure 2: The security of Bitcoin is based on blockchain technology.

First, cryptography realizes transaction encryption and privacy protection and allows secure message exchanges from participant to participant (P2P). Generally, the original message of the sender is encrypted for security reasons, which requires the receiver to decrypt. Meanwhile, private-public addresses are created by protocols. Second, DLT has a high risk, which influences the security of cryptocurrencies. According to Hileman and Rauchs [32], DLT varies according to data access restrictions and limits on which parties can validate transactions. The most typical ledger is the public ledger, which is a semi-anonymity that ensures that each user sees each transaction. Hence, they have a higher risk and are susceptible to attacks [33]. However, the decentralized consensus of blockchain transaction orders guarantees security that does not need trust among members. In particular, the blockchain protocol can act as an automated access control manager that does not require third-party trust [19]. Moreover, cryptocurrency incentives have significant effects on short-term operational decisions involving security in selecting exchanges, especially the cost of investing in security. Meanwhile, incentives at the protocol level of cryptocurrency are explicitly considered [34]. Thus, incentive misalignments in the cryptocurrency exchange market are critical for the security and viability of public blockchain ecosystems.

However, the multitude of criminals such as cybercrime in cryptocurrencies through DarkNet markets has been sharply rising in recent years [35]. First, user information has been collected and analyzed for a long time and is regarded as a valuable asset in the big data era. In addition, the decentralized nature of cryptocurrency has greatly decreased the possibility of securing each server that runs the code. In addition, fraud and theft in cryptocurrency are increasingly popular because of faulty system setups by exchange companies [1]. Furthermore, insider fraud and external security compromise are the main sources of exchange. Nevertheless, the European Court of Justice considered that Bitcoin transactions were exempt from value-added tax in 2015, which maintains the stability of cryptocurrencies [36].

Hence, trust in employing blockchain technology has become a crucial problem faced by cryptocurrencies to maintain their security and stability. First, the definition of trust in adopting blockchain technology includes security, comfort, and confidence [37, 38]. On the one hand, trust helps build a strong bridge for consumers to overcome perceptions of risk and insecurity [39]. In particular, numerous general user bases hold the view that cryptocurrencies are solely employed by criminals and are questionable in law. That is, the value fluctuation and the legality of cryptocurrency may limit investor trust. One of the most typical examples is the affair of the bankruptcy of Mt. Gox, mainly caused by the new code without version control, which has scared many users and damaged the image of cryptocurrency [40]. This also proves that risk can be generated by price volatility, discouraging consumers and merchants from holding cryptocurrency, which is also consistent with the view of PwC [41]. On the other hand, consumers' trust can build confidence. To achieve this purpose, permissioned ledgers, such as DLT that restrict network participation, can ensure that the parties who have no sufficient trust form and maintain a consensus of a set of shared facts [42, 43]. In addition, exchanges tend to make public display security investments and reassure customers to trust. Meanwhile, they compensate users for their own security breaches to construct trust. Above all, the proof of solvency reinforces consumers' trust in the exchange.

Next, trust plays an indispensable role in creating a security environment, which convinces users to accept blockchain technology. In general, blockchain technology is complicated for users to accept [37]. Consequently, directly or indirectly factors such as trust, security, and privacy can also encourage people to accept blockchain technology [44]. For instance, blockchain transaction systems are more likely to be accepted under the condition that usage risk is sharply reduced [45]. In addition, the lower cost and shorter time with privacy or control may attract consumers to use cryptocurrency [46]. To sum up, factors that directly or indirectly would encourage people to embrace technology mainly are trust, security, and privacy. In addition, trust is highly correlated with regulatory support and experience [37]. Therefore, the security and user acceptance of cryptocurrency can be enhanced by the development of better software.

To summarize, cryptocurrencies that adopt blockchain technology have shown great application advantages in finance and the Internet and have displayed a trend of rapid development in multiple fields. However, cryptocurrency, as an emerging digital virtual currency, is not stable and mature enough in terms of business management and technical implementation, and some security and privacy issues that are gradually exposed, and security incidents against the application of blockchain cryptocurrency also occur frequently.

3. Research Methodology

As shown in Figure 3, the framework of our technology and security analysis of cryptocurrency based on blockchain mainly includes security support from the blockchain technology platform and blockchain technology. The details are presented as follows: on the one hand, the majority of blockchain technology platforms, to enable the development of next-generation multiparty applications, utilize distributed ledger and confidential computing technologies, which foster and deliver digital trust between parties. Hence, we discuss security support from blockchain technology platforms involving the aspects of raised funds, duration, employees, and especially the consensus algorithm. On the other hand, blockchain technology shifts most users' trust from human beings to machines by decentralizing control over the currency. Hence, we also analyze the security support from blockchain technology.

In simple terms, our study focuses on the security of data authenticity and recording, blockchain structure, and protocols. To better explain the security of data authenticity and recording, we use the hash function (SHA256) as an example to describe its principle. In addition, we divide the blockchain structure into six layers and conclude that these layers are composed of security and basic components. Finally, we illustrate the security of the protocols in the case of Bitcoin and DAG. In particular, we compare the protocol security of SPECTRE and PHANTOM. Meanwhile, we also employ these examples to discuss the balance between security, efficiency, and functionality of cryptocurrency protocols.

4. Research on the Technology and Security of Cryptocurrency Based on Blockchain

Cryptocurrency employs blockchain technology to maintain security and transaction processes. Specifically, the security of cryptocurrency is supported by the blockchain technology platform and blockchain technology itself. Blockchain technologies such as hash encryption, electronic signatures, asymmetric encryption, distributed ledgers, smart contracts, and P2P networks are used to verify data and ensure safe storage.

4.1. The Security Support for Cryptocurrency from the Blockchain Technology Platform. Security support from blockchain technology platforms is insufficient. As shown in Figure 4, we present a radar chart of the total funds raised,

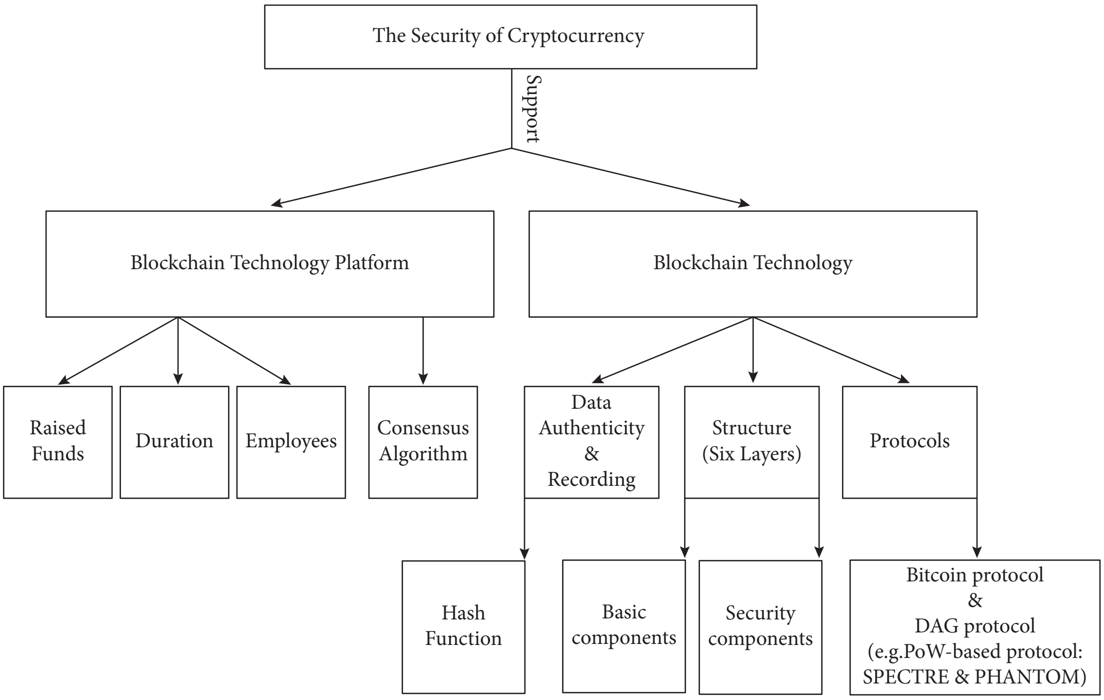
The Security of Cryptocurrency
Support
Blockchain Technology Platform
Blockchain Technology
Raised Funds
Duration
Employees
Consensus Algorithm
Data Authenticity & Recording
Structure (Six Layers)
Protocols
Hash Function
Basic components
Security components
Bitcoin protocol & DAG protocol (e.g.PoW-based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

Figure 3: Framework.

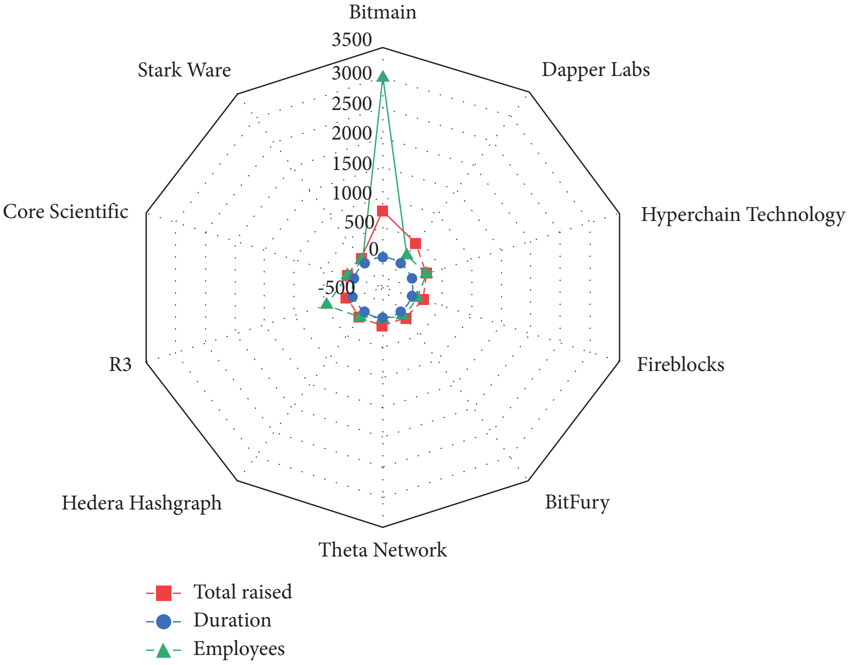

Figure 4: Radar chart of total raised funds, duration, and employees of blockchain technology platform.

duration, and employees of blockchain technology platforms. In Figure 4, the total raised funds of Bitmain ranks top of blockchain technology platforms, Dapper Labs, and Hyperchain Technology, ranking the top two and three. However, the funds raised by blockchain technology platforms are much less than those of traditional Internet financial platforms, such as Lufax. In addition, the duration of these blockchain technology platforms is between 3 and 10, and at an average of 5.8, which indicates that the global support and infrastructure for cryptocurrency are growing rapidly in the last decade, but most of these companies are young start-ups. Blockchain, which is treated as an immutable DLT, is the underlying technology behind cryptocurrencies [47]. Hence, the ability of blockchain technology platforms to sustain the security and stability of cryptocurrencies may be significantly deficient. Moreover, Bitmain employees rank first among blockchain technology platforms. In particular, Bitmain has 3000 staff, whereas StarkWare has only 37. Additionally, the employees of the blockchain technology platform are ranked as follows: Bitmain > $R3$ > Hyperchain Technology > Dapper Labs > Hedera Hashgraph > Core Scientific > BitFury > Fireblock > StarkWare > Theta Network. In other words, the human resource gap among blockchain technology platforms is prominent. In addition, there is a marked difference in the speed of the crisis response of blockchain technology platforms. Thus, our results are consistent with the market share of Bitmain and prove that Bitcoin has been the largest manufacturer of new Bitcoin mining machines and hardware.

Blockchain technology platforms also play a crucial role in the selection of consensus algorithms for blockchain practitioners. First, a consensus mechanism with high security requires computational resources. These platforms employ computationally intensive asymmetric key technology to help users identify and verify transactions. Second, available blockchain technology platforms lack uniformity in accessing built-in APIs. A typical example is that Bitmain leverages the inflexibility of Bitcoin's PoW and makes full use of its computation capability of miners to achieve its success after promoting their Antminer-ASIC chip products.

4.2. The Security Support for Cryptocurrency from Blockchain Technology

4.2.1. Analysis of the Security of Data Authenticity and Recording of Cryptocurrency Based on Blockchain Technology. The security of data authenticity and the recording of cryptocurrency mainly depend on encryption. Specifically, digital signatures and cryptographic hash functions significantly influence the security of cryptocurrencies.

Digital signatures and their hashing algorithm can confirm whether the identity of the signatory and the transaction have been identified. Meanwhile, they confirmed ownership. Technically, attackers, owing to the cryptographic hash function such as the SHA256 algorithm, have to guess 256-bit strings correctly to breach the security systems of cryptocurrencies. The cryptographic hash function is infeasible to be inverse under the current computing power. In other words, there is no better method than guess and random check for attackers to find a message of arbitrary length that has a specific string of 256 bits (note that acquiring the message requires, on average, 2^{256} guesses) in general, which benefits the given piece of security of cryptocurrency. Additionally, the records in the blockchain can be queried by every participant, which indicates that the information in the system is transparent and open, and reliable.

4.2.2. Analysis of the Cryptocurrency Security Based on the Structure of Blockchain Technology. The structure of blockchain technology, as it is shown in Figure 5, is considered a hierarchical system and mainly includes the applicaryer, contract layer, incentive layer, consensus layer, network layer, and data layer. Each layer contained basic and security components. On the one hand, basic components are used to realize the main business logic functions of the layer. On the other hand, security components are used to deal with frequent security threats and provide threat response solutions and technical security support for the layer and upper layer. In addition, these security components may have certain connections or joint effects in the blockchain.

The application layer involves all services and features implemented in the form of smart contracts and is based on a remote cloud. Hence, users in a blockchain system can also employ application-layer services. Meanwhile, the application layer can provide an interface for the underlying message transmission and application. The application layer mainly includes the basic components—APIs and cross-chain heterogeneity, and the security components—regulatory mechanism and cloud service. The application programming interface (API) is not provided to interact with service interfaces in the blockchain. In addition, heterogeneous blockchains migrate data from one blockchain to another. Therefore, to ensure confidentiality and privacy, a cross-chain data migration architecture was generated. In addition, the regulatory mechanism of blockchain has drawn the government's attention and increased regulatory costs. Nevertheless, regulatory mechanisms, such as laws and regulations, secure the democratic accountability of blockchain technology. Furthermore, cloud services can provide identity authentication for IoT devices based on their computing and resource storage abilities.

The contract layer is designed to set rules for blockchain systems to interact with each other. First, advanced smart contracts can achieve programs and commands, operate asset transactions, and manage smart assets in blockchain 2.0, which further expands the application layer. For users, smart contracts are automatic guarantee plans that can ensure the objectiveness of the execution. Specifically, these contracts release or transmit data when they meet certain conditions. Contracts such as Hyperledger can deal with mutual trust issues among participants. Likewise, script coding plays a critical role in maintaining the security of smart contracts. Furthermore, the sandbox environments vary from country to country. Additionally, the sandbox regulation involves the regulatory sandbox, industry sandbox, and umbrella sandbox. More importantly, formal verification of blockchain is chiefly based on mathematics and can check and verify unknown vulnerabilities, such as logical vulnerabilities in contracts. Employing a testing network can guarantee configuration flexibility. For example, a test network was adopted in the Ethereum wallet. Furthermore, program analysis tools were used to optimize and correct the programs. Hence, smart contracts, script coding, sandbox environments, formal verification, testing networks, and program analysis tools can be considered components. Nevertheless, the programming language provides a standard method to write the blueprints and contracts of blockchain.

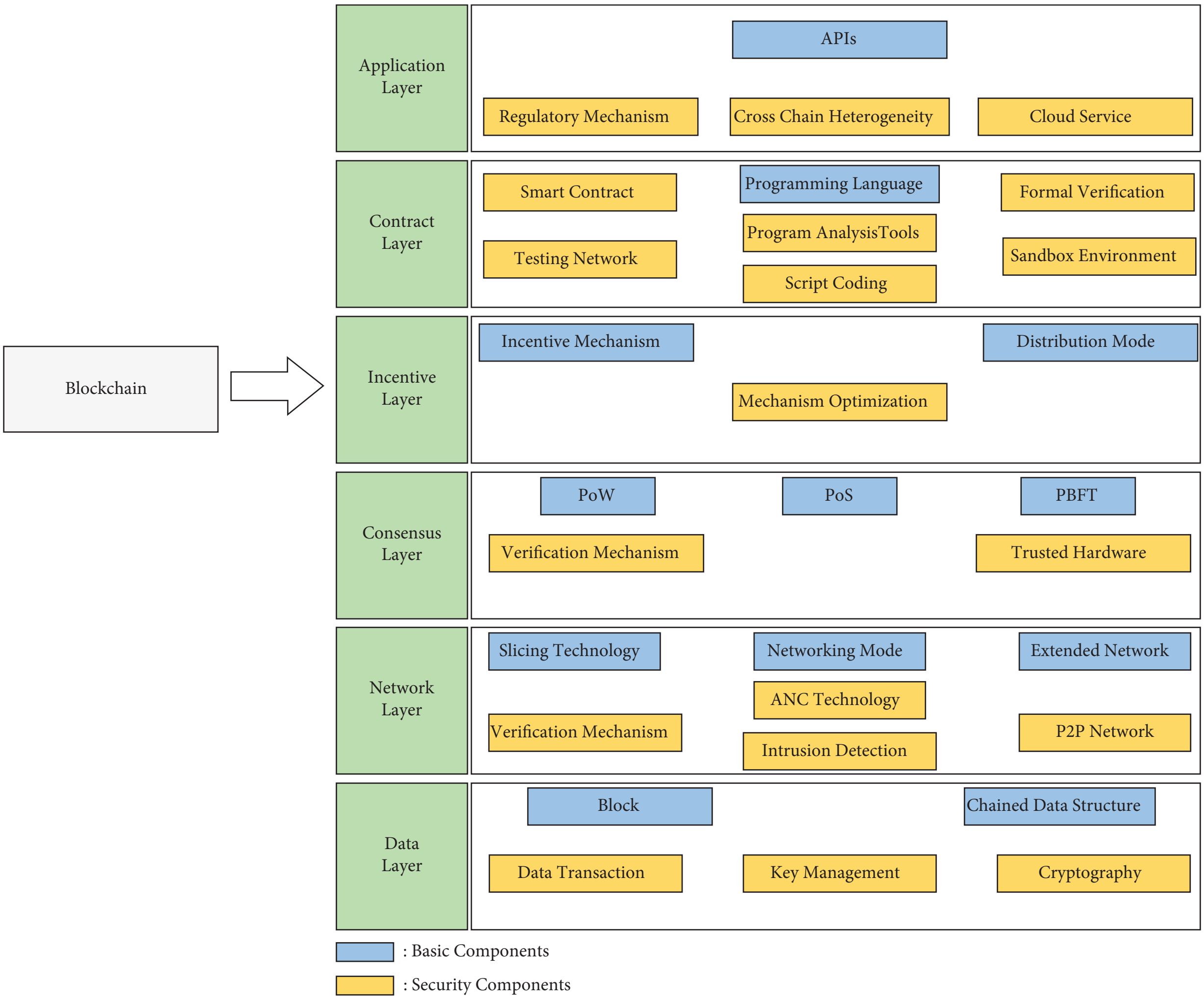

Figure 5: The basic structure of blockchain.

The incentive layer involves incentive mechanisms in cryptocurrencies to accelerate resource sharing, stimulate group intelligence, and promote collaborative communication. In addition, the incentive mechanism is regarded as a monetary incentive that responds to information about events. Meanwhile, monetary incentives share the correct information. Specifically, the initiators provide incentives after verifying the repliers' signatures from its procedure in the blockchain. In addition, incentive schemes can be used to detect malicious miners. Next, the distribution mode in the incentive layer can operate data and store and handle additional images that contribute to parallel large-image processing. Moreover, the incentive layer integrates economic incentives and distribution mechanisms into the blockchain.

The consensus layer mainly contains consensus protocols that are adopted to share information and conduct transactions. Moreover, consensus agreements league multiple organizations to build a consortium system. Moreover, the consistent and efficient problems in distributed scenarios of blockchain can be solved by a consensus mechanism. The prevailing consensus protocols mainly include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). These protocols aim at maintaining a peer-peer consensus state for blockchain systems. More importantly, trusted hardware such as Intel SGX is used to improve the performance of PoW and PBFT. In addition, trusted hardware such as the TrustZone of Intel SGX can also enhance security at a slight cost of performance. More precisely, the security of trusted hardware relies on a trusted computing base (TCB). Additionally, the smaller the TCB, the better the security. In fact, the consensus mechanism can verify and record data into a blockchain, which makes a blockchain ledger that is immutable, irrevocable, and traceable.

The security of the network layer has a decisive effect on the security of the cryptocurrency system. In particular, the bigger the network, the stronger the protection against attacks and data corruption, which makes Bitcoin the most secure blockchain. Meanwhile, the network may require a Bitcoin core (see Figure 2) for users. In general, the network layer receives and transmits data and verification mechanisms. For instance, the P2P network structure has the features of decentralization, load balance, fault tolerance, and privacy protection [20, 48]. Meanwhile, the P2P network can be a small-world model, which implies that the robustness and data integrity of the network can be guaranteed dynamically when nodes are changing. In addition, the security and privacy of P2P data transactions are critical for P2P networks. Thus, we conclude that the P2P network is a security component for the blockchain. More importantly, P2P networks can verify and synchronize data. In general, a network layer specifies a verification mechanism. For instance, the network nodes verify the received data or new blocks based on predefined specifications. Hence, we may conclude that the verification mechanism in the network layer can be regarded as a "software-defined" trust and a security component. Next, the blockchain network layer encapsulates the networking mode. For example, the network layer contains a P2P network-networking mode. Most networking modes are peer-to-peer networks and can quickly detect the link state of the Internet. Furthermore, an extended network of miners can be generated using a hash code. Specifically, two miners simultaneously mine two different blocks, which may result in a fork. The blockchain is then extended to process transactions in the extended network. Similar to the P2P network, anonymity-providing networks also consider adversary security requirements and adversary models, even though their requirements regarding information propagation are different. In addition, the communication anonymity-providing systems safeguard the confidentiality of the exchanged data between the sender and receiver. However, anonymity is attacked by linking network data to the application data. Furthermore, the anonymity of the users can be attacked by gathering data from operating the seed node. For instance, many cryptocurrencies, such as Bitcoin, have issued operator policies to ensure security. Therefore, anonymous network communication (ANC) technology can be considered a security component. Furthermore, intrusion detection in the network layer detects endangered network behavior in computer systems. Generally, intrusion detection can be divided into anomaly-based and feature-based intrusion detection methods. The former is for normal user behavior definition and identification, and the latter is for the characteristics of the received packet behavior extraction and comparison. In intrusion detection, the improved semi-distributed topology can strengthen the stability of the system. In particular, the advantages of distributed networks make the accuracy rate reach the network limit. More importantly, the TCP/IP protocol in the network layer was utilized for information detection. Next, the slicing technology can multiplex a network that is virtualized and independent logical in identical physical network devices and delivers information-centric networking (ICN) services. A typical example is that the Internet of Things (IoT) edge network is built using an ICN slicing framework.

The data layer mainly contains data structures, block contents, and data transactions of the blockchain. The chained data structure refers to the blocks of data and information that are combined in chronological order, and then, these blocks are encrypted and recorded as a distributed ledger that cannot be tampered with or forged. All transactions were coordinated and executed through a public ledger. This layer targets data collection, validation, and manipulation. Data management makes data confidentiality possible, ensures data security, and protects the privacy of users from leaking. In addition, keys grow rapidly owing to the complexity of access relationships. Furthermore, key management achieves hierarchical access control and is stored in the blockchain, and acts as a public ledger. Specifically, the key pool assigns each node a unique key chain, which ensures hierarchical access control. Additionally, key management can simplify the key transfer handshake procedure, decrease the key transfer time, improve efficiency, and guarantee security. However, key management is usually controlled by users instead of a third party for privacy-oriented scenarios. Cryptography technology ensures the ability of the ledger to detect tampering with blockchain data. For instance, the hash (Merkle) tree solves the problem of authenticated nodes that act maliciously in a private blockchain. Moreover, users are expected to back up passphrases to ensure security and disclosure. Hence, we may conclude that data transactions, key management, and cryptography are security components.

4.2.3. Analysis of the Security of Cryptocurrency Based on the Protocols of Blockchain Technology. Cryptocurrency transactions are known to be high throughout and require fast confirmation times. Above all, security in cryptocurrency transactions is critical for users to invest. Therefore, cryptocurrencies have various protocols to solve these problems. However, the underlying technology of these cryptocurrencies is still centered on blockchain technology. Besides, their main ideas were consistent with the protocols proposed by Nakamoto [11]. The protocols of cryptocurrencies involve cryptography, distributed ledgers, decentralization, consensus mechanisms, and incentives to maintain an efficient and stable function and the security of a blockchain system.

Firstly, we compare the underlying ledger structure of Bitcoin with that of a directed acyclic graph (DAG). In general, the underlying ledger structure of Bitcoin is a single chain. Ideally, the next block can be packaged as a candidate block broadcast only after the previous one has been confirmed and added to the chain by the whole network. However, the block output speed is much faster than broadcast, which generates forks. To put it differently, a block is being dug up and broadcast before the whole network can confirm it. More importantly, Bitcoin determines its main chain based on the "longest chain consensus," which enables the exclusion of intentionally evil nodes and eliminates the situation that two nodes produce blocks simultaneity. Additionally, the consensus can discard forked blocks that are not part of the main chain. Nevertheless, forks are unavoidable due to accidental factors such as network latency. Thus, the security issues caused by forks have aroused our concern. The protocol of Bitcoin controls the block creation time of 10 minutes and stipulates that a block can be guaranteed to be on the "longest chain" after the confirmation of six blocks. Although the security risks caused by the fork can be avoided, these settings severely limit the transaction processing performance of Bitcoin, and the TPS (transaction per second) is solely about 7. However, it is noteworthy that DAG is expected to solve the problems above [48].

As it is shown in Figure 6, we make a more intuitive comparison between the two structures. DAG mainly has 5 mathematical properties, which are highly related to security issues. To start with, DAG has a topological structure that allows forking, and the topological order for all nodes can be transformed into a node sequence, where the number of the allowed forks is determined by the fork coefficient k (k is an integer greater than 0) of the system. To put it another way, the block output speed may exceed the broadcast speed. Meantime, the network node can record different information at the same time. More importantly, the system based on the DAG structure usually presents the characteristics of high concurrency, weak synchronization, and high TPS owe to the DAG asynchronous accounting method. Secondly, the connected nodes in the DAG can be sorted. Thirdly, DAG has a unique transitive closure. Fourthly, the shortest path and the longest path can be solved in linear time when given 2 nodes in DAG. Fifthly, DAG has a unique transfer protocol. However, the Bitcoin blockchain can only point to the previous unique block, while the DAG has the capability of pointing to multiple blocks. Specifically, the block header of the Bitcoin blockchain only contains a hash of one block, pointing to a unique parent block, whereas that of a DAG includes hash values for multiple blocks, pointing to different former ones.

To better explain the security of cryptocurrency protocols, we further compare 2 classic protocols of DAG blockchain including the PoW-based protocol "Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections" (SPECTRE) and PHANTOM. At first, we discuss the structure of SPECTRE, which ensures network security and robustness from its block produce, conflict resolution, and generated trusted transaction sets. Firstly, the SPECTRE was proposed by Ref. [49] who abandoned the traditional concept of the main chain in the protocol. In particular, all generated blocks are not discarded and form the structure of the ledger. As a matter of fact, the rules for mining the SPECTRE protocol are primitive. The protocol states that new blocks are generated based on the blocks' fork ends. In addition, the protocol also removes the requirement that miners maintain a nonconflicting transaction. These settings allow miners to operate simultaneously and reduce block time intervals significantly, maximizing transaction recording speed and increasing transaction processing capacity.

Secondly, the SPECTRE protocol, to ensure transaction processing efficiency, specifies that conflict resolution tasks have no occasion to be performed during the mining phase. Thus, SPECTRE is an efficient protocol that permits miners to concurrently and more frequently create blocks but does not need to agree on the main chain or is not affected by the network propagation delays. Meanwhile, knowledge of the propagation delay in the network is not necessary for running a mining node. More precisely, the SPECTRE protocol designs a mechanism to resolve conflicting transactions by calculating votes 47. Hence, we introduce the voting algorithm pseudocode of SPECTRE (see Figure 7).

SPECTRE defines that transactions in block x occur before block y, denoted as $\mathrm{x} < \mathrm{y}$; otherwise, $\mathrm{x} > \mathrm{y}$. Additionally, the voting algorithm is to be adopted to launch all nodes Z ($\mathrm{Z} \in G$) in the whole DAG block G to vote for the final and accurate transaction result when there is a conflict between the transaction information recorded in the block x and y. The voting process can be expressed as $vote_{x,y}(z, G)$, where $vote_{x,y}(z, G) = -1$ depicts $\mathrm{x} < \mathrm{y}$, $vote_{x,y}(z, G) = 1$ captures $\mathrm{x} > \mathrm{y}$, and $vote_{x,y}(z, G) = 0$ represents a draw. Specifically, the voting rules are that 2 conflicting blocks x and y vote for themselves (i.e., −1 and +1, respectively), the future blocks created after block x are denoted as $future(x)$, where future blocks of x can merely be backdated to x, and so can y. In addition, the blocks generated before x or y can be seen as the sum of their own past blocks, and be written as $past(x)$ and $past(y)$ separately. Subsequently, each block counts votes for its own future block and then votes for the one that wins the most votes. Thus, a voting conflict resolution process is completed.

To summarize, the algorithmic idea of voting ensures the network security of the DAG blockchain. On the one hand, the algorithm makes the honest block vote for the honest block. In addition, the honest block behind gives the stack power to the front. As a consequence, the malicious attack failed, and the security calculation power can reach 51% [25]. On the other hand, SPECTRE also analyzes malicious attacks that are unable to point to the previous block or produce blocks that are not distributed to neighboring nodes. In the voting algorithm, attackers with less than 50% of the power are failed. Therefore, the SPECTRE protocol can resist "double-spend attacks" and "censorship attacks" effectively.

Thirdly, the essence of the blockchain of cryptocurrency is a ledger whose transaction information directly determines the asset information of users. Hence, accurate, authentic, and nonmodifiable transaction information is increasingly imperative for cryptocurrency protocols. Besides, the procedure that SPECTRE protocol generates trusted transaction sets can be summarized as follows: first of all, it traverses the block, extracts the transaction information in turn, and then adds the conflict-free transaction to its set. However, conflict transactions with insufficient account balances may be added to the conflict transaction set. Next, conflicting transactions, according to the voting algorithm, are voted in turn and then generate conflicting block order sets, which makes identifying valid transaction information possible. Furthermore, the voted valid transactions are added to the conflict-free transaction set. Finally, the transactions that have been concentrated for more than a certain time in a conflict-free transaction set are adopted to build a trusted transaction pool, which ensures the transaction information is virtually unable to be tampered with. However, once two conflicting transactions are published simultaneously, such that the same funds are moved to two different locations, the identity of the prevailing transaction might remain undetermined for arbitrarily long periods,

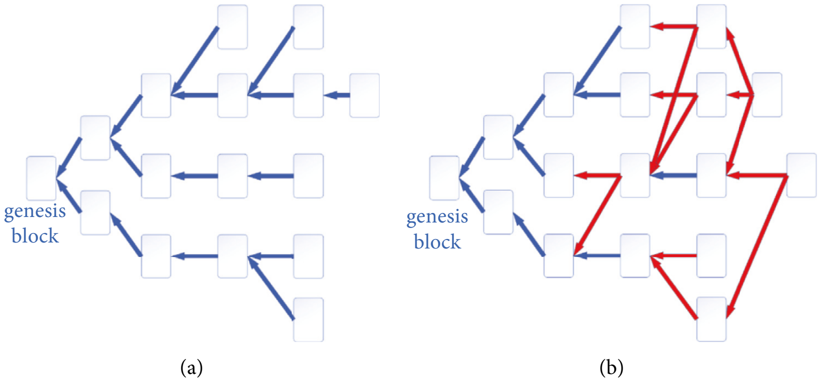

Figure 6: Structure comparison of Bitcoin blockchain (a) and DAG (b).

```
Algorithm 1 CalcVotes
Input: $G$–a block DAG
Output: $vote\,(virtual\,(G))$ – a pairwise ordering of blocks in $G$
if $G = \emptyset$ then
    return an empty ordering
for all $z \in G$ do
    $vote\,(z, past\,(z)) \leftarrow calcVotes\,(past\,(z))$   and break ties arbitrarily
for all $z \in G$ in some topological order (from leaves to root) do
    for all $x, y \in G\ (x \neq y)$ do
        if $(x \in \overline{past}\,(z) \wedge y \notin past\,(z)) \vee (x \in past\,(z), y = z)$ then
            $vote_{x,y}\,(z, G) \leftarrow -1$
        else if $(y \in \overline{past}\,(z) \wedge x \notin past\,(z)) \vee (y \in past\,(z), x = z)$ then
            $vote_{x,y}\,(z, G) \leftarrow +1$
        else if $x, y \in past\,(z)$ then
            $vote_{x,y}\,(z, G) \leftarrow vote_{x,y}\,(z, past\,(z))$
        else if $x, y \notin past\,(z)$ then
            $vote_{x,y}\,(z, G) \leftarrow \widetilde{sgn}\,(\Sigma_{z' \in}\ future\,(z, G)\ vote_{x,\,y}\,(z', G))$
$vote\,(virtual\,(G), G) \leftarrow \widetilde{sgn}\,(\Sigma_{z \in G}\ vote\,(z, G))$
return $vote\,(virtual\,(G), G)$
```

Figure 7: The voting algorithm pseudocode of SPECTRE.

which indicates that the owner's funds are secured by the cryptographic signatures.

From Figure 8, we can see that the RDL framework of SPECTRE meets the requirement of cryptocurrency security. In addition, honest users will do the same as long as an honest user ϵ-accepted a transaction using ChkRobustAccept, which benefits the security confirmation of transferring funds and then maintains the security of the RDL framework of SPECTRE.

Generally speaking, PHANTOM and SPECTRE have the same mining mechanism. Nevertheless, the protocol PHANTOM proposed by [50] makes up for the defect of SPECTRE that is unable to absolute sort for all the blocks. Above all, the PHANTOM identifies evil blocks by employing block connectivity analysis (note that block connectivity analysis mainly targets analyzing the edges pointed to and the ones that are pointed) and ensures their security. For instance, 2 common scenarios for attacks on DAG blockchains cause the reduced connection between evil blocks and other blocks. On the one hand, the generated blocks are not based on known end blocks, which results in fewer blocks that own blocks point to. On the other hand, blocks generated by other nodes cannot point to their own blocks if they are not released immediately. Moreover, given the maximum latency of the network, the honest blocks are bound to spread through the whole network after a certain period of time. Meantime, it is worth noting that connectivity has a threshold k below which blocks are considered evil and at an inferior position in sorting. Thus, honest blocks and evil blocks can be divided into strongly connected blue blocks and weakly connected red blocks, respectively. Additionally, PHANTOM, compared to SPECTRE, integrates smart contract functionality. Concretely, the language of smart contracts requires operations to be performed in a strict order, which requires that the smart contract-enabled blockchain network is characterized by a linear ordering of transactions in chronological sequence. Hence, PHANTOM creates a strict linear order for DAG blockchains and benefits the deployment of the smart contract.

To sum up, we compare the basic characteristics of the protocols of Bitcoin, SPECTRE, and PHANTOM in Table 1. Apparently, protocols play imperative roles throughout the implementation process of cryptocurrency. Above all, the underlying ledger structure and consensus mechanism are the 2 core elements (Figure 9) that make up a blockchain, and confirmation time, throughput limit, and ordering are

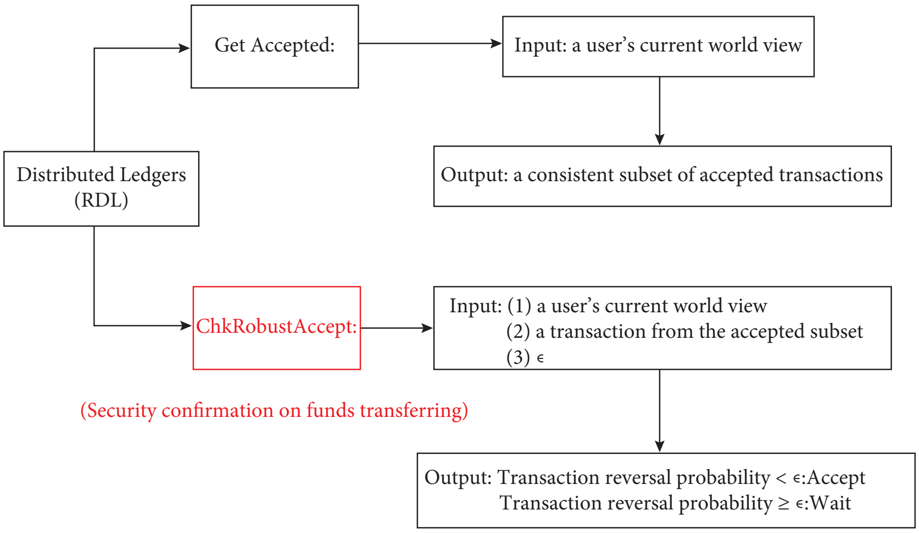
Get Accepted:
Input: a user's current world view
Output: a consistent subset of accepted transactions
Distributed Ledgers (RDL)
ChkRobustAccept:
Input: (1) a user's current world view
(2) a transaction from the accepted subset
(3) ϵ
(Security confirmation on funds transferring)
Output: Transaction reversal probability < ϵ:Accept
Transaction reversal probability ≥ ϵ:Wait

Figure 8: The security in RDL framework.

Table. 1: The basic characteristics of Bitcoin, SPECTRE, and PHANTOM.

Protocol	Ledger structure	Transaction conflict solution	Confirmation times		Throughput limit	Ordering
			Conflicts	No conflicts		
Bitcoin	Single chain	Longest chain	Slow	Slow	Latency	Linear
SPECTRE	DAG	Voting procedure	Not guaranteed	Very fast	Capacity	Pairwise
PHANTOM	DAG	Block connectivity analysis	Very slow	Slow	Capacity	Linear

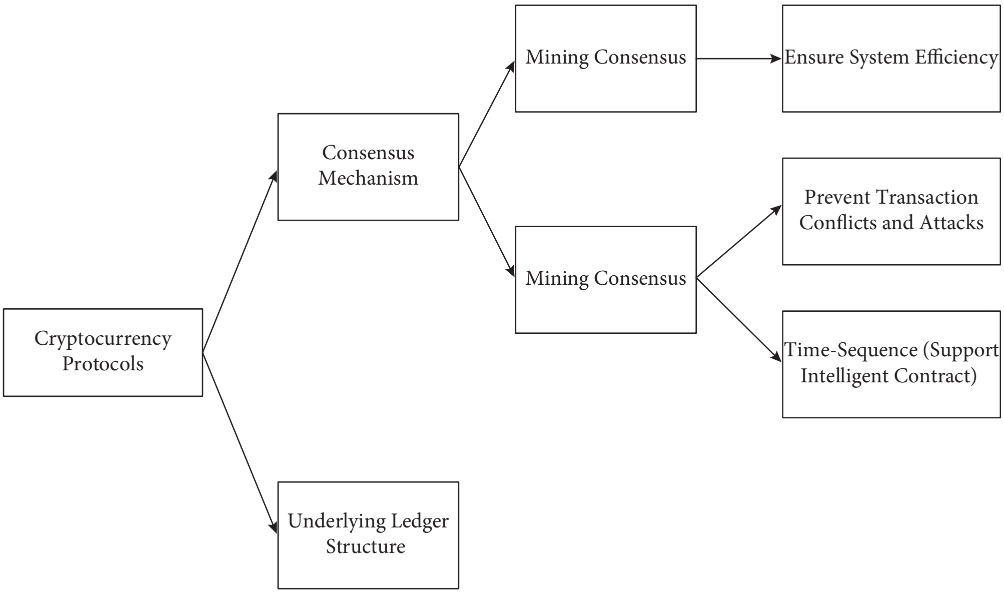
Mining Consensus
Ensure System Efficiency
Consensus Mechanism
Prevent Transaction Conflicts and Attacks
Mining Consensus
Cryptocurrency Protocols
Time-Sequence (Support Intelligent Contract)
Underlying Ledger Structure

Figure 9: The core elements of cryptocurrency protocols.

prerequisites for smart contracts. In particular, Bitcoin, acting as the first formal cryptocurrency protocol, represents the single main chain structure and linear order. Additionally, the transaction information in low-height blocks has a higher priority than that in high-height blocks. Meanwhile, the high height blocks are unable to contain the transaction that conflicts with the low height blocks. What's more, the Bitcoin protocol, to minimize the risk of a fork, has no choice but to stipulate the waiting periods of up to six blocks and ten minutes for transaction confirmation. Nevertheless, SPECTRE reconstructs the underlying ledger structure prescribed by Bitcoin, allowing for a large number of forks. Additionally, block heights cannot represent linear order, and neither the transactions in the front blocks are necessarily preceded that of the later fork blocks. Furthermore, the validity of the transaction information is determined by the voting algorithm. More importantly, the block voting algorithm can be implemented immediately. Meantime, the protocol allows for the inclusion of all forked blocks and has stronger transaction processing power than that of Bitcoin, up to 10 seconds of transaction confirmation time, more comprehensive attack resistance, and actual 51% security computing power. The PHANTOM protocol implements linear ordering of DAG blockchain structures, as well as conflict-free transactions and trusted transaction confirmation. The protocol costs a lot of time but meets the deployment requirements of smart contracts.

5. Limitations and Concluding Remarks

Nevertheless, our study has some inevitable limitations, which are expected to be solved in the near future. Firstly, some cryptocurrency protocols are not open source, which indicates that we cannot make intuitive comparisons on the protocol differences of the first 10 cryptocurrencies. Secondly, the influences of the total funds raised, duration, and employees of blockchain technology platforms on the technology progress and security of cryptocurrency are not clear. Besides, users may not give enough trust to cryptocurrencies in the short term even though they are technically safe. Meanwhile, the future of cryptocurrencies is highly uncertain with the contraction of national policies on emerging currencies. Thirdly, the protocols of Bitcoin, SPECTRE, and PHANTOM have their own advantages in terms of security capabilities. However, how to improve their security capabilities from the protocol itself is difficult and restricted by user demand.

Our purpose was to provide a point of entry for financial researchers and the government to gain a better understanding of the significant issues surrounding the security of cryptocurrencies based on blockchain. In particular, this article reviews the technological implementation of cryptocurrency, and the security and stability of cryptocurrency, and analyzes security support from blockchain technology platforms and blockchain technology. The empirical results of the top 10 blockchain technology platforms show that the security support from these platforms is insufficient and immature. Among these, the Bitmain platform plays a critical role in security support and has significant advantages in terms of raised funds, duration, and human resources compared to the study of Zyskind et al. [19] and Choi [13]. In addition, these blockchain technology platforms provide computational resources and benefit the selection of consensus algorithms for blockchain practitioners.

Next, the digital signatures and principle of the hash algorithm (SHA256) show that encryption ensures the security of cryptocurrencies. In particular, the former identifies the identity of the signatory and transaction, while the latter confirms ownership. In addition, SHA256 is infeasible for computing in the reverse direction and is difficult to attack. Moreover, the records in the blockchain can be queried by every participant, making the system information transparent and open reliable. Then, we further study Fu and Fang [14] and propose a blockchain structure that is composed of the security components and basic components of six layers that are independent and cannot be extended completely and have a certain coupling among them.

Furthermore, we compare the underlying ledger structure of Bitcoin and DAG and find that Bitcoin determines its main chain based on the “longest chain consensus,” which enables the exclusion of intentionally evil nodes, eliminates the situation that two nodes produce blocks simultaneity, and discards forked blocks that are not part of the main chain. Nevertheless, these forks have aroused security concerns that cannot be solved by Bitcoin totally. In addition, DAG has 5 mathematical properties, which are highly related to security issues. Moreover, we further compare 2 classic protocols of DAG blockchain including SPECTRE and PHANTOM and find that the structure of SPECTRE ensures network security and robustness from its block production, conflict resolution, and generated trusted transaction sets. Meanwhile, the voting algorithm of SPECTRE makes resolving conflicting transactions by calculating votes and ensuring the transaction information that is virtually unable to be tampered with possible. In particular, the security calculation power of SPECTRE can reach 51%, and resist “double-spend attacks” and “censorship attacks” effectively. Furthermore, the RDL framework of SPECTRE meets the requirement of cryptocurrency security. Next, we also find that the protocol PHANTOM makes up for the defect of SPECTRE, which is unable to absolute sort for all the blocks. Besides, PHANTOM identifies evil blocks by employing block connectivity analysis and ensures its security. Eventually, we compare the basic characteristics of the protocols of Bitcoin, SPECTRE, and PHANTOM and find that protocols play imperative roles throughout the implementation process of cryptocurrency even though they have significant differences. Besides, the underlying ledger structure and consensus mechanism are the 2 core elements that make up a blockchain, and confirmation time, throughput limit, and ordering are prerequisites for smart contracts.

The results also yield several practical implications for the security of cryptocurrencies. First, the scale and amount of blockchain technology platforms should be increased. Meanwhile, these platforms are expected to safeguard sensitive business data while they are being used, which can compensate for their insufficient support for the security and stability of cryptocurrencies. For instance, blockchain technology platforms ought to focus on shared business problems across markets faced by customers and secure aggregated datasets based on their computational resources.

Second, these platforms are supposed to revolve around the improvement of the consensus mechanism, especially the balance between decentralization, security, and scalability of the consensus mechanism. Then, a consensus mechanism can act as the core link to solve the problem of consistency and maintain the security of the blockchain consensus. Third, the hash function and other encryption algorithms are facing the threat of emerging quantum computing technology, which may integrate blockchain technology with quantum cryptography to secure the necessary data. Blockchain technology is expected to implement a more secure privacy protection scheme while exchanging data efficiently and actively exploring emerging encryption techniques such as homomorphic encryption and zero-knowledge proof, and privacy protection techniques such as anonymous communication technology. Fourth, the internal mechanism among the security components of the six layers should be concentrated on in future studies. Fifth, the balance between security, efficiency, and functionality of cryptocurrency protocols should be drawn attention to and regarded as the goal of future exploration. Above all, the RDL framework in protocols should be considered to maintain the security of cryptocurrencies.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Feiyu Xie and Chao Yu contributed equally to this work. They are the cofirst authors.

Acknowledgments

The authors are grateful for the financial support from the National Natural Science Foundation of China (71971055, 72173018).

References

[1] P. D. DeVries, "An analysis of cryptocurrency, bitcoin, and the future," *International Journal of Business Management and Commerce*, vol. 1, no. 2, pp. 1–9, 2016.

[2] M. Risius and K. Spohrer, "A blockchain research framework," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 385–409, 2017, https://link.springer.com/article/10.1007/s12599-017-0506-0.

[3] T. Tarasova, O. Usatenko, A. Makurin, V. Ivanenko, and A. Cherchata, "Accounting and features of mathematical modeling of the system to forecast cryptocurrency exchange rate," *Accounting*, vol. 6, no. 3, pp. 357–364, 2020.

[4] P. Febrero and J. Pereira, "Cryptocurrency Constellations across the Three Dimensional Space: Governance Decentralization, Security, and Scalability," *IEEE Transactions on Engineering Management*, 2020, https://ieeexplore.ieee.org/abstract/document/9254134.

[5] S. Davidson, P. De Filippi, and J. Potts, "Blockchains and the economic institutions of capitalism," *Journal of Institutional Economics*, vol. 14, no. 4, pp. 639–658, 2018.

[6] V. Shermin, "Disrupting governance with blockchains and smart contracts," *Strategic Change*, vol. 26, no. 5, pp. 499–509, 2017.

[7] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: understanding the challenges facing blockchain technology in financial services," *Information and Organization*, vol. 29, no. 2, pp. 105–117, 2019.

[8] R. Kirkland and D. Tapscott, "How Blockchains Could Change the World," 2016, https://www.mckinsey.com/industries/technology-media-and telecommunications/our-insights/how-Blockchains-could-change-the world.

[9] A. Walch, "The bitcoin blockchain as financial market infrastructure: A consideration of operational risk," *NYU Journal of Legislation and Public Policy*, vol. 18, p. 837, 2015, https://ssrn.com/abstract=2579482.

[10] K. Werbach, "Trust, but verify: why the blockchain needs the law," *Berkeley Technology Law Journal*, vol. 33, p. 487, 2018.

[11] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, Article ID 21260, 2008.

[12] A. Noda, "On the evolution of cryptocurrency market efficiency," *Applied Economics Letters*, vol. 28, no. 6, pp. 433–439, 2021.

[13] T.-M. Choi, "Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains," *Transportation Research Part E: Logistics and Transportation Review*, vol. 128, pp. 17–29, 2019.

[14] D. Fu and L. Fang, "Blockchain-based trusted computing in social network," in *Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pp. 19–22, IEEE, Chengdu, China, October 2016.

[15] Y. Su and Q. Fan, "Renewable energy technology innovation, industrial structure upgrading and green development from the perspective of China's provinces," *Technological Forecasting and Social Change*, vol. 180Article ID 121727, 2022, https://www.sciencedirect.com/science/article/abs/pii/S0040162522002530.

[16] Y. Su, X. Jiang, and Z. Lin, "Simulation and relationship strength: characteristics of knowledge flows among subjects in a regional innovation system," *Science Technology & Society*, vol. 26, no. 3, pp. 459–481, 2021.

[17] E. C. Bank, "Virtual currency schemes," 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[18] T. Moore and N. Christin, "Beware the middleman: empirical analysis of bitcoin-exchange risk," *Financial Cryptography and Data Security*, vol. 7859, pp. 25–33, Springer, 2013, https://link.springer.com/chapter/10.1007/978-3-642-39884-1_3.

[19] G. Zyskind and O. Nathan, "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings of the 2015 IEEE Security and Privacy Workshops*, pp. 180–184, IEEE, CA, USA, May 2015.

[20] Y. Lu, "The blockchain: state-of-the-art and research challenges," *Journal of Industrial Information Integration*, vol. 15, pp. 80–90, 2019.

[21] D. He, S. Li, C. Li et al., "Security analysis of cryptocurrency wallets in android-based applications," *IEEE Network*, vol. 34, no. 6, pp. 114–119, 2020.

[22] A. Sunyaev, "Distributed ledger technology," *Internet Computing*, Springer, Cham, pp. 265–299, 2020.

[23] V. Buterin, "The meaning of decentralization," 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

[24] K. Fani, M. Ferreira, and C. de Vroomen, "An exploration of state-of-the-art blockchain scalability approaches," https://www.semanticscholar.org/paper/An-Exploration-of-State-ofthe-Art- Blockchain-Fani-Ferreira/7cdeb2c8e132c2e003255d03dc3d14684831f8942019.

[25] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: a fast and scalable cryptocurrency protocol," *IACR Cryptol. ePrint Arch.*vol. 2016, no. 1159, 2016.

[26] X. Li, J. Xu, Z. Zhang, X. Lan, and Y. Wang, "Modular security analysis of oauth 2.0 in the three-party setting," in *Proceedings*

of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 276–293, IEEE, Genoa, Italy, September 2020.

[27] N. Sakimura, J. Bradley, B. de Medeiros, and C. Mortimore, “Openid Connect Core 1.0 Incorporating Errata Set 1,” 2014, http://openid.net/specs/openid-connect-core-10.html.

[28] J. Cant, “Gatehub Crypto Wallet Data Breach Compromises Passwords of 1.4m Users,” 2019, https://cointelegraph.com/news/gatehub-cryptowallet-data-breach-compromises-passwords-of-14m-users.

[29] T. Bui, S. P. Rao, M. Antikainen, and T. Aura, “Pitfalls of open architecture: how friends can exploit your cryptocurrency wallet,” in *Proceedings of the 12th European Workshop on Systems Security*, pp. 1–6, Dresden Germany, March 2019.

[30] K. Schwab, “The Fourth Industrial Revolution: What it Means, How to Respond,” *Economy, Culture & History Japan Spotlight Bimonthly*, Japan Economic Foundation, Tokyo, 2016.

[31] S. Lu, S. Li, W. Zhou, and W. Yang, “Network herding of energy funds in the post-Carbon-Peak Policy era: does it benefit profitability and stability?” *Energy Economics*, vol. 109, Article ID 105948, 2022.

[32] G. Hileman and M. Rauchs, “Global cryptocurrency benchmarking study,” *Cambridge Centre for Alternative Finance*, vol. 33, pp. 33–113, 2017.

[33] R. S. King, S. Williams, and D. Yanofsky, “By reading this article, you’re mining bitcoins,” 2013, http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins.

[34] S. Azouvi and A. Hicks, “Sok: Tools for Game Theoretic Models of Security for Cryptocurrencies,” 2019, https://arxiv.org/abs/1905.08595.

[35] Interpol, “Interpol holds first darknet and cryptocurrencies working group,” 2018, https://www.interpol.int/Newsand-Events/News/2018/INTERPOL-holds-first-DarkNet-and Cryptocurrencies-Working-Group.

[36] G. Hileman, “State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass,” 2016, http://www.coindesk.com/state-of-bitcoin-blockchain-2016.

[37] H. Albayati, S. K. Kim, and J. J. Rho, “Accepting financial transactions using blockchain technology and cryptocurrency: a customer perspective approach,” *Technology in Society*, vol. 62, Article ID 101320, 2020.

[38] D. W. McCloskey, “The importance of ease of use, usefulness, and trust to online consumers,” *Journal of Organizational and End User Computing*, vol. 18, no. 3, pp. 47–65, 2006.

[39] D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and validating trust measures for e-commerce: an integrative typology,” *Information Systems Research*, vol. 13, no. 3, pp. 334–359, 2002.

[40] R. Mcmillan, “The inside story of Mt. Gox, Bitcoin’s 460 Million Disaster,” 2014, https://www.wired.com/2014/03/bitcoin-exchange/.

[41] P. W. Coopers, “Money Is No Object: Understanding the Evolving Cryptocurrency Market,” 2015, https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-evolution.html.

[42] R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, “Distributed ledger technology: applications and implications,” *Strategic Change*, vol. 26, no. 5, pp. 481–489, 2017.

[43] R. Gendal-Brown, “On Distributed Databases and Distributed Ledger,” 2017, https://gendal.me/2016/11/08/on distributed-databases-and-distributed-ledgers/.

[44] E. D. Matemba and G. Li, “Consumers’ willingness to adopt and use WeChat wallet: an empirical study in South Africa,” *Technology in Society*, vol. 53, pp. 55–68, 2018, https://www.sciencedirect.com/science/article/abs/pii/S0160791X17302105.

[45] A. Kesharwani and S. Singh Bisht, “The impact of trust and perceived risk on internet banking adoption in India,” *International Journal of Bank Marketing*, vol. 30, no. 4, pp. 303–322, 2012, https://www.emerald.com/insight/content/doi/10.1108/02652321211236923/full/html.

[46] C. Martins, T. Oliveira, and A. Popovič, “Understanding the internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application,” *International Journal of Information Management*, vol. 34, no. 1, pp. 1–13, 2014.

[47] M. H. u. Rehman, K. Salah, E. Damiani, and D. Svetinovic, “Trust in blockchain cryptocurrency ecosystem,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1196–1212, 2020.

[48] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: beyond bitcoin,” *Applied Innovation*, vol. 2, no. 71, pp. 6–10, 2016.

[49] R. Böhme and T. Okamoto, “Financial Cryptography and Data Security,” *revised selected papers* in *Proceedings of the 19th International Conference, fc, san juan, puerto rico*, vol. 8975, pp. 26–30, Curaçao, March 2015.

[50] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, “Spectre: Serialization of Proof-Of-Work Events: Confirming Transactions via Recursive Elections,” *Computer Science*, 2017, https://www.semanticscholar.org/paper/SPECTRE-%3A-Serialization-of-Proof-of-work-Events-%3A-Sompolinsky-Lewenberg/65f1613a4f1b015fc64608b787227de0549f4cec.

[51] Y. Sompolinsky and A. Zohar, “Phantom,” IACR cryptology ePrint archive,” Report 2018/104, International Association for Cryptologic Research, France, 2018.