IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 July 2023, accepted 29 July 2023, date of publication 2 August 2023, date of current version 11 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3301340

RESEARCH ARTICLE

Research on Blockchain-Based FinTech Trust Evaluation Mechanism

YING SONG[1,6], (Senior Member, IEEE), CHAOHAO SUN[2], LANXIN LI[3], FEIFEI WEI[4], YUEHENG LIU[5], AND BAOLIN SUN[1,6]

[1]School of Information Engineering, Hubei University of Economics, Wuhan 430205, China
[2]Department of Technical Business, China Huarong Financial Leasing Company Ltd., Hangzhou 310016, China
[3]School of Accounting, Hubei University of Economics, Wuhan 430205, China
[4]School of Information Management, Hubei University of Economics, Wuhan 430205, China
[5]Department of Secretary, Wuhan Cyber Security Association, Wuhan 430010, China
[6]Hubei Internet Finance Information Engineering Technology Research Center, Hubei University of Economics, Wuhan 430205, China

Corresponding authors: Feifei Wei (wff781224@hbue.edu.cn) and Baolin Sun (blsun@163.com)

This work was supported in part by the National Social Science Foundation of China under Grant 21BJY147, and in part by the Hubei Internet Finance Information Engineering Technology Research Center under Grant IFZX2202 and Grant IFZX2213.

ABSTRACT The financial technology (FinTech) has promoted the wide application of FinTech with the help of artificial intelligence, blockchain, cloud computing, data science and other new technologies. Trust evaluation has become a forward-looking issue for the rapid development of FinTech. The existing trust evaluation methods of FinTech do not consider the impact of the timeliness, reliability and non-invasive factors of trust on trust evaluation, which results in low accuracy of trust evaluation and incapability of effectively identifying malicious behaviors of users. Firstly, this paper introduces the blockchain technology to construct a four-layer architecture structure and multiple trust evaluation indicators based on blockchain service data. Secondly, the paper proposes a blockchain based FinTech trust evaluation mechanism (BFTEM), which utilizes blockchain to record relevant data and multiple trust parameters during the transmission process of each block, and verify the trust degree issued by the trust holder through the comprehensive trust value of the user. Finally, the block generation time, throughput, delayed response time and comprehensive trust value are experimentally studied through simulation experiments. Simulation experiments show that BFTEM mechanism can better improve the security and reliability of FinTech data, and has advantages in improving the accuracy of trust evaluation and expanding potential applications.

INDEX TERMS Fintech, blockchain, trust, trust evaluation.

I. INTRODUCTION

With the help of artificial intelligence, blockchain, cloud computing, data science and other new technologies, the financial technology (FinTech) promotes the innovation of the application architecture and paradigm of FinTech and expands the application field of the FinTech [1]. Since all users of the FinTech are interconnected, user authentication has become a key part of the security of the FinTech. A FinTech user security authentication system [2], which is extendable and adaptable to limited resources, is needed. The current user authentication solution requires a centralized trusted party for authentication, which will lead to a single point of failure.

Blockchain is a new application mode of computer technology such as distributed data storage, consensus mechanism, point-to-point transmission and encryption algorithm. With the characteristics of decentralization, tamper resistance and reliability, blockchain makes it possible for data processing, data security and data transmission in the FinTech with no need for reliance on a centralized third party to determine the authenticity and trust relationship of user information [1], [2]. Based on the distributed data storage and linked list structure, the blockchain is a string of data blocks (i.e. blocks) generated by using the public key cryptosystem. Each data block contains the relevant information about the processing of that

The associate editor coordinating the review of this manuscript and approving it for publication was Seifedine Kadry.

batch of data, used to verify the validity of its information and generate the next block.

Before the application of the FinTech, it is necessary to identify and eliminate untrusted users, so the trust evaluation of users becomes one of the important problems to be solved in the FinTech. In order to dynamically evaluate the trust degree of FinTech users, some trust management and evaluation mechanisms need to be designed [3]. The goal of these mechanisms is to track the historical trust records among users to detect malicious behavior attacks. Trust evaluation mechanisms are divided into two categories: centralized and distributed. (1) In a centralized trust evaluation mechanism, the central user needs to store and calculate by itself the trust values of the relevant users' processes. In order to accurately evaluate the trust value of the local user, the trust value of the user can also be evaluated through the indirect trust value of other users. It is obvious that this centralized trust evaluation suffers from a single point of failure and bottleneck. (2) In the distributed trust evaluation mechanism, the calculation of trust value of users is mainly restricted by two aspects. First, the user can easily tamper with the local trust value stored on it, which makes the trust evaluation process vulnerable to malicious acts of the user; Second, resource-constrained FinTech users do not have sufficient capacity to meet the maintenance and use of trust calculation and trust update. In the data transmission process of the FinTech, users based on the blockchain technology can be linked to the current block data through the hash value in the previous block. Using the public key system, the authenticity of the FinTech data information and blocks can be verified before they are added to the blockchain. Once the block is linked to the blockchain, it can be ensured that the transmission process between users is securely recorded and tamper resistant [4].

To sum up, the research on trust model and trust evaluation mechanism in the current FinTech environment has laid a good foundation for trust evaluation of FinTech users, but there are still shortcomings in the current trust evaluation:

1) Due to ignoring the influence of trust timeliness, reliability and non-intrusive factors on trust evaluation, the trust behavior of users cannot be better evaluated, thus reducing the accuracy of user trust evaluation.

2) Because the differences of trust characteristics of different users and the evaluation of the credibility of recommended users are ignored, the malicious behavior of users cannot be effectively identified.

3) The lack of effective suppression methods for malicious users reduces the effectiveness of trust evaluation methods.

Facing the above challenges, this paper proposes a Blockchain-based FinTech Trust Evaluation Mechanism (BFTEM). BFTEM mechanism introduces blockchain technology to realize distributed trust evaluation. With the support of the blockchain, the trust value of a user can be generated by using a hash function public key. The blockchain will record this process and serve as the trust evaluation for the FinTech data transmission. In summary, the main contributions of BFTEM mechanism are summarized as follows.

1) By introducing the blockchain technology and improving the public key generation algorithm of hash function, the security and integrity of FinTech data are effectively maintained, and the security risks of traditional centralized management data are avoided.

2) This paper proposes a blockchain based FinTech trust evaluation mechanism (BFTEM). In BFTEM, the blockchain is used to record the relevant data in the setting process of each block, which helps the FinTech user to verify the trust degree issued by the trust holder, so as to realize the reliable transmission of FinTech data.

The remainder of the paper is organised as follows. Section II discusses background and some of the related work; Section III introduces the blockchain-based trust evaluation architecture; Section IV defines the building a multi trust evaluation indicator model in FinTech; Section V focuses on establishing trust evaluation algorithms and theoretical analysis; In Section VI, the simulation experimental research on trust evaluation algorithms; Finally, section VII presents the conclusions and future work.

II. BACKGROUND AND RELATED WORK

A. THE CONCEPT OF TRUST IN THE FINTECH

In the FinTech, trust can be regarded as a dependency relationship between users [4], [5], [6]. Trust can be divided into three types. The first type is behavior based trust, that is, the expected behavior of users; the second type is computing based trust, that is, trust between computing users; the third type is technology-based trust, which is maintained by evaluating the trust between users [4], [5], [6]. With the rapid growth of the scale and complexity of the FinTech, the trust between the users of the FinTech has increasingly become the focus of attention. Boldrin et al. [6] put forward the overall one-time principle project (TOOP) architecture that relies on the concept of trusted information source. TOOP ensures the safe data transmission between data providers and data consumers. Blockchain technology can effectively solve security and trust issues in FinTech, and also achieve consensus on the state of distributed ledgers. Afzaal et al. [7] proposed a secure and trustworthy blockchain based crowdsourcing (STBC) consensus protocol to address trust issues. The STBC is an effective automatic technology based on formal methods, which is used to ensure the correctness of STBC consensus protocol. In order to ensure the trust between users, Zhang et al. [8] proposed a blockchain-based trusted network connection protocol (BTNC). This protocol realizes mutual user authentication, platform authentication and trusted network access through encryption between FinTech users, so as to ensure the reliable trust between FinTech users.

B. THE TRUST EVALUATION MECHANISM

Trust model is an important concept in public key cryptography, which usually refers to the model of finding and traversing trust paths used in the process to establish trust relationships and verify certificates [9]. Xu et al. [10]

proposed a dynamic multidimensional trust model for information service quality evaluation. The evaluation model aggregates service rating and user credit to evaluate service quality. Javaid [11] proposed a blockchain-based wireless sensor Internet of Things (WSIoTs) trust model. In the WSIoTs model, only after the server passes through identity verification, it can add new users in the FinTech, use the proof of authorization (PoA) and consensus mechanism to verify the FinTech data, as well as add trust to the blockchain.

Based on the trust definition and trust model in the interaction process, trust evaluation synthetically constitutes many basic elements of trust, and finally calculates the degree of trust that an entity should have. The trust evaluation mechanism can define users to carry out trust evaluation in related activities such as data collection, analysis and transmission in order to complete trust decisions. Trust evaluation can be used in FinTech security protocols, and can guide the establishment of new application system security mechanisms in combination with blockchain and other related research results. Li et al. [12] proposed a trust evaluation model based on blockchain in order to ensure the privacy and security of vehicles in the Internet of Vehicles. The model constrains and regulates the behavior of vehicles through trust evaluation mechanism, and uses blockchain to realize the data security of vehicles. Lee et al. [13] proposed a mechanism of evidence fuzzy multi criteria decision making (EFMCDM) based on multi-dimensional trust quantification scheme. EFMCDM mechanism quantifies trust evaluation in a collaborative environment. Trust perception comes from initialization trust behavior, which in turn affects subsequent trust perception.

C. THE APPLICATION OF BLOCKCHAIN IN FINTECH

Because blockchain has the characteristics of distributed ledger Technology (DLT), consensus mechanism and smart contract, it can well solve the trust and security problems between FinTech users. In the FinTech, blockchain technology is applied to more computing power devices (such as edge computing servers), and then connected to an existing blockchain network. This can improve the adaptability of the FinTech, and better solve the problem of single point of failure problem.

Ahmed et al. [14] proposed a decentralized authentication structure based on blockchain, which clusters FinTech users according to their computing power, energy reserve and location. Users in each cluster authenticate through the hierarchical structure of interconnected blockchain. At the same time, a consensus protocol based on identity encryption key signature is introduced to reduce processing load. Cui et al. [15] proposed a hybrid blockchain structure, which uses local blockchains to authenticate IoT users, and uses public blockchains to connect multiple user clusters. Liu et al. [16] proposed an access-control mechanism based on the capabilities of IoT users, which registers the identity (ID) of IoT users and is managed by smart contracts in the alliance blockchain. Agyekum et al. [17] proposed a data sharing method of IoT based on blockchain storage and management, which uses existing blockchain technology to store and share public key technology based on the identity encryption of IoT users and information centric. Li et al. [18] proposed a blockchain-based trust system to prevent malicious data transmission and storage in the IoT, and store the trust value in the blockchain. Li et al. [19] proposed a probabilistic verification scheme, which effectively reduces the propagation delay of data blocks and the occurrence of blockchain block bifurcation, and further enhances the security of data transmission, the resistance to dual overhead attacks, trust evaluation, etc. Ullah et al. [20] proposed a decentralized distributed storage and sharing scheme based on blockchain in the IoT, which provides end-to-end encryption and fine-grained access control, uses Diffie-Hellman key exchange protocol to share keys between data owners and users, and replaces proof of work (PoW) consensus mechanism with PoA, which improves the throughput of the system.

D. MECHANISMS FOR THE INTEGRATION OF BLOCKCHAIN AND TRUST

Blockchain records transactions as blocks and forms a linked list structure. Any user in the FinTech obtains a hash value for each newly generated block, connects the hash value with the previous block to the current block for forwarding, and forms an irreversible chain [21], [22], [23], [24], [25].

Zhou et al. [22] discussed that the main research fields of blockchain include basic technology architecture, privacy and security, IoT applications and FinTech scene applications, etc., especially in edge computing servers (ECS), cryptocurrency and blockchain technology based on application requirements. Yang et al. [23] analyzed that there are a large number of ECS distributed in the Internet. These ECS can provide reliable access, storage, computing tasks, etc. to the users in the Internet, which can integrate the blockchain into the ECS and reduce the processing delay of the terminal users on the blockchain. In order to improve the reliability and security of FinTech users, viriyasitavat et al. [24] proposed a service specification formulation method based on blockchain technology, and integrated the proposed service specification and blockchain technology into the service quality framework of service applications to support service selection and workflow composition. Barenji [25] proposed a blockchain based trust mechanism to solve the trust problem in cloud manufacturing, aiming at the trust relationship between cloud manufacturing suppliers and consumers. Li et al. [26] introduced the identity authentication scheme based on blockchain into the service evaluation model and proposed a new blockchain-based trusted service evaluation model (BCSE). In this BCSE, only users that successfully pass the authentication can submit trust evaluation information to the edge computing server, and the registration and authentication records of user identity and the review of the edge computing server are stored in the blockchain. The registration and authentication records of user identities and the review of edge computing servers are stored in the blockchain network. Aiming at the problems that the application source

TABLE 1. Summary of work related to blockchain based fintech trust mechanism.

Mechanism/ Algorithm	Trust mechanism	Blockchain mechanism	Mechanism/Algorithm Characteristics
LBTM [2]	Decentralized trust evaluation solution	Ethereum-based private blockchain	Lightweight blockchain-based trust management system (LBTM)
STBC [7]	Manage and evaluate trust attributes	Record user behavior information and updates in blockchain	Formally verified Secure and Trustworthy Blockchain-based Crowdsourcing (STBC) consensus protocol
WSIoT [11]	Building a blockchain based trust model	Proof of Authority (PoA) consensus algorithm	A Secure and Efficient Trust Model for Wireless Sensor IoTs using Blockchain (WSIoT)
EFMCDM [13]	Multi-dimensional trust quantification schemes	Record Trust Entropy	Design and comparative analysis of evidential fuzzy multi-criteria decision-making (EFMCDM)
BTS [18]	Deep reinforcement learning mechanism management and evaluate trust value	Record and report malicious data in blockchain to improve security	Blockchain-based trust system with assistant of drones to deter malicious data reporting in intelligent IoT
IoTChain [20]	Trusted third-party auditor (TPA)	Proof-of-work (PoW) consensus mechanism	Ground-breaking blockchain-based IoT information paradigm
BCSE [26]	Trusted service evaluation model	Blockchain-based identity authentication scheme	Blockchain-based trusted service evaluation model (BCSE)
STE [30]	Trust value of dynamic malicious devices	Semi-centralized blockchain	Semi-centralized trust management system architecture based on blockchain in both single and multiple domains
AAT [31]	Anonymous authentication and decentralized trust evaluation methods based on trust	Record user behavior in blockchain	An anonymous trust authentication scheme based on blockchain trusted trust evaluation

data of the IoT is easy to be tampered with and stolen, and information sharing lacks a credit guarantee mechanism, Jiao et al. [27] proposed a trusted upload scheme of IoT users based on blockchain. The scheme carries out trusted design from three dimensions: user hardware, transmission link and platform, and provides relevant references for similar designs.

In the application of FinTech, trust management is one of the forward-looking issues in establishing dynamic modeling, security prevention, and other characteristics of FinTech terminal devices. Pal et al. [28] proposed a blockchain based trust framework and implementation mechanism, which allows independent trust providers to implement different trust metrics in a distributed manner and based on a common set of trust evaluation mechanisms.

In the traceability scenario brought about by blockchain, most existing studies overlook the impact of peer evaluation on trust management. In terms of improving user trust evaluation and management, Wang et al. [29] proposed an intelligent trust evaluation mechanism based on ECS, which comprehensively evaluates the reliability of users by using probability graph model. The mechanism also evaluates the reliability and security of the user from the aspects of data acquisition, data processing and data transmission, and also reduces the energy consumption of the user. Liu et al. [30] discussed the challenges of computing, storage and communication faced by blockchain and trust evaluation system, and proposed a single domain and multi-domain semi-centralized trust evaluation (STE) system architecture based on blockchain. By aggregating direct and indirect trust information, the architecture carefully designed attenuation function, recommended reliability and adaptive weight to calculate the trust value of dynamic malicious devices. Research shows that the trust model is effective in identifying malicious users and mitigating the impact of malicious users. Feng et al. [31] proposed an anonymous authentication trust (AAT) scheme through trusted trust evaluation in blockchain based ECS, which better solves the conflict between trust evaluation and anonymity.

Although the trust evaluation algorithms mentioned above have effectively improved access control issues and trust cooperation among users in internet applications, IoT applications, and FinTech applications, there is relatively little research on ensuring a multi trust domain environment, dynamic and flexible access control mechanisms, and trustworthy trust evaluation processes in FinTech applications. In addition, FinTech users with limited resources do not have sufficient computing power to meet trust computing and trust maintenance processing. Compared with the above methods, the focus of this paper is to introduce blockchain technology and improve the public key system generation algorithm of hash function to ensure the security and integrity of data, achieve trust management and evaluation of Fintech through blockchain technology, and ensure the fairness and tamper resistance of trust evaluation of Fintech users. A summary of typical work related to blockchain based FinTech trust mechanisms is shown in Table 1.

III. BLOCKCHAIN-BASED TRUST EVALUATION ARCHITECTURE

The main components of the framework are various terminals of the FinTech, edge servers, trust computing servers and other related hardware devices. All kinds of users in the

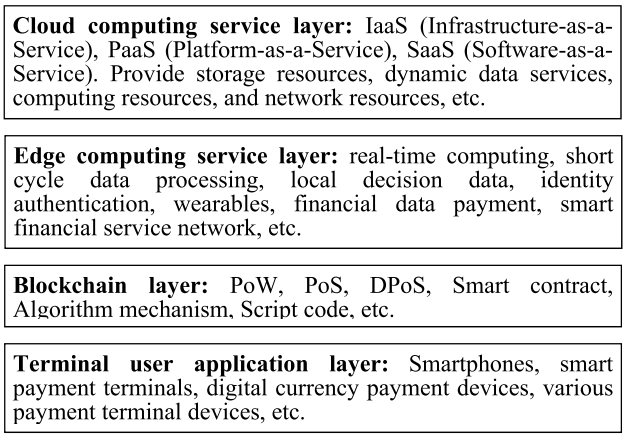

FIGURE 1. Four-layer architecture of service workflow based on blockchain.

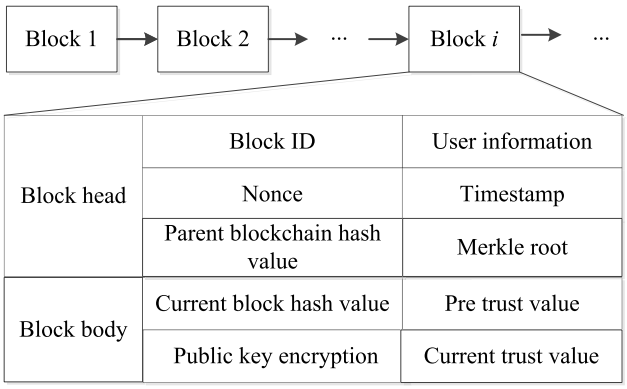

FIGURE 2. Data model of blockchain trust.

FinTech will work together to perform data transmission and processing, trust computing, collaborative services, etc.

A. BLOCKCHAIN-BASED STRUCTURE IN THE FINTech

FinTech users use blockchain applications for data transmission and processing, unload the computing tasks of blockchain applications through edge computing servers, and store blocks in edge computing servers. For example, the PoW and data transmission security of each FinTech user. The computing tasks of FinTech terminal users and intelligent users can be transferred to the edge computing server near the FinTech. Every link between FinTech terminal users and intelligent user computing units is protected by public key infrastructure. Therefore, the FinTech can be regarded as four-layer network model: cloud computing service layer, edge computing service layer, blockchain layer and terminal user application layer. Fig. 1 shows the four–layer architecture of blockchain based on service workflow in the FinTech.

Cloud computing service layer: the cloud computing service layer is the highest level of the entire FinTech service architecture, mainly providing standardized and standardized services. It supports seamless integration, data storage and data processing from terminal user layer to blockchain layer and edge computing server layer.

Edge computing service: the edge computing service layer is conducive for key generation and management, trust computing and updating.

Blockchain layer: the blockchain layer aims to build data blocks between terminal users and edge servers. It is a global distributed ledger, composed of blocks that encapsulate the number of transactions, including information about specific domains related to different management trust domains, trust calculation results of each user, etc. The blockchain layer adopts a data model based on data transmission and processing to achieve a consensus among all groups of blocks between various applications. The main functions of this layer are: consensus mechanism, transaction-based data model, P2P network, proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), proof of authorization (PoA), etc.

Terminal user application layer: the terminal user layer is composed of FinTech users for data generation, processing and transmission. It consists of multiple FinTech terminal users that provide specific application functions. The terminal users, as the interface for data collection and exchange, can be physical or virtual devices, such as FinTech devices, intelligent devices, hardware and software.

B. DATA MODEL BASED ON BLOCKCHAIN TRUST

Blockchain is a distributed database, which does not require third-party verification and central authority. After the integration of blockchain and trust, the distributed database converts all data of the FinTech into associated data and stores it in a block. This block is constructed within a certain period of time, and points to the previous data block with a hash pointer. All blocks form a complete single chain. Blockchain technology ensures the security and centralization of data in the transmission of the FinTech according to time sequence, asymmetric data block encryption algorithm, trust value update, etc. This block is mainly composed of block header and block body. The data model of blockchain trust is shown in Fig. 2.

The hash value is calculated and updated by the edge computing server of the FinTech and stored on the blockchain. The hash value on the blockchain is used to verify the authenticity and security of the FinTech users. SHA256 encryption operation is performed on each block header to generate a hash value, through which the corresponding block in the blockchain can be identified. Meanwhile, each block can reference the previous block (parent block) through the "Parent Block Hash Value" field in its block header.

C. CHARACTERISTICS OF HASH FUNCTION

In FinTech applications, hash functions are used to generate integrity codes for FinTech data generation, storage and transmission, and to authenticate the transaction users and their transaction data. After a main block is created by the FinTech user, an encrypted hash function can be used to link it to the

TABLE 2. Authentication information table of user.

Information Item Name
FinTech user ID
Edge computing server ID
Hash function authentication value of the block
Serial number of the block

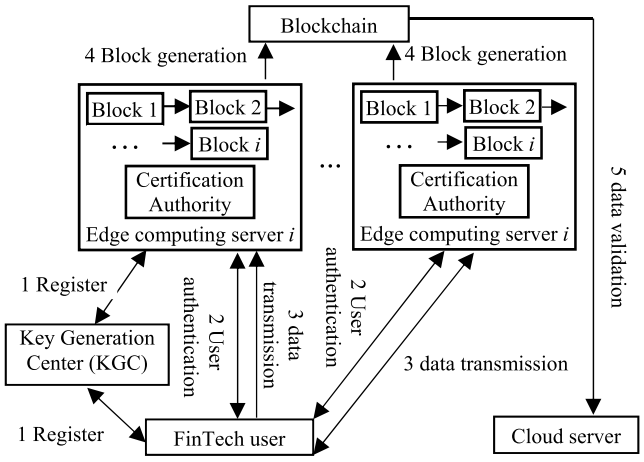

FIGURE 3. User security authentication process of BITEA algorithm.

next block. In the process of data transmission in the FinTech, hash function can be used to ensure its security [32]. The characteristics of hash function are:

1) Unidirectionality: Given an input message m, a hash value h is obtained through the hash function, which is expressed as h= hash(m). Otherwise, m cannot be deduced from h.

2) Uniqueness: For any given two input messages m_1 and m_2, if ($m_1 \neq m_2$), then hash(m_1) $\neq$ hash(m_2).

3) Anti-collision: For a given message m_1, another different message m_2 cannot be found, so that hash (m_1) = hash (m_2).

In addition, the execution speed of hash functions means the speed at which these function operations occur during processing [33]. There are more application scenarios for high quality hash functions.

D. SECURITY AUTHENTICATION PROCESS OF BFTEM MECHANISM

In the FinTech, users without identity signature are insecure and untrusted. Only after registration and identity signature can users join the application process of the FinTech to ensure the authenticity and security of users. Authentication information item of user in the BFTEM mechanism is shown in Table 2. Fig. 3 is the user security authentication process of the BFTEM, and Algorithm 1 is the joining mechanism of trusted users in the FinTech.

In trust user join algorithm (Algorithm 1), FinTech user i, Number of FinTech user n, Edge computing server (ECS), Cloud computing server (CCS), the FinTech certification center (CA), the public key (PK), the private key (SK).

Algorithm 1 Trust user join algorithm

1. **Input Parameters**: User i, user i's public key PK_i and private key SK_i;
2. User i sends identity signature to ECS, and ECS obtains the corresponding public key PK_i;
3. User i uses the private key SK_i to encrypt the data, and its related information is sent to ECS to calculate the related trust value;
4. ECS decrypts the information sent by user i through public key PK_i and uploads the corresponding information to the blockchain;
5. When FinTech user i enters another ECS, it shall be handled again according to step 2-4;
6. ECS uploads the corresponding blockchain to CCS.

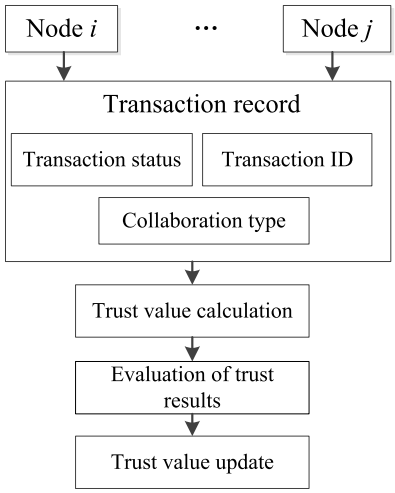

FIGURE 4. Trust model based on blockchain.

E. BLOCKCHAIN-BASED TRUST MODEL

The trust model based on blockchain mainly provides a general trust evaluation. In this model, each data transmission process of the user is transmitted to the trust calculation server, which evaluates the trust according to the trust index and obtains the corresponding trust value. Fig. 4 is a trust model based on blockchain.

IV. BUILDING A MULTI TRUST EVALUATION INDICATOR MODEL

A. SYSTEM MODEL

In the FinTech, the trust value of a user cannot be directly calculated from the user itself. It needs to be calculated by referring to the trust evaluation of other users in the FinTech, that is, the trust value of the user is obtained through data processing and transmission. In the process of data transmission, it is necessary to accurately judge the authenticity of the received message, so the concept of user trust is introduced.

Suppose the FinTech has n users, which can be expressed as N= {1, 2, …, i, …, n}. If user i believes that the behavior of user j brings good results, then user i trusts user j, and the

degree of trust can be measured by the degree of trust. In the trust evaluation of the FinTech, user i will evaluate the trust value of the behavior of neighbor user j before establishing the trust relationship.

Definition 1: trust is the expectation of the evaluation user on the service ability or cooperation probability of the target user. The quantitative expression of the prediction of the cooperation probability of the evaluation user on the target user is the trust value.

Definition 2: the direct trust value is the predicted value of the cooperation probability and service ability of the object with which the subject has direct interaction behavior in combination with historical direct interaction data. The direct trust value of user i to user j is denoted as t_{ij}.

Definition 3: the recommended trust degree is the prediction value of the service ability or cooperation probability of the target user by the subject according to the trust degree value transmitted by other users. The direct trust value of user i to user j is denoted as t_{ji}.

Definition 4: let $T = \{T_1, T_2 \ldots T_n\}$ denote the list of recommended trust degrees of users. Here, $T_i = \{t_{1i}, t_{2i} \ldots t_{mi}\}$ denotes the set of various recommended trust values obtained by user i through m times of data transmissions. Then the average recommended trust value is the recommended trust value of user i, which can be expressed as $r_i = (t_{1i} + t_{2i} + \ldots + t_{mj})/m$.

Definition 5: let $L = \{L_1, L_2 \ldots L_n\}$ denote the trusted computing degree list of the user, where $L_i = F_i(d_i, r_i)$ denotes the trusted computing degree of the data sent by the user i. d_i is the distance between user i and the edge computing server, and r_i represents the recommended trust value of user i.

B. TRUST VALUE OF USER HONESTY

The trust value $Th_{ij}(t)$ of the user honesty degree indicates the trust honesty degree between the user i and the user j, and can be calculated by the number of data transmission trust times jointly evaluated by two users. At time $t = 0$, users i and j do not interact. $Th_{ij}(t)$ changes with time. The positive interaction increases $Th_{ij}(t)$, while the negative interaction decreases $Th_{ij}(t)$. In this model, $Th_{ij}(t)$ can be calculated by equation (1).

$$Th_{ij}(t) = \begin{cases} \frac{|T_i \cap T_j|}{|T_i \cup T_j|}, & T_i \cap T_j \neq \emptyset \\ 0, & T_i \cap T_j = \emptyset \end{cases} \tag{1}$$

where, $|T_i \cap T_j|$ represents the total number of mutual data transmission trusts between user i and user j, $|T_i \cup T_j|$ represents the sum of the number of data transmission trusts between user i and user j.

C. TRUST VALUE OF USER AWARENESS

User awareness refers to the number of times of data transmission trust between user i and user j within a certain time t. If the degree of mutual knowledge of the users is higher in time t, the trust value of the degree of mutual knowledge is higher. In this trust factor, the user trust value $Ti_{ij}(t)$ based on the acquaintance relationship measures the degree of interaction experience according to the time t. It can be calculated by the number of data transmission trust between user i and user j and the maximum number of data transmission trust between user i and any adjacent user k in a period of time. $Ti_{ij}(t)$ can be calculated by formula (2)

$$Ti_{ij}(t) = \begin{cases} \frac{1}{\lg(10+|T_i \cap T_j|)}, & |T_i \cap T_j| \neq 0 \\ 0, & |T_i \cap T_j| = 0 \end{cases} \tag{2}$$

D. CALCULATION CAPABILITY OF USERS

Suppose that the total memory of the mobile user $i$is M_{ti}, M_{ri} is the remaining memory, E_{tj} represents the total energy, and E_{rj} represents the remaining energy. The credibility of the mobile user i is L_i and r_j is the credibility obtained by the mobile user j. m is the total number of mobile users whose reliability is successfully calculated by mobile user i. The trust calculation capability of the mobile user i is calculated by formula (3):

$$Tc_i(t) = \begin{cases} \alpha(\frac{M_{ri}}{M_{ti}} + \frac{E_{ri}}{E_{ti}}) + (1-\alpha)(\frac{\sum_{i=1}^{m}(\frac{rj}{Li} or \frac{Li}{rj})}{m}) \\ if \ r_j \leq L_i, \ \frac{r_j}{L_i} \ is \ used; \\ if \ r_j > L_i, \ \frac{L_i}{r_j} \ is \ used; \end{cases} \tag{3}$$

where, $Tc_i(t)$ is the trust computing capability of the mobile user i. The trust computing capability of a user is related to its available memory and energy. Adjustable parameters α ($0 \leq \alpha < 1$) is used to balance memory, energy and trust computing experience.

E. COMPREHENSIVE TRUST VALUE OF USERS

For the comprehensive trust evaluation of user i and user j, three trust value factors such as user honesty, user mutual knowledge and user computing ability are used in the data transmission trust evaluation process. User i evaluates the comprehensive trust value $T_{ij}(t)$ of user j at time t, then user i evaluates the comprehensive trust value of user j through the following formula (4):

$$T_{ij}(t) = \lambda_1 Th_{ij}(t) + \lambda_2 Ti_{ij}(t) + \lambda_3 Tc_i(t) \tag{4}$$

where $\lambda_1 + \lambda_2 + \lambda_3 = 1 (0 \leq \lambda_1, \lambda_2, \lambda_3 < 1)$.

V. ANALYSIS OF TRUST EVALUATION

A. TRUST VALUE EVALUATION ALGORITHM

In the process of FinTech data transmission, it is necessary to detect malicious acts in the data transmission process in real time, calculate the trust value of related users, update the trust value of users, and provide trust evaluation to other users. Algorithm 2 is a trust evaluation mechanism in the process of real-time data transmission of users.

B. BLOCKCHAIN TRUST UPDATE

Due to the limited memory and computing capacity of FinTech users, the data participating in trust calculation in the BFTEM mechanism is only stored in the edge computing

Algorithm 2 Trust evaluation algorithm

1. **Input Parameters**: $(i, j, M_{ti}, E_{ti}, E_{ri})$
2. **Output**: $T_{ij}(t)$
3. For $(i = 0; i \leq n; i++)$
4. For $(j = 0; j \leq n\text{-}1; j++)$
5. Calculate $Th_{ij}(t)$, $Ti_{ij}(t)$
6. End For
7. End For
8. For $(i = 0; i \leq n; i++)$
9. If $(r_j \leq L_i)$
10. Calculate r_j/L_i
11. Else
12. Calculate L_i/r_j
13. Calculate $Tc_i(t) = \alpha(\frac{M_{ri}}{M_{ti}} + \frac{E_{ri}}{E_{ti}}) + (1-\alpha)(\frac{\sum_{i=1}^{m}(\frac{rj}{Li} or \frac{Li}{rj})}{m})$
14. End For
15. For $(i = 0; i \leq n; i++)$
16. For $(j = 0; j \leq n\text{-}1; j++)$
17. Calculate $T_{ij}(t) = \lambda_1 Th_{ij}(t) + \lambda_2 Ti_{ij}(t) + \lambda_3 Tc_i(t)$
18. End For
19. End For

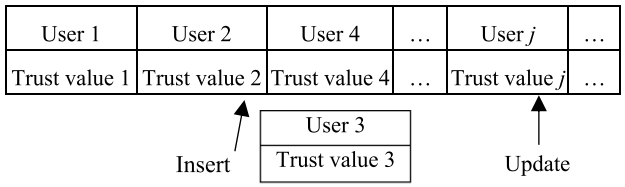

FIGURE 5. User trust update data structure based on blockchain.

Algorithm 3 User trust value update algorithm

1. **Input Parameters**: $(i, j, T_j, L_j, T_{ij}(t))$
2. For $(i = 0; i \leq n; i++)$
3. If $(T_j \notin T)$
4. Add T_j, L_j, $T_{ij}(t)$ to T
5. Else
6. Update T_j, L_j, $T_{ij}(t)$
7. Output: T, L
8. End For

server in each trust management domain. The trust record contains the service time of each user, user ID, trust value, list of direct interaction users and other related data. Fig. 5 is a block chain based user trust update data structure.

In the FinTech, the trust value of users' needs to be updated after evaluation and calculation. Algorithm 3 is the user trust value update mechanism.

C. INFORMATION ENTROPY ANALYSIS OF BLOCKCHAIN TRUST

According to the data model based on the blockchain, the trust value is calculated and stored in the current blockchain after each data transmission. In this way, the trust value can be predicted and analyzed by the quantitative prediction method, so as to predict the trust trend of the user.

In the BFTEM trust evaluation mechanism, the probability of the next block can be constructed based on the hash function of trust in the blockchain. In information theory, information entropy is a measure of uncertainty of random variables. X *is* a discrete random variable with finite value, and its probability distribution is:

$$P(X = x_i) = p_i, \quad i = 1, 2, \ldots, n \tag{5}$$

Then the information entropy of the random variable X can be defined as:

$$H(X) = -\sum_{i=1}^{n} p_i \log p_i \tag{6}$$

When the value of $H(X)$ is smaller, it indicates that the trust value of the user is more stable after the data transmission of the FinTech, and the trust trend is more stable.

D. COMPLEXITY ANALYSIS OF BFTEM MECHANISM

In the BFTEM trust evaluation mechanism, for each FinTech data processing process, the complexity of the BFTEM trust evaluation is equal to $O(n^2)$. This complexity is reasonable when powerful FinTech service providers, cloud computing servers and many terminals are involved. For storage complexity, it can be calculated by replacing the storage space of old block data with the hash operation in the latest block when maintaining the recommended trust value.

VI. EXPERIMENTAL EVALUATION

A. SETTING OF SIMULATION EXPERIMENT ENVIRONMENT

In the simulation experiment, Python software is used to evaluate the performance of the blockchain in the FinTech, because it has become a popular simulator for analyzing mobile networks and mobile payments.

Data source: In experimental analysis, some of the data comes from banking institutions and FinTech companies, while the other part is generated by computer simulators.

Simulation experiment environment: simulation experiment unit is equipped with 10 ECS and 200 FinTech users. FinTech user is freely distributed within a 10km×10km area for data processing and transmission. Their user trust rates are 70%, 80%, and 90%, respectively. The average running time of each simulation experiment can be set to 600 seconds, generating 200 FinTech transfer transactions per second. Execute multiple simulation runs with different parameter values for each scenario, and then select the average data of these simulation runs. Using normal random variables, the payment arrival time of each FinTech user follows the Poisson distribution. The relevant parameters are shown in Table 3.

In the BFTEM trust evaluation simulation experiment, the number of data transmission changes from 1×10^3 to 10×10^3. The verification time in the data transmission process of the FinTech will be determined according to the time required to calculate the recommended value based on the trust value

TABLE 3. Simulation experiment parameters.

Parameters Name	Parameters
Experimental Scope	10km×10km
Number of Fintech Users	200
Number of ECS	10
Transmission Radius of Fintech User	500m
Number of Fintech Transactions Generated Per Second	100/s
Simulation Time	600s
Trusted Service Values	80%
Maximum Number of Attacks	1000
Comparative Trust Mechanism	STBC [7], EFMCDM [13]

stored in the blockchain. The time for validation and request operations increases linearly with the number of transactions and queries, respectively.

In the trust evaluation mechanism, different trust can be applied to multiple trust evaluations in the same FinTech data processing, and the specification of each trust evaluation can be formulated by considering the trust requirements associated with one FinTech data processing.

B. PARAMETER DESCRIPTION OF SIMULATION EXPERIMENT

(1) Block generation time: the block generation time is the average generation time of a single block. In the simulation experiment, the workload is configured by adjusting the task generation frequency of each user, and then the block generation time is monitored.

(2) Trust rate: In FinTech, trust rate refers to the ratio of the number of users who meet the trust requirements to the total number of users.

(3) Throughput: throughput refers to the maximum number of messages

(4) Delay: delay refers to the response time of each transaction. The transaction processing time can be confirmed according to different task generation frequencies.

(5) Comprehensive trust value: the accuracy of the comprehensive trust value measures the ability to trust trusted behaviors that evaluate the security of the application process and the payment success rate.

C. ANALYSIS OF SIMULATION EXPERIMENT RESULTS

In the simulation experiment, a blockchain based FinTech trust evaluation mechanism (BFTEM) is compared with the secure and trustworthy blockchain based crowdsourcing (STBC) [7] and the evidence fuzzy multi criteria decision making (EFMCDM) [13].

The block generation time is mainly used to evaluate the average generation time of a single block generated by the BFTEM. In the BFTEM, the generation time of blocks is mainly tested through different trust rates. In the experiment, the initial trust values of FinTech users can be set to 70%, 80% and 90% respectively, and the number of FinTech users

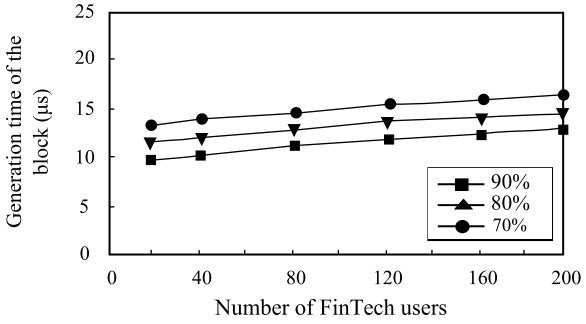

FIGURE 6. Generation time of blocks under three different trust values.

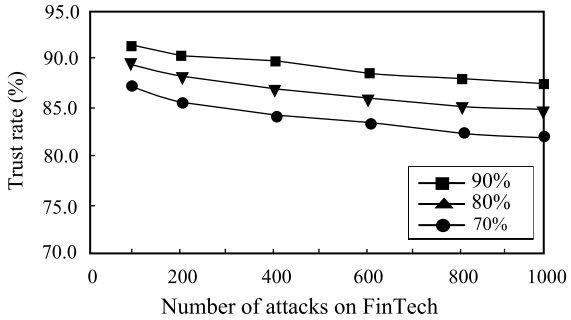

FIGURE 7. Comparison of trust rates under three different initial trust values.

gradually increases from 20 to 200. The experimental results are shown in Fig. 6. It can be seen from the results in Fig. 6 that when the trust degree increases, the generation time of the block is relatively reduced. As the number of FinTech users' increases, the generation time of blocks increases accordingly.

Decentralized testing is mainly used to evaluate the trust reliability of the BFTEM mechanism. In BFTEM, decentralized testing can be conducted by setting different trust rates. In the experiment, the initial trust values of FinTech users can still be set at 70%, 80%, and 90%, respectively. The number of FinTech attacks gradually increased from 100 to 1000, and the experimental results are shown in Fig. 7. From the results in Fig. 7, it can be seen that as the number of attacks increases, the trust value decreases. However, when the initial trust rate is high, the attacks received are relatively slow, indicating that a high initial trust rate has a good guarantee effect on trust security.

In the current research on trust evaluation of FinTech based on blockchain, most methods are to add trust information of FinTech users to the block. This may make trust information and evaluation more memorable and tampering. In the BFTEM mechanism, security authentication mechanisms such as identity signature are used to reduce the risk of trust information and ensure the security of trust information and updates. It can be seen in Fig. 8 that the memory of the block in the BFTEM mechanism is much smaller than that of the traditional block. It can be concluded that BFTEM mechanism has better memory scalability.

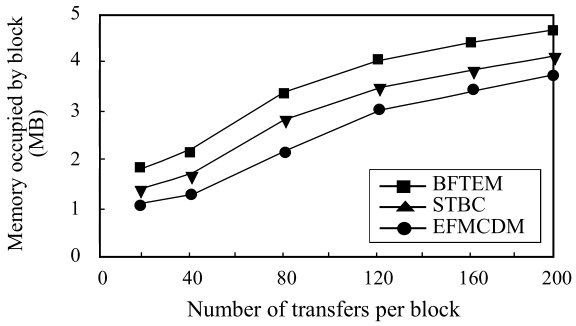

FIGURE 8. Comparison of block memory occupied by three trust algorithms.

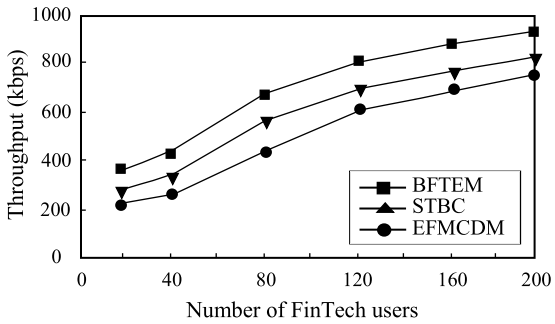

FIGURE 9. Comparison of data throughput by three trust algorithms.

Throughput is a measure of the amount of FinTech data that can be processed by the FinTech in a unit time. Fig. 9 depicts that the throughput of the FinTech gradually increases with the rise of the amount of FinTech data. At first, the throughput of the FinTech was low, and its FinTech users were relatively small. With the increase of the number of FinTech users, the heat of data processing went up, and the security of the network was strengthened. The amount of data sent and received between the FinTech users also increased, and the throughput of the FinTech also lifted. It can be seen from the data throughput in Fig. 9 that the throughput of BFTEM mechanism is higher than that of STBC and EFMCDM mechanisms, mainly because BFTEM uses the blockchain technology to improve the security and reliability of trust.

The improvement of the comprehensive trust value can improve the security and transmission success rate of the FinTech data processing process, and can also reflect the ability of the blockchain trust evaluation mechanism to resist untrustworthy behaviors. In the simulation experiment, the ratio of the initial trust degree of the FinTech user can be set to 80%, the number of FinTech data transmission changes from 1×10^3 times to 10×10^3 times, and the data processing of each server is random. In this environment, BFTEM trust evaluation mechanism is compared with STBC, EFMCDM and other trust evaluation mechanisms. Fig. 10 shows the comparison of the comprehensive trust values of the three trust mechanisms. From the experimental results in Fig. 10, it can be seen that with the continuous increase of data

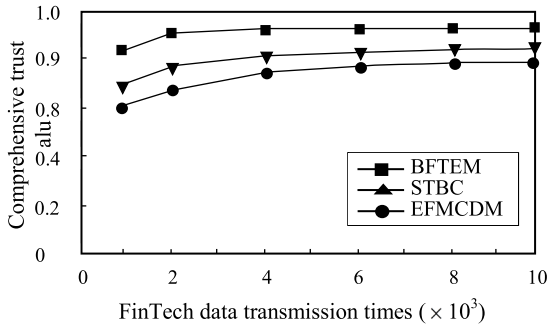

FIGURE 10. Comparison of comprehensive trust value of three trust algorithms.

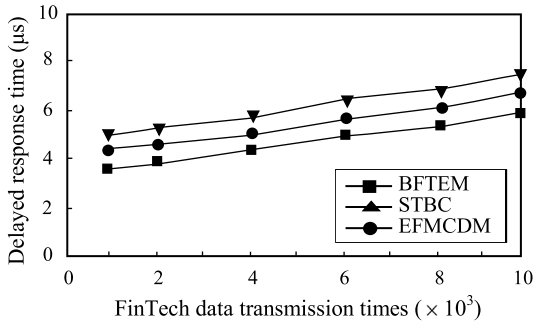

FIGURE 11. Comparison of delay response time t by three trust algorithms.

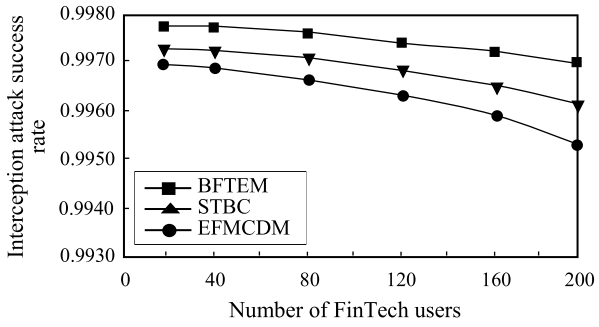

FIGURE 12. Comparison of interception attack success rate of three trust algorithms.

transmission times of the service providers, the comprehensive trust value is also rising, which also shows that the BFTEM mechanism can better improve the trust level.

The delayed response time refers to the average response time of each FinTech data block, which is mainly used to confirm the generation and processing of data blocks by each user. Fig. 11 shows the average delay response time of three trust evaluation mechanisms. As shown in Fig. 11 with the increase of the data volume of the FinTech, the delay response time of the BFTEM mechanism is also growing. The delay response time of the BFTEM mechanism is lower than that of the STBC and EFMCDM mechanisms. The main reason is that BFTEM uses the blockchain technology, which reduces the trust safety response time and improves the reliability of the users.

Security is the most important parameter in the application of FinTech. In the simulation experiment, the security attack is also studied. In the experiment, the number of users of the FinTech gradually increases from 20 to 200. The comparison of the probability of successful interception of attacks by the three mechanisms is shown in Fig. 12. It illustrates that the success rate of blocking attacks of BFTEM mechanism is higher than that of STBC and EFMCDM mechanisms, which indicates that the trust of BFTEM mechanism is better integrated with the blockchain technology, and its framework is more secure.

VII. CONCLUSION

Artificial intelligence, blockchain, cloud computing, data science and other new technologies have promoted the wide application of the FinTech (FinTech) technology. Blockchain has ensured the safe and reliable operation of the FinTech system. Trust, as a subjective and fuzzy evaluation standard, can evaluate the security and reliability of the data transmission and processing of the FinTech. By introducing blockchain and public key generation algorithm with improved hash function, this paper constructs a four-tier architecture and multitrust evaluation index model based on blockchain service data flow, maintains the security and integrity of FinTech data, and avoids the security risk of traditional centralized management data. On this basis, a blockchain-based FinTech trust evaluation mechanism (BFTEM) is proposed.

In the BFTEM mechanism, the blockchain is used to record the relevant data in the setting process of each block, which helps the FinTech users to verify the trust degree issued and quickly identify malicious users by the trust holders. In this way, the user can safely and reliably realize the data transmission of the FinTech. The simulation results show that BFTEM mechanism reduces the cost of trust identification of FinTech users, improves the security and reliable application of FinTech trust mechanism, and has advantages in improving trust calculation accuracy and potential applications.

With the development of FinTech research, its application scenarios will become more ecological. In the future, we will explore the application of dual blockchain architecture, reconstructed blockchain architecture, multidimensional transformation hash function and other technologies in various scenarios of the FinTech to improve its application quality.

REFERENCES

[1] R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A survey on blockchain for industrial Internet of Things," *Alexandria Eng. J.*, vol. 61, no. 8, pp. 6001–6022, Aug. 2022.

[2] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "LBTM: A lightweight blockchain-based trust management system for social Internet of Things," *J. Supercomput.*, vol. 78, no. 6, pp. 8302–8320, Apr. 2022.

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

[4] M. Becker and B. Bodó, "Trust in blockchain-based systems," *Internet Policy Rev.*, vol. 10, no. 2, p. e1555, Apr. 2021.

[5] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for Internet of Vehicles," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1397–1409, Jul. 2021.

[6] L. Boldrin, G. P. Sellitto, and J. Tepandi, "TOOP trust architecture," in *The Once-Only Principle* (Lecture Notes in Computer Science), vol. 12621. Springer, 2021, pp. 126–140.

[7] 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.

[8] J. Zhang, Z. Wang, L. Shang, D. Lu, and J. Ma, "BTNC: A blockchain based trusted network connection protocol in IoT," *J. Parallel Distrib. Comput.*, vol. 143, pp. 1–16, Sep. 2020.

[9] P. S. Challagidad and M. N. Birje, "Multi-dimensional dynamic trust evaluation scheme for cloud environment," *Comput. Secur.*, vol. 91, Apr. 2020, Art. no. 101722.

[10] Z. Xu, X. Li, W. Xiong, Q. Lin, and J. Mao, "A dynamic multi-dimension trust model for information service quality evaluation," *Proc. Comput. Sci.*, vol. 187, pp. 601–606, Jan. 2021.

[11] N. Javaid, "A secure and efficient trust model for wireless sensor IoTs using blockchain," *IEEE Access*, vol. 10, pp. 4568–4579, 2022.

[12] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021.

[13] 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.

[14] M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," *Egyptian Informat. J.*, vol. 23, no. 2, pp. 345–361, Jul. 2022.

[15] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Mar. 2020.

[16] Y. Liu, Q. Lu, S. Chen, Q. Qu, H. O'Connor, K.-K. R. Choo, and H. Zhang, "Capability-based IoT access control using blockchain," *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 463–469, Nov. 2021.

[17] K. O. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the Internet of Things based on blockchain," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1685–1696, Mar. 2022.

[18] T. Li, W. Liu, A. Liu, M. Dong, K. Ota, N. N. Xiong, and Q. Li, "BTS: A blockchain-based trust system to deter malicious data reporting in intelligent Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22327–22342, Nov. 2022.

[19] M. Li, Y. Qin, B. Liu, and X. Chu, "Enhancing the efficiency and scalability of blockchain through probabilistic verification and clustering," *Inf. Process. Manag.*, vol. 58, no. 5, Sep. 2021, Art. no. 102650.

[20] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment," *IEEE Access*, vol. 10, pp. 36978–36994, 2022.

[21] G. Kumar, R. Saha, M. K. 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.

[22] L. Zhou, L. Zhang, Y. Zhao, R. Zheng, and K. Song, "A scientometric review of blockchain research," *Inf. Syst. e-Bus. Manag.*, vol. 19, no. 3, pp. 757–787, Sep. 2021.

[23] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[24] W. Viriyasitavat, L. D. Xu, and Z. Bi, "Specification patterns of service-based applications using blockchain technology," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 4, pp. 886–896, Aug. 2020.

[25] R. V. Barenji, "A blockchain technology based trust system for cloud manufacturing," *J. Intell. Manuf.*, vol. 33, no. 5, pp. 1451–1465, Jun. 2022.

[26] F. Li, X. Yu, R. Ge, Y. Wang, Y. Cui, and H. Zhou, "BCSE: Blockchain-based trusted service evaluation model over big data," *Big Data Mining Anal.*, vol. 5, no. 1, pp. 1–14, Mar. 2022.

[27] Y. Jiao and C. Wang, "A blockchain-based trusted upload scheme for the Internet of Things nodes," *Int. J. Crowd Sci.*, vol. 6, no. 2, pp. 92–97, Jun. 2022.

[28] S. Pal, A. Hill, T. Rabehaja, and M. Hitchens, "A blockchain-based trust management framework with verifiable interactions," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108506.
[29] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2054–2062, Mar. 2020.
[30] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in IoT system," *IEEE Trans. Services Comput.*, vol. 16, no. 2, pp. 858–871, Mar. 2023.
[31] W. Feng, Z. Yan, L. T. Yang, and Q. Zheng, "Anonymous authentication on trust in blockchain-based mobile crowdsourcing," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14185–14202, Aug. 2022.
[32] H. Krawczyk and T. Rabin, "Chameleon hashing and signatures," U.S. Patent 09/021 880, 19 980 211, Feb. 11, 1998.
[33] O. Belej, K. Staniec, and T. Więckowski, "The need to use a hash function to build a crypto algorithm for blockchain," in *Proc. DepCoS-RELCOMEX*, vol. 1173, 2020, pp. 51–60.

YING SONG (Senior Member, IEEE) received the master's degree in geographical information system and the Ph.D. degree in photogrammetry and remote sensing from Wuhan University, Wuhan, China, in2004 and 2011, respectively. She is currently a Professor with the School of Information Engineering, Hubei University of Economics, Wuhan. Her research interests include wireless communication, mobile edge computing, network protocol and blockchain technology, and financial technology. She has published more than 30 research papers and the author of two books in the above areas.

CHAOHAO SUN received the M.S. degree from the University of California Riverside, USA, in 2016. He is currently an Economist of financial with China Huarong Financial Leasing Company Ltd., China. His research interests include financial network technology and financial data transmission.

LANXIN LI received the B.S. degree in economics from the Huaxia Institute of Technology, China, in 2022. She is currently pursuing the M.S. degree in economics with the Hubei University of Economics, China. Her research interest includes risk management.

FEIFEI WEI received the Ph.D. degree in management science and engineering from the Huazhong University of Science and Technology, China, in 2013. She is currently an Associate Professor with the School of Information Management, Hubei University of Economics, Wuhan, China. Her research interests include information management systems, trust evaluation, and economics commerce. She has published more than 30 journals and conference papers and the author of a book in the above areas.

YUEHENG LIU received the M.E. degree. He is currently a Secretary General of the Wuhan Cyber Security Association. He is a second level Technician. He also serves as the Deputy Secretary General of the Wuhan Internet Industry Federation. He is a Senior Member of the China Computer Society and a member of the Computer Security Professional Committee. His research interests include information security technology and financial network security technology.

BAOLIN SUN received the master's and Ph.D. degrees 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, network optimization, and ad hoc networks. He has published more than 150 journal and conference papers and the author of four books in the above areas. He is an IAENG member and one of the Editorial Board Guest Members of the World Sci-Tech Research and Development, and an International Standard Draft organizing members of ISO/IEC JTC1/SC6. He was awarded the Province Special Prize by the Hubei Province Government, in 2007.