IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 20, 2022, accepted May 13, 2022, date of publication May 23, 2022, date of current version June 3, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3177275

Research on Multidimensional Trust Evaluation Mechanism of FinTech Based on Blockchain

YING SONG[1,2], CHAOHAO SUN[3], YUN PENG[2,4], YUE ZENG[5], AND BAOLIN SUN[1,2]

[1]School of Information and Communication Engineering, Hubei University of Economics, Wuhan 430205, China
[2]Research Center of Internet Financial Information Engineering Technology of Hubei Province, Wuhan 430205, China
[3]China Huarong Financial Leasing Company Ltd., Hangzhou 310016, China
[4]School of Finance, Hubei University of Economics, Wuhan 430205, China
[5]School of Software Engineering, Jinling Institute of Technology, Nanjing 211169, China

Corresponding authors: Baolin Sun (blsun@163.com) and Yue Zeng (zengy@jit.edu.cn)

This work was supported by the National Social Science Foundation of China under Grant 21BJY147.

ABSTRACT New technologies such as Internet, cloud computing, artificial intelligence (AI) and blockchain have greatly promoted the innovation of financial industry structure and paradigm, improved the efficiency of financial services and brought the spillover of the financial technology (FinTech) risk. The existing financial regulation methods cannot meet the needs of the development of FinTech, therefore, there is an urgent need to improve the trust mechanism. Blockchain can effectively solve the problems of security and trust in FinTech. This paper will explore the expression method of trust index in blockchain, and build based on blockchain a multi-dimensional trust index system and evaluation mechanism (MDTEM) for FinTech. Firstly, a four-level blockchain structure has been built, including cloud level blockchain, Internet level blockchain, contract level blockchain and application level blockchain in the FinTech ecological environment to ensure the security, reliability and trustworthiness of financial services. Secondly, according to the trust structure of blockchain on FinTech payment behavior, the index system and evaluation mechanism of direct trust, indirect trust, recommendation trust and feedback trust of FinTech based on blockchain are designed. Finally, the trust simulation experiment of FinTech mechanism is carried out from three aspects: data sending, data transmission, data reception and delivery success rate. Simulation results show that the proposed MDTEM trust mechanism can better improve the safe and reliable application of FinTech trust mechanism.

INDEX TERMS FinTech, blockchain, multidimensional trust, trust mechanism.

I. INTRODUCTION

With the rapid development of new technologies such as cloud computing, mobile Internet and artificial intelligence (AI), intelligent products and services have been widely developed, including smart phones, mobile terminal devices, mobile financial services, smart cities and intelligent vehicles. Especially in the field of financial technology (FinTech), these newly developed products and services have brought about the interconnection of all things and computing, with the characteristics of intensive computing, strong timelines and high data reliability, which result in great challenges in recognition ability, trust evaluation, security authentication and computing power for mobile devices. Thus, better security mechanism, trust evaluation mechanism and computing mode are urgently needed to improve the security and reliable processing capability of FinTech terminal equipment [1]–[4]. Combined with new technologies such as mobile Internet, blockchain, cloud computing and AI, this paper clarifies the index system and evaluation mechanism of FinTech trust, and puts forward suggestions for future challenges.

FinTech has new technological paradigm and multi-dimensional characteristics. Its core is the mutual promotion, interaction and integration of financial industry and new technology, and finally promotes the subversive innovation of financial industry structure [5]. New innovation will reconstruct each of the financial applications, form a new organizational form or pattern, reshape the underlying logical structure of finance, and achieve better financial innovation. New technological innovation speeds up the data flow between different financial entities, helps effective financial information and funds flow from financial institutions to real industries, and makes FinTech capable to prevent risks. Due to the development of blockchain technology,

The associate editor coordinating the review of this manuscript and approving it for publication was Hayder Al-Hraishawi.

Chawla [6] redeveloped crowdfunding, platform, organization and governance in finance, and proposes a new algorithm and organizational structure for the integration of trust and blockchain by introducing the integration mechanism of trust and blockchain into traditional financial theory. FinTech is mainly used in financial business processing, monitoring, reporting, compliance and other financial issues. It is important to correctly deal with the rapidity, security and reliability of financial data, and to improve the theoretical basis and research methods related to FinTech.

Blockchain is a new mode to generate and update data in the Internet space by new technologies including distributed data storage, point-to-point data transmission, distributed node consensus algorithm, encryption algorithm and so on. Blockchain uses the intelligent contract composed of automatic script code to process data [5]–[7]. The essence of blockchain is a decentralized database, which is also the underlying technology of bitcoin. As the basic supporting technology of digital currency, blockchain can build its information effectiveness and classification transactions in a decentralized public environment in a safe and verifiable way [8]. The blockchain records digital transactions as blocks, and forms a linked list structure. Any node in the Internet obtains a hash value for each newly generated block, and then this hash value binding with the previous block is put into the current block for forwarding, which forms an irreversible chain and stores in the distributed database [9]. Blockchain technology can be used for mobile Internet, wireless Internet, clearing and settlement of cross domain financial assets, financial transaction records, transmission of financial data, identity authentication, access control, and supply chain process traceability management, etc. Blockchain can reduce the problem of attack in key distribution, solve the single point of failure of key nodes, and ensure the anonymity of node data ownership with considerable potential in establishing a more secure FinTech field [10]–[12].

Trust is to learn from the experience of others, effectively reduce the high perceived risk and uncertainty caused by the interaction between the subject and unfamiliar targets, and quickly establish the perceived trust of unfamiliar subjects. Trust mechanism is the basis of FinTech payment. The development of FinTech business needs a trust mechanism established through relevant processes, such as transactions and processing based on financial information. Trust represents the value consensus of all parties in FinTech transactions. To some extent, trust mechanism is more dependent on FinTech business information. Trust evaluation mechanism is one of the most challenging issues for the security and efficiency of FinTech [7]–[9].

Although the integration of blockchain and FinTech has effectively promoted the development of FinTech, its integrated trust evaluation index and trust evaluation mechanism still need to be improved and optimized.

Challenges: the shortcomings of the existing blockchain based trust mechanism bring the following challenges.

1) How to design a multi-dimensional trust index system suitable for the security and reliability of FinTech services?

2) The existing trust evaluation mechanisms rarely considers the impact of the dimension and weight of trust indicators.

3) Trust management and evaluation can be distributed through the consistent trust database using blockchain technology to avoid centralized management.

Contribution: This research work aims to propose a better evaluated trusted, safe and reliable multi-dimensional trust evaluation mechanism (MDTEM) based on blockchain in FinTech to meet the above challenges. The MDTEM mechanism is characterized by:

1) Build a four-level blockchain structure of cloud level, Internet level, contract level and application level to ensure the security, reliability and credibility of FinTech data;

2) Design multi-dimensional trust evaluation mechanisms (MDTEM) such as direct trust, indirect trust, recommendation trust and feedback trust of FinTech service providers based on blockchain, and establish comprehensive trust value through adaptive weight mechanism;

The remainder of the paper is organised as follows. Section II discusses the related work; Section III introduces the integration framework of blockchain and FinTech, and the data structure of blockchain trust evaluation; Section IV defines the trust index system in FinTech; Section V designs a FinTech trust evaluation mechanism based on blockchain; In Section VI, the simulation experiment is studied and analyzed; Finally, section VII presents the conclusions and future work.

II. RELATED WORK

With the rapid development of mobile Internet and FinTech in recent years, blockchain technology has improved the security, contract and efficiency of service provider authentication, data payment and data transmission of FinTech.

A. BLOCKCHAIN AND SMART CONTRACT TECHNOLOGY

Blockchain has experienced exponential growth in the past few years, which provides a new mechanism for FinTech business interaction and decentralized transactions. Blockchain is an important underlying support technology in digital currency applications, with a more reliable, complete and secure distributed architecture, by supporting secure and trusted distributed data transmission. In essence, Blockchain has the key characteristics of decentralization, distribution and consistency, which can effectively improve the application of FinTech [3], [4]. However, security and privacy have become thorny issues. Even though blockchain provides decentralized peer-to-peer security for all financial transactions, there are still many security vulnerabilities. The sustainable growth of blockchain lies on maintaining the security. How to ensure the financial payment trust mechanism in blockchain has always been the key to its success [5]–[7].

Smart contract (or consensus mechanism) refers to a set of protocols defined in digital form, with dynamic changes

and computer programs running on the blockchain system. Smart contract ensures the execution of fraud free contract without any trusted third party. Smart contracts can improve the decentralized storage of FinTtech services, the independent execution of contract codes, and the decentralized establishment of trust and the intelligent processing of digital assets on the blockchain ledger [8]–[11]. The smart contract functions as an autonomous entity on the blockchain, which can execute logic determinedly according to the data provided to the blockchain. Compared with traditional contracts, smart contracts entitle their users to compile the agreements and trust relationships by providing automated transactions without the supervision of central authorities. In order to prevent contract tampering, smart contracts are copied to each node of the blockchain network [8]–[9]. Wei *et al.* [10] proposes a data transaction authentication model (DTAM) based on the blockchain of FinTech business and smart contract, and wrote the content of financial data transaction authentication into the smart contract and deployed it on the blockchain of FinTech business. Their study ensures that the authentication data to be saved forever and not be tampered with. Blockchain is also the core technology in smart contract applications. Through probabilistic and deterministic contracts, blockchain can quickly improve trust identification and evaluation in the field of FinTech [11]. In addition, Blockchain can expand the trust relationship from user level to all related applications of FinTech. Singh *et al.* [12] proposes a blockchain-based distributed trust management scheme. The scheme uses smart contract technology and introduces the concept of blockchain fragmentation to reduce the load on the main blockchain and improve the data transaction throughput. Afzaal *et al*. [13] proposes a secure and trustworthy blockchain based crowdsourcing (STBC) consensus protocol. STBC protocol selects nodes with high trust from blockchain management nodes, crowdsourcing service providers and consumers as trust verifiers to verify transaction data and block data to prevent malicious behaviors. In the whole network, the scheme maintains and updates the reliability of nodes and the trust value of nodes through blockchain technology, and also promotes the trust relationship between nodes. Thus, blockchain is one of the key technologies for the security of FinTech application environment [14], [15]. Besides, when blockchain extends from a single trust model to a multi-dimensional one or distributed one, the whole model can be described as a parallel combination of smart contracts and users with the objective function maximized and stronger trust model achieved in the FinTech application environment.

B. INTEGRATION OF BLOCKCHAIN AND FinTech

FinTech is a new field in the current financial application research. New technologies such as mobile Internet, blockchain, AI and cryptography are applied to FinTech. In the field of financial payment, the advantages of blockchain technology such as disintermediation, openness, transparency and non-tampering are more and more used to record financial transaction information on the financial blockchain, and to solve problems such as long term payment, low payment fees and bad transparency [5], [6]. When financial transactions are generated between mobile Internet devices, they remain unchanged throughout the life cycle of the blockchain, ensuring the security and integrity of the trust database. Blockchain technology can reduce the cost of FinTech, improve the efficiency of financial payment, and create a new financial model.

FinTtech risk assessment is a comprehensive evaluation system with three-dimensional digital infrastructure, diversified supervision modes, compound uncertainty and incomplete knowledge. Blockchain technology is considered as a reliable solution to the long-standing trust problem among financial partners in FinTech businesses [16]. Because blockchain helps to improve the security of FinTech transactions and data exchange, enhance the efficiency and quality of FinTech business communication, and increase business reliability. Javaid [17] proposes a blockchain based Internet of things trust model, which records the data transactions executed by nodes in the Internet of things into the blockchain, and uses the Proof of Authority (PoA) consistency algorithm to verify and add the data information in the block. Routledge and Zetlin-Jones [18] proposes an Ethereum network exchange rate stability policy mechanism in the smart contract blockchain environment. The policy mechanism dynamically adjusts the exchange rate through the smart contract blockchain, which can better eliminate speculative attacks and implement the commitment to the policy in a better way. Chang *et al*. [19] discusses that blockchain technology is an influential technology in the application of FinTech, and a presenter of planned behavior theory based on blockchain technology in FinTech, managing the knowledge sharing of financial services in a more structured way.

C. TRUST MECHANISM OF FinTech

Due to the inherent attribute of the openness of mobile Internet, the risk of FinTech services makes the risk of Internet service providers' trust evaluation services more complex. The reliability of the trust evaluation service provider meets the needs of the service requester and ensures that the performance of the trust evaluation application is more reliable. The failure of the service will reduce the trust between mobile Internet trust evaluation services, which will bring setbacks to FinTech trust evaluation services. It is very important to detect unreliable service providers from reliable ones to ensure the security, reliability and computing power of the mobile Internet environment for FinTech services. To sum up, the trust evaluation mechanism of FinTech services will be one of the important methods to effectively evaluate reliable services.

The trust evaluation of FinTech services has attracted the attention of many researchers in the FinTech industry, and several revolutionary results have been produced. Gao *et al*. [20] studies the design of multi-dimensional trust evaluation mechanism for Internet of Thing (IoT) users, and proposes a service-oriented cooperation mechanism, which

can evaluate the credibility of mobile users and improve the reliability of mobile users. Huang *et al*. [21] studies the trust management in vehicle edge computing and proposes a distributed reputation management system (DREAMS), which divides the trust dimension into three dimensions: similarity, familiarity and timeliness, AI technology and multi weight subjective logic are used to maintain and update the trust information of local services. Yuan and Li [22] provides a reliable computing trust algorithm based on multi-source feedback mechanism in the Internet of things environment, which can better improve its computing power and reliability in terms of storage, energy and terminal device communication overhead. Cui *et al*. [23] proposes a new distributed trusted edge computing platform, which combines blockchain technology with mobile edge computing to enable each participant to establish a trusted system.

Xu *et al*. [24] proposes a solution to the conflict of interest and lack of trust in swarm intelligence. Firstly, a reward and punishment model is used to adjust the incentive mechanism of stakeholders, and then the blockchain intelligent contract technology is used to realize the predefined rules of trust on multiple trust servers on the Internet to form a trustless swarm intelligence platform. In order to improve device utilization and reduce trust computing load and trust path redundancy in mobile environment, Du *et al*. [25] proposes a graph theory based computational trust evaluation optimization model (TM-GT). In the TM-GT model, firstly, the directed weighted graph of trust relationship is constructed, and then the adaptive aggregation method based on information entropy theory is used to aggregate the trust value, correct the difference between multi-source trusts, and finally filter the nodes that obviously do not meet the trust requirements to reduce the computing consumption. Feng *et al*. [26] studies the data collection methods such as mobility, low cost and flexibility in the financial data collection process of mobile crowdsourcing (MCS), and constructs a decentralized MCS model based on blockchain. The model anonymously verifies the trust scheme through trusted trust evaluation, changes the user's public/private key pair, and mixes the newly changed key in multiple forged keys, solving the trust and security problems of data collection in MCS. Lockl *et al*. [27] studies the evaluation of the sensor data recording and monitoring system of the Internet of things based on blockchain, and proposes to use the smart contract technology of blockchain to evaluate the availability, integrity and computing cost of data. This evaluation mechanism has brought higher operation efficiency. These trust mechanisms and evaluations mainly solve the problems of security, trust and evaluation in the Internet, especially the trust mechanism of blockchain technology applied to mobile Internet, which better optimize and improve the trust problems related to mobile edge computing, smart contract, data monitoring and many others [28], [29].

Aiming at the trust rating of message sources in vehicle network, Yang *et al*. [30] uses Bayesian inference model to verify the trust level of messages, and proposes a vehicle network decentralized trust management system based on blockchain technology, which can improve the evaluation of trust level more efficiently. Kouicem *et al*. [31] proposes a hierarchical and scalable blockchain trust management protocol to support mobility in large-scale distributed IoT systems. The protocol transmits the trust information provided by the service provider to the mobile intelligent object through the blockchain technology, so as to speed up the trust decision better. The trust value of dynamically changing IoT, cloud computing and fog computing services is one of the key issues in current trust management. Mousa *et al*. [32] establishes a trust management framework, which uses the concept adopted by society to evaluate its initial trust value by observing the behavior of newcomers without trust resources, so as to achieve better trust management. Hussain *et al*. [33] studies the problem of machine trust in social behavior, and proposes an evidence fuzzy multi-criteria decision-making mechanism based on multi-dimensional trust quantification; the conclusion of this study shows that trust perception will initialize trust behavior, and that trust behavior will affect subsequent trust perception. Atwa *et al*. [34] proposes a risk-based trust evaluation advanced model (RTEAM). RTEAM is an entity centered trust model. Associating risks with that whether believing the reported event or not, RTEAM detects the event status, and evaluates based on multifaceted trust and multi hop trust. Therefore, RTEAM shortens the processing time, saves resources, and consumes a certain amount of energy. Malakhov *et al*. [35] analyzes the problems arising from the application proof-of-work (PoW) in the permissioned blockchain, and proposes a solution, which constructed a quantitative analysis model to estimate the hash ability of balancing heterogeneous PoW, based on the sliding window algorithm. However, the trust evaluation of blockchain application in FinTech remains to be explored.

III. INTEGRATION FRAMEWORK OF BLOCKCHAIN AND FINTECH

A. BASIC FRAMEWORK FOR THE INTEGRATION OF BLOCKCHAIN AND FinTech

The basic framework for the integration of blockchain and FinTech can be divided into four-levels: Cloud level, Internet level, Contract level and Application level. In this framework, each FinTech service terminal device is connected to the Internet and the cloud server. The FinTech terminal equipment registers with the certification authority through the edge server to realize the mutual communication between any pair of equipment in the FinTech Internet environment. The basic framework of the integration of blockchain and FinTech is shown in Figure 1.

In the cloud level blockchain, all FinTech servers are connected to the cloud, and all data generated by terminal devices are stored in the blockchain. Blockchain has a special data structure for maintaining status and transaction history. Each block contains a hash that binds itself to the previous block. All data blocks are instantiated and distributed to all cloud server in the Internet, in that way allowing data to be stored in

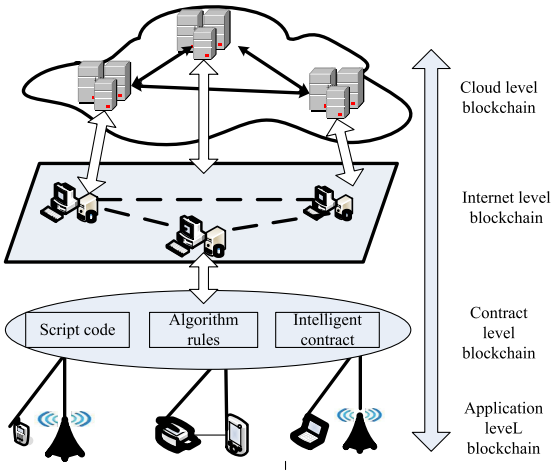


FIGURE 1. Basic framework for the integration of blockchain and FinTech.

an effective, verifiable and permanent way. Digital signatures and hashes are used in the blockchain to ensure data integrity. Once a data block is inserted into the chain, all data blocks in the chain cannot be modified to ensure that data in the blockchain will not to be miswritten. Its typical applications include: data block, Merkle tree, hash function, blockchain structure, time stamp, public encryption, etc.

In the Internet level blockchain, FinTech servers are installed on servers with cloud service functioning as a blockchain manager is responsible for blockchain control, including creating, verifying and storing individual transactions and transaction blocks. After generated by the FinTech terminal device, transaction blocks will broadcast to the Internet supported by the FinTech server. As the blockchain manager, the interconnection server will periodically integrate the received transactions into a block with consensus protocol, and broadcast the block to other edge servers for verification. In this way, some key security functions in blockchain network are realized, including privacy protection, identity management, information security, credibility, counter-attack, the use of advanced encryption technology and decentralized access control.

In the contract level blockchain, it mainly ensures an agreement in the blockchain system for the relevant nodes in FinTech reach, and then to realize intelligent processing through script code and algorithm. Therefore, the participant nodes in the blockchain system have the same confidence, that their ledger is consistent and accurate, and have the same consensus. The consensus of blockchain system means that all honest nodes with high trust value agree to a value/transaction. Values/transactions are generated by honest/trusted nodes. The main contents include: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), distributed mechanism, smart contract, algorithm mechanism, script code, etc.

In the application level blockchain, millions of different devices with financial applications are connected to the financial network. At this level, the privacy and confidentiality of data related to financial transactions must be guaranteed, as privacy breaches may occur because each participant can access all information in the public blockchain. Its typical applications include: programable coin, programable finance, programable society, etc.

B. DATA STRUCTURE OF BLOCKCHAIN

Due to the distributed characteristics of blockchain database, blockchain technology does not need third-party verification and central authority. The distributed database converts all transaction data on the Internet into associated strings and stores them in a block. This block is constructed within a certain time. The hash pointer is used to point to the previous data block, and all blocks form a complete single chain. The blockchain data structure of FinTech business is shown in Figure 2. The distributed database is also verified by the asymmetric encryption algorithm in cryptography to encrypt the internal data and ensure the security of the data.

In Figure 2, the data block size of the blockchain is B_i. It is assumed that there is N_m all mobile Internet devices. All mobile data in the Internet have security parameter k, and through the blockchain based multi hash function H: $\{0,\ 1\}^i \ \rightarrow \ \{0,\ 1\}^k$. The output value of the multi hash function H is expressed as a k-bit stream $m_k(= h^k(s))$ $(k \in [1, 2, \ldots, m]$, $s \in R\{0,1\}^k)$, where k is the safety parameter and s is the seed.

In order to generate a data stream, all mobile Internet users use $R\{0,1\}^n$ to create n bit blocks, as shown in formula (1). According to formula (1), the corresponding block $B_{(n,b)}$ can be generated for n packets, and then the processing process related to formula (2) can be carried out, and thus the data stream delivered to the mobile Internet can be generated.

$$B_{(n,b)} = \{(n, b)|b = 1, 2, \ldots, m\} \tag{1}$$

$$H_x(m_k) = P_{[(x,b)]} = \{(x, b)|x = \text{number of packets}, \quad b = \text{number of blocks}\} \tag{2}$$

The Internet data stream consists of two hash values, such as formula (3) and formula (4), depending on the number of packets in sequence number i and hash function H(·) The first and last packets of mobile Internet data stream depend on level 1 to ensure the continuous process of the data stream with the hash chain will not be interrupted, the data generated by adjacent mobile Internet devices will not be lost. Thus, real-time data management is realized.

$$\mathrm{H}_{(x+1,x+2)\ \mathrm{mod}\ 2^l}(m_x) \quad if\ x = 2n - 1 \tag{3}$$

$$\mathrm{H}_{(x-2,x-2)\ \mathrm{mod}\ 2^l}(m_x) \quad if\ x = 2n \tag{4}$$

This structure verifies mobile Internet data by adding signatures to the first and the last packets of multiple hash chains generated in the process of creating mobile Internet data streams. Thus, it has less overhead than adding signatures to all data stream packets. In particular, the edge server can obtain the hash value of the data stream m_k and check whether the mobile Internet data stream has changed through the hash

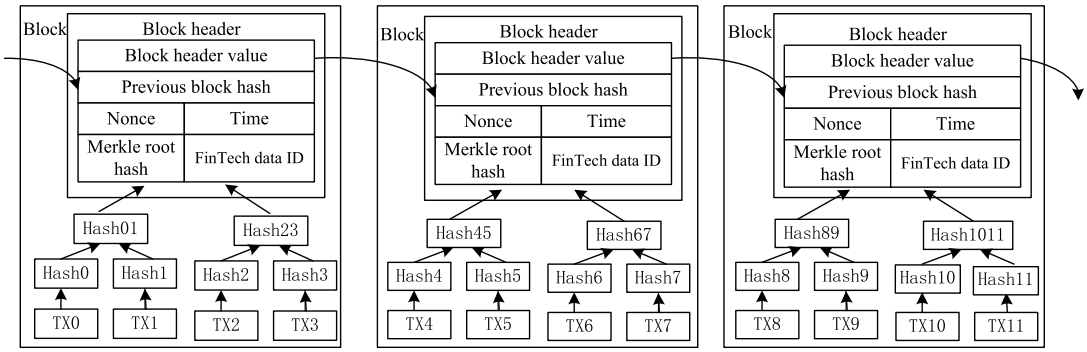


FIGURE 2. Data structure of blockchain.

value contained in $P_{[(x,b)]}$ even if the first and the last signed data packets are lost.

C. INTEGRATION OF BLOCKCHAIN AND TRUST MECHANISM

As one of the key underlying supporting technologies of FinTech, blockchain can build FinTech affairs in a safe and verifiable way in a decentralized FinTech ecological environment. Due to the impact of mobile environment, FinTech business, and blockchain technology, processing capacity of mobile terminals are limited in the internet of FinTech. So, it is necessary to integrate blockchain and trust mechanism, to add trust indicators to the blockchain list, and to realize the identification of customer security and trust degree. Figure 3 shows the structure of the integration of blockchain and trust mechanism.

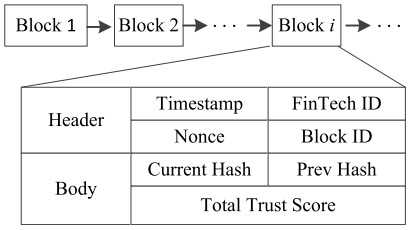


FIGURE 3. The integration structure of blockchain and trust mechanism.

IV. ANALYSIS OF TRUST RELATIONSHIP IN FINTECH

A. THEORY OF TRUST

Trust, a key concept in management, has a wide impact on FinTech in multi-level analysis. In traditional theory, trust is composed by three dimensions: ability, emotion and integrity.

Due to the trust relationship with FinTech, the blockchain is regarded as an important technical tool in establishing decentralized financial business in FinTech. In this ecosystem, services belonging to different parties can be organized, and service contributions in the mobile Internet can receive appropriate encouragement. Many blockchain based methods have been proposes to improve the trust relationship of FinTech.

Definition 1: Direct trust can be regarded as the trust evaluation obtained from the historical payment information that the service requester d_i to the service provider d_j within a certain period of time. The direct trust evaluation based on blockchain trains the trusted and untrusted behavior patterns of relevant users through blockchain and machine learning firstly. Then, according to the behavior data recorded in the blockchain trust and the matching of their related patterns, the trust weight of successful matching is accumulated. The trust is evaluated based on the blockchain, machine learning and objective behavior. The latest service interaction score set provided by service provider i to service provider j is recorded as $S_{ij} = \{s_1, s_2 \ldots s_n\}$, where the payment success score is 1 and the failure score is 0. The trust sequences are stored in the relevant trust evaluation data server. Direct trust DT_{ij} can be calculated by the risk probability model of formula (5).

$$DT_{ij} = \frac{p \times q^{-1/\alpha}}{p+q} \tag{5}$$

where p is the number of successful deliveries in a certain time t, q is the number of failed deliveries in a period of time t, using the penalty factor α. It can prevent sudden attacks by untrusted or malicious service providers after accumulating a high degree of trust.

Definition 2: Indirect trust value is to store the payment process from the requester to the service provider in the trust database within a certain period of time. The trust server will calculate the trust relationship between the FinTech service provider and the service requester according to the trust evaluation value of the service provider. It is an indirect way for the FinTech service requester to obtain the trust relationship of the service provider. The IT_{ij} of indirect trust can be calculated by formula (6).

$$\mathrm{IT}_{ij} = \frac{1}{n} \times \sum_{k=1}^{n} T(t_k) Pr_{ik} RT_{kj} \tag{6}$$

where $T(t_k)$ represents credibility, Pr_{ik} represents reliability, and RT_{kj} represents the trustworthiness of the service provider itself.

Definition 3: Recommendation trust is a special type of trust composed of the public neighbors of service requesters

and service providers. Only considering the interaction between service requesters and service providers is not enough to deal with various trust relationships in FinTech services. Recommendation trust depends on two aspects: the level of trust of the recommender himself, and the level of trust of the recommender to the service provider. Thus, different weight is given to each recommender.

The server k of the public neighbor directly trusts the service provider j and recommends it to the service requester i. The recommended trust R_{ij} stores the trust evaluation value in the trust evaluation server in the form of matrix, and the trust evaluation server updates and manages it. To reduce boasting, the trust evaluation server sets the value of DT_{11}-DT_{nn} to 0. The RT_{ij} of recommended trust can be calculated by formula (7).

$$RT_{ij} = \begin{bmatrix} 0 & DT_{12} & \cdots & DT_{1n} \\ DT_{21} & 0 & \cdots & DT_{2n} \\ \vdots & \vdots & \vdots & \\ DT_{n1} & DT_{n2} & \cdots & 0 \end{bmatrix} \tag{7}$$

Definition 4: Feedback trust evaluation can be regarded as a trust evaluation value aggregated based on the opinions of other direct neighbor servers.

In the feedback trust evaluation mechanism is based on blockchain, so it is necessary to calculate the trust relationship formed by the fusion of direct trust and recommendation trust, and to generate weights to balance its impact on the final trust. The advantages of establishing feedback trust are improving the trust of service requesters and the transaction payment rate, and promoting the optimization and iteration of FinTech. Feedback trust evaluation needs to be established to make feedback trust of service requesters to be transmitted to financial regulators faster. According to various trust relationships and aggregation rules, feedback trust FT_{ij} can be calculated by formulas (8) and (9)

$$FT_{ij} = \frac{1}{k} \sum_{l=1}^{k} Q_{ij}^{l} \tag{8}$$

$$Q_{ij}^{l} = DT_{i2} \times DT_{23} \times \cdots \times DT_{lj} \tag{9}$$

where: Q_{ij}^{l} represents the feedback trust value calculated from the l-th trust path from service requester i to service provider j; i=1, 2, $\cdots$, n, j represents the numbers of all servers passing through the trust path; FT_{ij} represents the aggregate value of feedback trust of all trust paths between two servers, that is, the trust relationship between server i and server j; l represents the total number of trust paths between servers.

Definition 5: Comprehensive trust refers to the aggregation and normalization of the results of relevant trust, such as direct trust, indirect trust, recommendation trust and feedback trust, based on blockchain to obtain the final trust evaluation result.

Comprehensive trust is the trust relationship derived from the comprehensive consideration of service requestors to service providers. It is the final trust evaluation value aggregated from the direct trust, indirect trust, recommendation trust and feedback trust obtained by financial services in a certain period of time. When no direct service record between financial service providers is available, recommendation trust and feedback trust are regarded as comprehensive trust to build the trust relationship between unfamiliar financial service providers. The comprehensive trust T_{ij} can be calculated by formula (10)

$$T_{ij} = w_1 DT_{ij} + w_2 IT_{ij} + w_3 RT_{ij} + w_4 FT_{ij} \tag{10}$$

where w_1, w_2, w_3, and w_4 are the adaptive weights of direct trust, indirect trust, recommendation trust, feedback trust, etc., respectively. Moreover, $w_1 + w_2 + w_3 + w_4 = 1 (0 \leq w_1, w_2, w_3, w_4 < 1)$.

V. FINTECH TRUST EVALUATION BASED ON BLOCKCHAIN

A. MEASUREMENT OF MULTI-DIMENSIONAL TRUST INDEX IN FinTech

According to the requirements of FinTech security, the MDTEM index of the blockchain are defined as five levels: very low (value: 0-0.2), low (value: 0.2-0.4), medium (value: 0.4-0.6), high (value: 0.6-0.8) and very high (value: 0.8-1.0). Then, the evaluation function of multidimensional trust of blockchain is established. Finally, the evaluation and analysis of multidimensional trust of blockchain are realized.

In the trust discrimination of FinTech, the qualitative discrimination category is easier to understand than the quantitative one. Using the digital identity trust discriminant function, the qualitative category can be determined according to the quantitative trust score. The categories are defined in detail as follows:

No trust ($0 \leq t_i \leq 0.2$): Digital identity is not trustworthy at all. Service providers can only provide uncritical or public services to service providers, and their only purpose is to identify recurring service providers.

Low trust ($0.2 < t_i \leq 0.4$): The credibility of digital identity is limited. The relying party can only accept the identity of noncritical services, which is intended to improve the barriers to re-entry using the new identity. This is reasonable for using the reputation system to reduce the whitewash after accumulating negative feedback.

Medium trust ($0.4 < t_i \leq 0.6$): Digital identity has a general degree of trust. Service providers can use identity when there is a low risk. For example, a person orders goods in an online store with a limited two digit number. Payment failure due to misuse of digital identity may be considered tolerable by the service provider.

Higher trust ($0.6 < t_i \leq 0.8$): The credibility of identity is high. In case of high risk, the service provider can accept the identification. For example, book a hotel room or an apartment.

Best trust degree ($0.8 < t_i < 1$): The trust of digital identity is advanced, and the highly critical applications or behaviors that can be accepted by service providers are limited by law.

B. BUILD A MDTEM MECHANISM FOR FinTech BASED ON BLOCKCHAIN

According to the MDTEM risk index system, the trust risk index is defined in the blockchain list. Moreover, the blockchain and trust risk quantitative index database is established, and the monitoring and management of customer trust identification and real-time processing of FinTech are realized. The trust indicators are defined as follows:

1) ATTRIBUTE TRUST

It is an attribute of the service providers participating in FinTech. (including name, date of birth, gender, registration time, location and other relevant information).

$$\mathrm{ATrust}(a, b) = (|a_b \cap b_a|)/N \tag{11}$$

where $|a_b|$ represents the trust of service provider a to service b, $|b_a|$ represents the trust of service provider b to service a, and N represents the number of service operators.

2) CREDIBILITY TRUST

It is a trust attitude between service providers a, which has a negative or positive impact on credibility.

$$\mathrm{CreTrust}(a) = |\text{positive attitude} - \text{negative attitude}| \tag{12}$$

3) INTERACTIVE TRUST

It is the communication time and processing time of FinTech transactions between computing service provider a and computing service operator Z.

$$\mathrm{ITrust}(a) = \sum_{z=1}^{n} a_z \tag{13}$$

where a_z represents the sum of communication time and processing time of service operator Z.

4) PROCESSING CAPABILITY TRUST

It is the processing capability of service provider a, etc. $\mathrm{CTrust}(a) =$ the processing capability of service provider a.

5) PARTICIPATION TRUST

It reflects the degree of service providers participation in FinTech.

$$\mathrm{PartTrust}(a) = |\text{number of participants}|/\text{total number} \tag{14}$$

6) TIME TRUST

It is a time-based trust relationship between service providers.

$$\mathrm{TTrust}(a, b) = \alpha N_p(a, b)/(\alpha N_p(a, b) + (1 - \alpha)N_q(a, b)) \tag{15}$$

where $N_p(a, b)$ represents the trusted time between service provider a and b, and $N_q(a, b)$ represents the untrusted time between a and b, α is the weight coefficient, $0 \leq \alpha < 1$.

7) FRIEND TRUST

The friend trust relationship between neighbors a and b in FinTech activities can be expressed as follows.

$$\mathrm{FTrust}(a, b) = |\mathrm{F}(a) \cap \mathrm{F}(b)|/|\mathrm{F}(a) \cup \mathrm{F}(b)| \tag{16}$$

where $|\mathrm{F}(a)|$ represents the number of trusted neighbors by the friend of service provider a, and $|\mathrm{F}(b)|$ represents the number of trusted neighbors by the friend of service provider b.

The comprehensive trust between service providers a and b is calculated as follows:

$$\begin{aligned}\mathrm{Trust}(a, b) = {} & \alpha_1 \cdot \mathrm{ATrust}(a, b) + \alpha_2 \cdot \mathrm{CreTrust}(a) + \alpha_3 \\ & \cdot \mathrm{ITrust}(a) + \alpha_4 \cdot \mathrm{CTrust}(a) + \alpha_5 \\ & \cdot \mathrm{PartTrust}(a) + \alpha_6 \cdot \mathrm{TTrust}(a, b) + \alpha_7 \\ & \cdot \mathrm{FTrust}(a, b)\end{aligned} \tag{17}$$

where $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 = 1$, $(0 \leq \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 < 1)$.

C. TRUST EVALUATION OF BLOCKCHAIN

Based on the influence of service providers on FinTech behavior, the calculated task success score and the deviation score of each agent can be added to generate a total trust score. Then, consistent trust scores among all service providers are maintained by the capability of blockchain.

When the trust evaluation system starts, the distributed server generates a trust block for each FinTech business and saves its trust score. Obviously, the first block contains the relevant values of all FinTech businesses. Then, through a mathematical hash function, the updated total trust score is saved in the time stamped block and linked with the previous block. Therefore, each FinTech business will have an immutable blockchain. The total trust score of FinTech server u_j can be calculated by formulas (18), (19) and (20)

$$T_j = w_T \cdot p(T_j) + w_\delta \cdot \delta \tag{18}$$

$$p(T_j) = \sum_{i=1}^{n} p(T_j|D_i) \times p^t(D_i) \tag{19}$$

$$p^t(D_i) = (w_{(i,j)} + T_i^t)/2 \tag{20}$$

where w_T and w_δ is the weight, $w_T + w_\delta = 1$, $w_T + w_\delta \in [0, 1]$. D_i represents the ith server, $p(T_j)$ represents the current task success score of server u_j, δ is the adjustment factor, $p^t(D_i)$ represents the credibility score of server D_i at time t, T_i^t represents the trust score of server D_i at time t, and $w(i, j)$ represents the accuracy weight of server D_i on u_j. $p(T_j|D_i)$ represents the difference between the aggregate $p(T_j)$ and each service report, that is, the accuracy of the corresponding task at time t.

The total trust score of each FinTech servicer a is added to the blockchain, and the difference between the last trust score of each FinTech business and the current trust score is calculated to identify potential harmful service providers. Since all FinTech businesses have experienced similar environmental conditions, the difference between the previous

trust score and the existing trust score of all FinTech businesses should be within the same range regardless of wind or normal weather. However, when the scale of one of the FinTech businesses is different from that of another, then it may be attacked. Algorithm 1 represents the pseudo code of the trust management algorithm.

Algorithm 1 Distributed Trust Management

1 **Input**: Initial trust value, $T_i^t = 0$, $p^t(D_i) = 0$, $p(T_j|D_i) = 0$
2 **Output**: T_j
3 for $u_j, j = 1, \ldots, n$ do
4 for $d_i, i = 1, \ldots, N$ do
5 Calculate $DT_{ij}, IT_{ij}, RT_{ij}, FT_{ij}$
6 Calculate comprehensive trust T_{ij}
7 Calculate $p^t(D_i), p(T_j|D_i)$
8 Calculate $p(T_j) = \sum_{i=1}^{n} p(T_j|D_i) \times p^t(D_i)$
9 end for
10 Calculate $T_j = w_T \cdot p(T_j) + w_\delta \cdot \delta$ 11 end for
12 Update trust T_j

VI. EXPERIMENTAL STUDY

A. SIMULATION ENVIRONMENT SETTINGS

In order to verify the proposed multi-dimensional trust index system and evaluation mechanism (MDTEM) based on blockchain in FinTech, this paper uses Python as a programming tool to simulate the trust relationship structure between service providers, determine experimental parameters, and verify the evaluation mechanism and the capabilities of service providers. In the simulation experiment, the MDTEM mechanism proposed in this paper is compared with typical distributed reputation management system (DREAMS) [21] and graph theory based computational trust evaluation optimization model (TM-GT) [25].

The environment settings of the simulation experiment are: in the model, $U = \{1, \ldots, i, \ldots, u\}$ is used to represent the set of servers, and $S = \{1, \ldots, j, \ldots, s\}$ is used to represent the set of FinTech servers in the system. The simulation detection area is set to 10000 m × 10000 m square, with 1000 nodes randomly placed to simulate mobile service providers with limited resources. The trust rate of service providers is set to 80%. The time of each simulation is set to 600 seconds. Several simulation running with different parameter values are performed for each scenario, and then the average data of these simulation runs are selected. The free space propagation model is used in the simulation experiment. The settings of other simulation parameters are shown in Table 1.

B. TRUST EVALUATION PARAMETERS

In the trust evaluation mechanism based on blockchain, trust evaluation is carried out from three aspects: data sending, data transmission and data reception of FinTech business.

TABLE 1. Parameters and related values.

Parameter description	Value
Network dimensions	10000 m×10000m
Number of service providers	1000
Number of trusted servers	3
Time attenuation coefficient	1
Adjustment coefficient of normal interaction evaluation	0.8
Maximum allowed evaluation difference	0.6
Number of times paid by the service provider	10×10^3
Simulation run time	600s
Time window for trust calculation	5s
Trusted service rate	80%

C. PERFORMANCE ANALYSIS OF DIFFERENT TRUST VALUES

In order to analyze the relationship between trusted and untrusted service providers in the MDTEM, 1000 mobile FinTech service providers are set in the simulation experiment. The proportion of trusted service providers is set to 80%, the number of FinTech business payments changes from 1×10^3 to 10×10^3, and the payment requests of each service provider are carried out randomly.

Firstly, in order to verify the performance of MDTEM mechanism in different trust values, 1000 service providers with three different trust values are simulated in the experiment. The trust values can be set as 90%, 80% and 70%. The payment times vary from 1×10^3 times to 10×10^3 times, and the payment requests of each service provider are carried out randomly. The results of payment success rate under three different trust value states are shown in Figure 4. From the experimental results, the higher the trust value, the higher the success rate of payment. When the trust value decreases, the payment success rate decreases very quickly. It shows that the level of trust value will have a great impact on payment.

Second, the performance of multidimensional trust evaluation mechanism is compared with that of DREAMS and TM-GT when sending data. Figure 5 shows the comparison of sending data trust values of three trust mechanisms. It can be seen from Figure 5 that, the trust value of the sent data is increasing with the growing number of data sent by the service provider, but the trust evaluation index of the multidimensional trust evaluation mechanism is higher than that of DREAMS and TM-GT mechanisms. Because the MDTEM mechanism uses blockchain technology, it can better improve the trust of sending data.

Third, the MDTEM is compared with DREAMS and TM-GT in the case of data transmission. Figure 6 shows the comparison of transmission data trust values under three trust mechanisms. It can be seen from Figure 6 that the data trust value in the financial network is increasing with the continuous increase of the amount of data transmitted by the

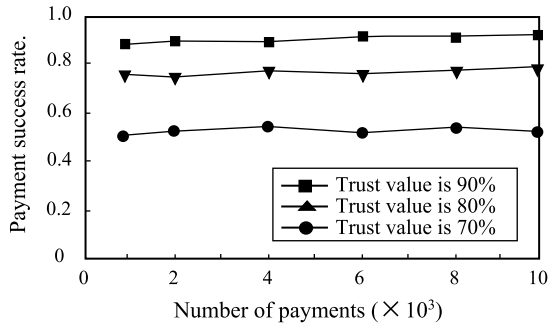


FIGURE 4. Comparison of payment success rate.

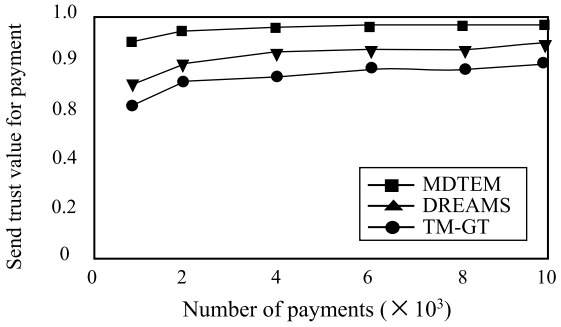


FIGURE 5. Send comparison of payment trust values.

financial network, but the multi-dimensional trust evaluation mechanism has higher trust evaluation than that of DREAMS and TM-GT mechanisms. Because the multi-dimensional trust evaluation mechanism uses blockchain technology to ensure the security of financial data in the transmission process. Therefore, the trust of the transmitted data is reliably improved.

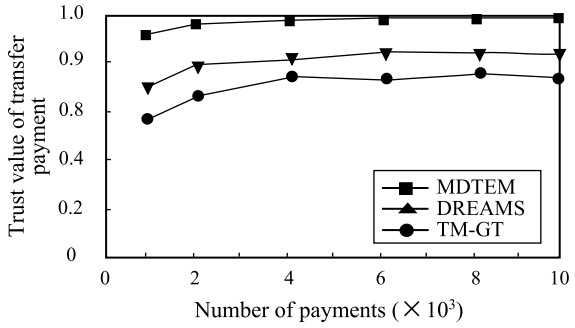


FIGURE 6. Comparison of transmission payment trust values.

Fourth, the performance of multi-dimensional trust evaluation mechanism is compared with that of DREAMS and TM-GT in the case of receiving data. Figure 7 shows the performance of received data trust values under three trust mechanisms. It can be seen from Figure 7 that, the data trust value in the financial network is increasing with the increasing amount of data received by the financial network, but the multi-dimensional trust evaluation mechanism has a higher trust evaluation than that of DREAMS and TM-GT mechanisms. Because the multi-dimensional trust evaluation mechanism uses blockchain technology, which improves the security and reliability of financial data in the process of data transmission, and ensures the trust of the received data.

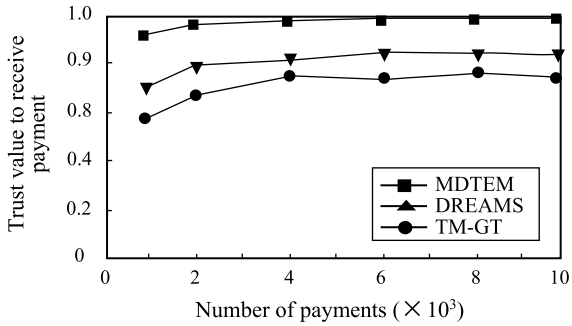


FIGURE 7. Comparison of received payment trust values.

Delivery success rate refers to the proportion of successful delivery times of FinTech in the total delivery times. It mainly reflects the ability of multidimensional trust evaluation mechanism to resist malicious behavior. A larger delivery success rate indicates that multidimensional trust mechanism has higher reliability. In order to verify the effectiveness of the multi-dimensional trust mechanism, the number of deliveries is changed from 1×10^3 to 10×10^3, and the proportion of malicious nodes is set to 20%. The performance of MDTEM is compared with DREAMS and TM-GT. The experimental results are shown in Figure 8. As can be seen from Figure 8, with the increase of delivery times, the delivery success rate is also increasing, but the increase speed slows down, and finally tends to a stable value. It also shows that MDTEM mechanism can better resist malicious nodes and improve the delivery success rate.

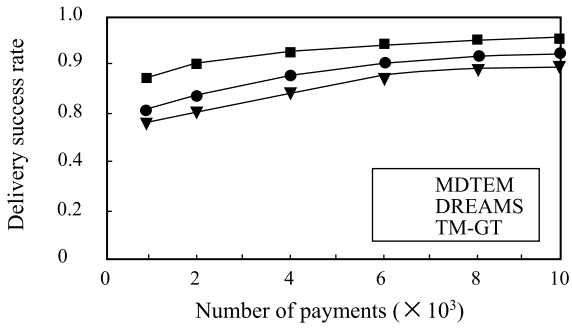


FIGURE 8. Comparison of delivery success rate.

VII. CONCLUSION AND FUTURE WORK

As the underlying support technology of FinTech, blockchain can improve the application of FinTech in a safe and verifiable way in a decentralized public environment. The development of FinTech trust evaluation mechanism has effectively promoted the integration of blockchain and FinTech.

This paper constructs the blockchain hierarchy of the FinTech ecological environment, designs the multi-dimensional trust index system and evaluation mechanism (MDTEM) based on the blockchain, and carries out the trust simulation experiment on the MDTEM mechanism from the three aspects of FinTech blockchain data sending, data transmission and data reception. Simulation results show that the proposed MDTEM trust mechanism can better improve the security and reliability of FinTech trust mechanism.

At present, this paper combines empirical data and simulation data to conduct an experimental study on the trust mechanism of data payment and data transmission in a small amount of FinTech. Processing explosion may occur in the situation of large-scale trust evaluation and processing, but this issue will be solved by different technologies in the future, such as using trust correction mechanism, trust timeliness, trust consistency mechanism and other methods to optimize trust evaluation. Future work will also consider the integration evaluation of blockchain, energy mechanism, and security attributes. In addition, simulation technology will be used to analyze the performance of the proposed evaluation mechanism, and thus to improve the reliability of the evaluation.

ACKNOWLEDGMENT

(Chaohao Sun is co-first author.)

REFERENCES

[1] P. Zhang and M. Zhou, "Security and trust in blockchains: Architecture, key technologies, and open issues," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 3, pp. 790–801, Jun. 2020.

[2] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Comput. Commun.*, vol. 169, pp. 179–202, Mar. 2021.

[3] X. Wu and J. Liang, "A blockchain-based trust management method for Internet of Things," *Pervas. Mobile Comput.*, vol. 72, Apr. 2021, Art. no. 101330.

[4] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020, doi: 10.1109/ACCESS.2020.2969820.

[5] D. D. H. Shin, "Blockchain: The emerging technology of digital trust," *Telematics Informat.*, vol. 45, Dec. 2019, Art. no. 101278.

[6] C. Chawla, "Trust in blockchains: Algorithmic and organizational," *J. Bus. Venturing Insights*, vol. 14, Nov. 2020, Art. no. e00203.

[7] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87643–87662, 2021, doi: 10.1109/ACCESS.2021.3068178.

[8] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021.

[9] G. Kumar, R. Saha, M. Rai, R. Thomas, and T. H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[10] W. Xiong and L. Xiong, "Data trading certification based on consortium blockchain and smart contracts," *IEEE Access*, vol. 9, pp. 3482–3496, 2021, doi: 10.1109/ACCESS.2020.3047398.

[11] D. Azzolini, F. Riguzzi, and E. Lamma, "Modeling smart contracts with probabilistic logic programming," in *Proc. Int. Conf. Bus. Inf. Syst.*, in Lecture Notes in Business Information Processing, vol. 394, 2020, pp. 86–98.

[12] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.

[13] H. Afzaal, M. Imran, M. U. Janjua, and S. P. Gochhayat, "Formal modeling and verification of a blockchain-based crowdsourcing consensus protocol," *IEEE Access*, vol. 10, pp. 8163–8183, 2022, doi: 10.1109/ACCESS.2022.3141982.

[14] C. Laneve, C. S. Coen, and A. Veschetti, "On the prediction of smart contracts' behaviours," in *From Software Engineering to Formal Methods and Tools, and Back* (Lecture notes in computer science), vol. 11865. Springer, 2019, pp. 397–415, doi: 10.1007/978-3-030-30985-5_23.

[15] N. Yadav and V. Sarasvathi, "Venturing crowdfunding using smart contracts in blockchain," in *Proc. 3rd Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Aug. 2020, pp. 192–197.

[16] M. Kowalski, Z. W. Y. Lee, and T. K. H. Chan, "Blockchain technology and trust relationships in trade finance," *Technol. Forecasting Social Change*, vol. 166, May 2021, Art. no. 120641.

[17] N. Javaid, "A secure and efficient trust model for wireless sensor IoTs using blockchain," *IEEE Access*, vol. 10, pp. 4568–4579, 2022, doi: 10.1109/ACCESS.2022.3140401.

[18] B. Routledge and A. Zetlin-Jones, "Currency Stability Using Blockchain Technology," *J. Econ. Dyn. Control*, May 2021, Art. no. 104155, doi: 10.1016/j.jedc.2021.104155.

[19] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees," *Technol. Forecasting Social Change*, vol. 158, Sep. 2020, Art. no. 120166.

[20] Z. Gao, W. Zhao, C. Xia, K. Xiao, Z. Mo, Q. Wang, and Y. Yang, "A credible and lightweight multidimensional trust evaluation mechanism for service-oriented IoT edge computing environment," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2019, pp. 156–164.

[21] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017, doi: 10.1109/ACCESS.2017.2769878.

[22] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

[23] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, and M. Xu, "A decentralized and trusted edge computing platform for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3910–3922, May 2020.

[24] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3538–3547, Jun. 2019.

[25] R. Du, K. Xu, and J. Tian, "Optimization scheme of trust model based on graph theory for edge computing," *Adv. Eng. Sci.*, vol. 52, no. 3, pp. 150–158, 2020.

[26] W. Feng, Z. Yan, L. T. Yang, and Q. Zheng, "Anonymous authentication on trust in blockchain-based mobile crowdsourcing," *IEEE Internet Things J.*, early access, Aug. 24, 2020, doi: 10.1109/JIOT.2020.3018878.

[27] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020.

[28] J. Kaur and S. Kaur, "Novel trust evaluation using NSGA-III based adaptive neuro-fuzzy inference system," *Cluster Comput.*, vol. 24, no. 3, pp. 1781–1792, Sep. 2021.

[29] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in VANETs," *J. Parallel Distrib. Comput.*, vol. 151, pp. 61–69, May 2021.

[30] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

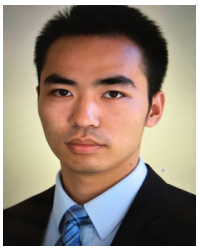
[31] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, "Decentralized blockchain-based trust management protocol for the Internet of Things," *IEEE Trans. Depend. Sec. Comput.*, vol. 19, no. 2, pp. 1292–1306, Apr. 2022, doi: 10.1109/TDSC.2020.3003232.

[32] A. Mousa, J. Bentahar, and O. Alam, "Multi-dimensional trust for context-aware services computing," *Expert Syst. Appl.*, vol. 172, Jun. 2021, Art. no. 114592.

[33] S.-W. Lee, S. Hussain, G. F. Issa, S. Abbas, T. M. Ghazal, T. Sohail, M. Ahmad, and M. A. Khan, "Multi-dimensional trust quantification by artificial agents through evidential fuzzy multi-criteria decision making," *IEEE Access*, vol. 9, pp. 159399–159412, 2021.

[34] R. J. Atwa, P. Flocchini, and A. Nayak, "RTEAM: Risk-based trust evaluation advanced model for VANETs," *IEEE Access*, vol. 9, pp. 117772–117783, 2021.
[35] I. Malakhov, A. Marin, S. Rossi, and D. Smuseva, "On the use of proof-of-work in permissioned blockchains: Security and fairnessa," *IEEE Access*, vol. 10, pp. 1305–1316, 2022, doi: 10.1109/ACCESS.2021.3138528.

YING SONG received the master's degree in geographical information systems and the Ph.D. degree in photogrammetry and remote sensing from Wuhan University, Wuhan, China, in 2004 and 2011, respectively. She is currently an Associate Professor with the School of Information and Engineering, Hubei University of Economics, Wuhan. She has published over 30 research papers. Her research interests include wireless communication, cloud computing, and financial technology.



CHAOHAO SUN received the master's degree in finance from the University of California at Riverside, Riverside, in 2016. His research interests include financial engineering and financial risk and evaluation. He has published over ten journals and conference papers in the above areas.

YUN PENG received the master's degree in economics and the Ph.D. degree in economics from Wuhan University, China, in 2003 and 2007, respectively. She is currently a Professor with the School of Finance, Hubei University of Economics, Wuhan, China. Her research interests include monetary theory and monetary policy. She has published over 30 journal articles and is an author of two books in the above areas.

YUE ZENG received the master's degree in vehicle operation engineering from the Wuhan University of Technology, China, in 2004, and the Ph.D. degree in computer science and technology from Xidian University, in 2011. He is currently a Professor with the School of Software Engineering, Jinling Institute of Technology, Nanjing, China. His research interest includes intelligent information processing. He has published over 40 journals and conference papers and is an author of four books in the above area. He is a Senior Member of CCF. He was awarded the Leader of Excellent Teaching Team of Province 'Qinglan' Project by the Jiangsu Provincial Department of Education, in 2018.

BAOLIN SUN received the master's degree in computer science and technology and the Ph.D. degree in computer science and technology from the Wuhan University of Technology, China, in 1999 and 2006, respectively. He is currently a Professor with the School of Information and Engineering, Hubei University of Economics, Wuhan, China. His research interests include multipath routing, parallel and distributed computing, networks optimization, and *ad-hoc* networks. He has published over 150 journals and conference papers and is an author of four books in the above areas. He is a member of IAENG, and one of the editorial board guest members of World Sci-Tech Research and Development, and also an International Standard Draft Organizing Member of ISO/IEC JTC1/SC6. He was awarded the Province Special Prize by the Hubei Province Government, in 2007.