Copyright ⓒ 2023 KSII

Reliable blockchain-based ring signature protocol for online financial transactions

Jinqi Su[1], Lin He[1], Runtao Ren[2,3*], and Qilei Liu[1]
[1] School of Economics and Management, Xi'an University of Posts and Telecommunications
Xi'an 710061, China
[2] School of Modern Post, Xi'an University of Posts and Telecommunications
Xi'an 710061, China
[3] Department of Information Systems, City University of Hong Kong
Hong Kong
[e-mail: runtaoren@gmail.com]
[*]Corresponding author: Runtao Ren

Received April 2, 2023; revised July 9, 2023; accepted July 31, 2023; published August 31, 2023

Abstract

The rise of Industry 5.0 has led to a smarter and more digital way of doing business, but with it comes the issue of user privacy and security. Only when privacy and security issues are addressed, will users be able to transact online with greater peace of mind. Thus, to address the security and privacy problems associated with industry blockchain technology, we propose a privacy protection scheme for online financial transactions based on verifiable ring signatures and blockchain by comparing and combining the unconditional anonymity provided by ring signatures with the high integrity provided by blockchain technology. Firstly, we present an algorithm for verifying ring signature based on distributed key generation, which can ensure the integrity of transaction data. Secondly, by using the block chain technique, we choose the proxy node to send the plaintext message into the block chain, and guarantee the security of the asset transaction. On this basis, the designed scheme is subjected to a security analysis to verify that it is completely anonymous, verifiable and unerasable. The protection of user privacy can be achieved while enabling online transactions. Finally, it is shown that the proposed method is more effective and practical than other similar solutions in performance assessment and simulation. It is proved that the scheme is a safe and efficient online financial transaction ring signature scheme.

Keywords: Blockchain, Ring Signature, Privacy & Security, Industry 5.0, Financial Transaction

http://doi.org/10.3837/tiis.2023.08.007 **ISSN : 1976-7277**

1. Introduction

The rapid rise of blockchain technology is due to the growing maturity of Internet information technology in the era of Industry 5.0. Blockchain technology and cryptography are playing a key role in the design and deployment of all kinds of financial transactions [1]. Now from 4.0 to 5.0 industry due to its adaptability, efficiency and responsiveness [2]. Industrial blockchain can play an important role at the infrastructure level of trusted data collection, cloud storage and integration of industrial platform services, as well as at the application level where it can enable the transfer of value in online transactions of financial assets. Essentially, the blockchain is a decentralized, secure ledger that links devices, systems, plants and regions through a hierarchical chain structure, particularly for data decision-making [3]. It can be combined with industrial networks to provide responsibility and trade and has a wide range of applications [4]. Currently, the existing asset trading technology is centralized, where data and information are stored in a centralized database, and the transaction process is completed by a "trusted" third party institution [5]. On the one hand, the failure of a centralized institution can bring the entire trading system to a standstill and also bring about a massive leakage of personal information, making it difficult to guarantee the security of the system [6]. On the other hand, compared with cash transactions, financial asset transactions have special data characteristics, and the imitation of data products is indistinguishable [7]. Registration data and transaction data are stored in a centralized database, which makes it easy to forge once the database is attacked, leaving the security of financial consumers and financial institutions unprotected in Internet financial transactions [8]. Therefore, the creation of a secure and secure environment for asset trading is of particular importance [9].

The rapid growth of blockchain applications is due to its advanced features of immutability, transparency, distribution, traceability, security and reliability [10]. Nakamoto first proposed blockchain technology in 2008 and designed a cryptocurrency scheme based on blockchain technology to achieve secure transfers between two parties, opening up a new field of vision to solve the information security problems of third-party institutions [11]. Using blockchain to store data has the advantages of being secure, trustworthy, non-repudiation and tamper-proof, allowing consensus and data sharing between untrusted nodes, as well as decentralisation and storing information in a peer-to-peer (P2P) network by automatically recording information in code [12]. Blockchain is important not only because it changes the process of online transactions, but also because of its ability to achieve consistency by storing data in a de-trusted environment. Using the signature principle of public key cryptography, people around the world can securely transfer different types of digital assets peer-to-peer over the internet[13].

However, current blockchain-based transaction mechanisms are constantly changing, making them still highly vulnerable to a wide range of cyber threats. Ring signatures are an important method for ensuring blockchain security. This method is a promising class of group signatures, characterized by the ability to achieve arbitrary anonymity for the signer, and the ability for the verifier to validate the signature without others being able to determine the authenticity of the signature by the result of that signature. With the development of ring signature technology, ring signature technology has received extensive attention from scholars at home and abroad. Furthermore, ring signatures can be divided into threshold ring signatures, verifiable ring signatures and identity-based ring signatures. The verifiable ring signature enables the identity of the messenger to be verifiable. The receiver can verify and trace the identity information of the message sender after receiving the message, achieving a higher level of trust. Therefore, in this paper, we propose a verifiable ring signature scheme for

privacy and security protection when users pass information in online transactions.

1.1 Our Contribution

In the paper, we propose a blockchain-based ring signature protocol for online financial transactions, with the aim of adding a ring signature algorithm to the process of blockchain-based online financial transactions to anonymize and protect transaction data by leveraging the unconditional anonymity of ring signature technology. Unlike traditional transactions, ring signatures allow users to transact anonymously by sending transaction information with a signature, ensuring that the user of the transaction is anonymous and that the information is not tampered with during transmission.

In summary, this paper has three main contributions:

(1) First, to solve the privacy and security threats in the process of online financial transactions based on blockchain technology, we introduce ring signature technology and propose a verifiable ring signature algorithm. At the same time, the operational efficiency of the system can be greatly improved while ensuring security.

(2) Second, we have designed a reliable ring signature protocol for online financial transactions. This system combines blockchain technology with a proposed ring signature algorithm that can be used for anonymous authentication and encrypted storage in blockchain systems.

(3) Based on the concept of distributed key agreement, this algorithm improves the traditional key distribution of third party trust bonds，and solve the problem of key loss caused by the unrealistic or malicious attacks of the trusted third party. The results of this project will provide a new solution for the problems of data sharing, synchronization of information and privacy in Internet financial transactions.

1.2 Organization

The remainder of the paper has the following structure. In Sect. 2, we summarize and analyze the relevant work in the article. In Sect. 3, we describe the mechanism of action of blockchain and ring signatures and their application in the context of this paper. In Sect. 4, we design a solution for online financial transactions based on blockchain technology combined with ring signature algorithms and present a verifiable ring signature algorithm. In sect. 5, we perform an auditable safety analysis. In Sect. 6, We evaluate and compare the proposed solution with other similar solutions. Finally, in Sect. 7, we summarize the article and make a few conclusions.

2. Related Work

Over the past few years, a number of blockchain-related studies have been conducted by a variety of scholars on asset trading. Christidis et al. [14] proposed a scheme to transfer digital ring assets on the blockchain. On this basis, the flow of digital assets is achieved through smart contracts using the characteristics of blockchain and the Internet of Things. Cui et al. [15] proposed a blockchain-based trading system, which addresses issues related to data caching, data replication and retention of transaction data in data asset transactions, safeguarding the rights and interests of transaction users from being appropriated by the trading platform and protecting their data privacy and security. Roman et al. [16] studied the use of smart contracts for trading digital assets. However, due to its publicly traceable nature, while blockchain is able to build trusted interaction environments between untrustworthy parties, it does not allow

for true anonymity.

As a result, a great deal of research has been carried out by scholars in recent years to address both privacy and security issues. For example, Pramanik et al. [17] proposed a four-dimensional framework the same big data analytics approach used to analyze and remove the new generation of privacy-preserving data, for protecting data privacy. The advantage is that people will be able to use their critical analysis results to improve their Big Data analytics strategy deployment in their business environment, to make better use of Big Data to innovate and grow sustainably. He et al. [18] proposed a new blockchain privacy-preserving search model and designed a new blockchain searchable encryption scheme for this problem. The model can realize the virtual search and matching efficiently, but the efficient work makes the computational cost increase as well. Bhushan et al. [19] provide insights into the security and privacy of blockchain technology to reveal the challenges it faces and to explore how blockchain technologies are addressing them. But do not actually provide empirical proof of a solution to any privacy problem.

Sun et al. [20] highlight the high risk that at-tackers may pose to business transactions and private data by compromising sensitive assets to gain access to financial information, thus posing a high risk to commercial transactions and private data. However, since the solution uses Answer Set Programming (ASP) to expand the logic of LC, it overcomes the special limitation of LC which has unconditional security , despite their advantages, offer limited protection to users of the same node. Peng et al. [21] proposed VF-Chain, a verifiable and auditable blockchain-based federated learning framework for addressing their user privacy concerns. The advantage of this method is that it can increase the efficiency of verification proof and support the safe rotation of committees. Dai et al. [22] integrated blockchain into network slices and network software specifically for SAGSINs, targeting Internet privacy violations. Zaghloul et al. [23] discussed the security and privacy protection of bitcoin. Andola et al. [24] analyzed the anonymity of blockchain-based electronic cash. However, they all have the problem of high overheads.

To enhance anonymity, many people have applied ring signatures in blockchain systems, among which, in 2001, in the context of how to leak secrets anonymously, Rivest first proposed a new signature technique, the ring signature. Chow et al. [25] proposed a novel identity-based ring signature scheme that only requires two pairing operations to be performed for any group size. Chen et al. [26] proposed based on an anonymous identity of ring signature P2P network system. However, the application of bilinear pairing adds significant computational costs and communication overheads, making the application of the scheme significantly more expensive. It can be seen that the privacy mechanism of the ring can indeed mix many public keys to hide the real input address. It is possible to use ring signatures as an encryption tool for hiding inputs. Breaking event tracking in the mix of real event addresses makes it difficult to create event hiding maps and reach destinations, but the communication overhead and computational costs are also difficult to cut, depending on the application scenario and the basics of the program.

According to the above summary, we can see that the property security and privacy of online users has been paid attention to all over the world, and ring signature as an emerging tool has natural anonymity advantages in applying to the privacy and security issues of blockchain. At present, domestic and international research on the application of ring signatures on blockchain has become mature, but there are still problems such as large scheme overhead, large computational cost and long running time. It is still challenging to design a secure and efficient verifiable ring signature scheme with low overhead for blockchain financial online transactions.

3. Preliminaries

3.1 Blockchain and Smart Contract

Blockchain is a decentralized distributed ledger, often used in new digital cryptocurrencies. Blockchain theory is the foundation and technology that has led to applications such as bitcoin and Ethernet [27]. The decentralized, transparent, immutable, non-falsifiable and traceable characteristics of blockchain can make it excellent for application scenarios that require information interaction, such as finance, healthcare, communications, cybersecurity and resource sharing, and it has attracted considerable attention and innovative research from scholars in these fields.

Blockchain is a data structure assembled in the order of time, similar to a linked list. It is a distributed, decentralized ledger that uses cryptography to ensure it is immutable and tamper-proof, allowing simple, sequential relationships to be securely stored and verified within the system [28]. Each block contains all the information that makes up the block at the current time, providing an immutable data store. Depending on the type of access that an application or system uses, they can generally be categorized as public, specialized, and federated. Its universal underlying technology framework can bring about profound changes in finance, business, science and technology, politics and other fields.

Blockchain integrates multiple technologies into a complex and large-scale architecture [29]. Based on the blockchain infrastructure model proposed by Zhang et al.[30] and Zuo et al. [31], this paper enriches the content of the model as shown in **Fig. 1**. Based on the structure of top to bottom, there are 6 levels: Application, Contract, Motivation, Consensus, Network and Data.

- **Application Layer:** For blockchain application scenarios and cases, enhance and encapsulate existing blockchain technology.
- **Contract Layer:** Smart Contracts Encapsulation, Scripts, Algorithms.
- **Incentive layer:** In the blockchain technology system, an economic element is introduced, rewards are distributed in the form of tokens, and a uniform algorithm is used.
- **Consensus Layer:** Ensure that decision making across the distributed network is fast, efficient, effective and consistent.
- **Network Layer:** Networking mechanism, transmission protocol, data verification mechanism and other information for distributed networks.
- **Data Layer:** The basic block of the block is wrapped up, and it is associated with the structure information of the data, the timestamp of the data.

Among them, time stamp based blockchain structure, distributed node consensus mechanism, economic motive based on consensus computation ability. In addition, flexible and programmable smart contracts are a distinctive innovation point of blockchain technology.

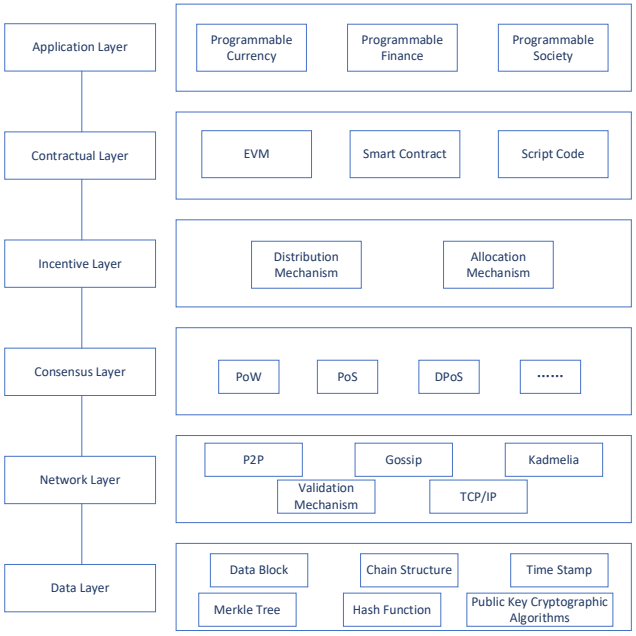

Fig. 1. Blockchain Infrastructure Model

One of the most attractive uses of blockchain technology is the Intelligent Contract Concept, which is transparent, immutable, and free from corruption [32]. The Smart Contract, originally introduced in 1995 by Nick Szabo, is a set of obligations in digital form, which contains all the obligations that can be fulfilled by all parties [33]. The perfect combination of blockchain and smart contracts is Ethereum. Smart contracts can receive external transaction requests and event triggers as code running in the Ethereum virtual machine. Smart contracts herald the start of the Blockchain 2.0 era, in which smart contracts offer a safe, secure platform for automatic execution of contractual clauses, rather than relying on trusted intermediaries. Lawyers or banks, for instance, resulting in lower transaction costs, lower administrative costs and faster transaction times. **Fig. 2** illustrates how a smart contract can be structured.

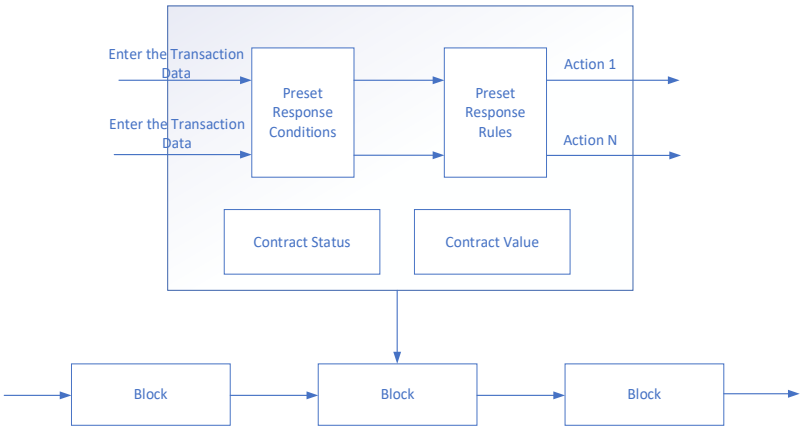

Fig. 2. Smart Contract Model

3.2 Ring Signature

Ring signatures are a class of signatures that evolved from group signatures. In 2001, in the context of how to leak secrets anonymously, Rivest first proposed a new signature technique, the ring signature. The signer can temporarily filter and randomly select members to form a group according to different scenarios, and the signer collects the member's public key and combines it with his own private key to create a ring signature [34]. Instead of a specific public key, the signature is verified with a set of public keys. There is no central trust, no swarm building process, and the signers are completely anonymous to the verifier [35]. The advantage of this solution is that no one else in the ring can forge it except for the person who signed it. An external attacker cannot forge a signature even if he has obtained a valid ring signature [36]. In a particular environment that requires long-term protection of information, the absolute anonymity of a ring signature can be very useful.

There are three underlying algorithms for ring signature, namely: Keygen, Sign, Verify. **Fig. 3** shows the flowchart of the ring signature algorithm.

- **Keygen:** The user creates a key pair (pk, sk), where sk is the private key, which pk is the public key.
- **Sign:** The signer signs the information M with his own private key and the public key collection $L = \{pk_1, pk_2, \ldots, pk_n\}$ of the owner, generating a ring signature σ, one of these parameters σ forms a ring according to certain rules.
- **Verify:** In the ring signature scenario, after entering a signature σ, a message M, and the public key of a ring member, if the ring signature is verified, it is output $True$. Otherwise, output $False$.

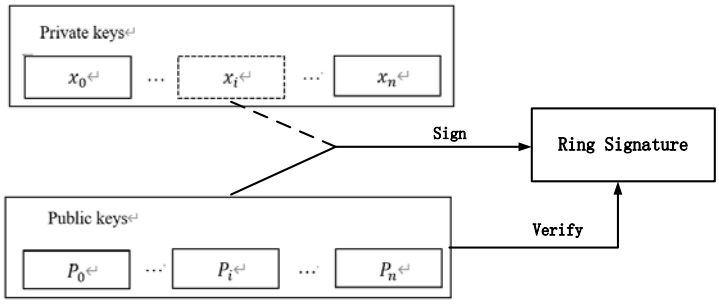

Fig. 3. Ring Signature Algorithm Model

3.3 Bilinear Maps

Bilinear groups can be described by quintuples (p, G_1, G_2, G_T, e). In the quintuple, p is a given security constant λ. The related large prime numbers, G_1, G_2 and G_T, are multiplicative cyclic groups of order p, and e is a bilinear map e: $G_1 \times G_2 \to G_T$, which meets the following three conditions:

- **Bilinearity:** given any $P \in G_1$, $Q \in G_2$, $a, b \in Z_q^*$, there is always $e(aP, bQ) = e(P, Q)^{ab}$;
- **Non-degeneracy:** for $\exists P \in G_1, Q \in G_2$, it is satisfied that $e(P, Q) \neq 1$;
- **Computability:** the bilinear map e: $G_1 \times G_2 \to G_T$ is efficiently computable.
  For all $P \in G_1, Q \in G_2$, the map e is symmetric since $e(P^a, Q^b) = e(P^b, Q^a) = e(P, Q)^{ab}$.

3.4 Difficult Assumptions

The following describes the difficult assumptions underlying the security of the ring signature scheme in this paper.

Suppose that G_1 is a cyclic group generated by P, the order of which is a prime number q, and there exists a bilinear map e: $G_1 \times G_1 \rightarrow G_2$. We assume that multiplication and inversion in G_1 can be computed in a unit time, and let a, b, and c be elements of Z_q^*.

- **Definition 1. Discrete Logarithm Problem：** Pick the generating element g and given y, compute $a \in Z_q^*$ such that $y = g^a mod\ p$ is difficult.
- **Definition 2. Decision Bilinear Diffie-Hellman:** It is known that G_1 is a group of order g, and that g is a generating element of this group. Given a random choice of a, b, c on Z_q^* and given that the attacker A knows g^a and g^b, it is impossible to distinguish (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c) with negligible probability.

4. Blockchain-Based Online Financial Transaction Ring Signature Model

In this section, we present a safe and secure solution for the protection of the privacy of financial transactions. Combined with the tracking ring signature algorithm, the transaction data can be safely shared.

4.1 System Model

The online financial transaction model of this article is shown in Fig. 4, which includes four entities: transaction user A, transaction user B, blockchain, and third-party financial institutions, as described below:

1. Transaction User A (Trading Data Generator): User A generates system parameters and keys through a decentralized exchange, outputs transactions and uploads them encrypted. Then, an intelligent contract is established with access control and decryption algorithms, which are packaged and sent to the blockchain nodes.

2. Transaction User B (Transaction Data Receiver): User B is the recipient of the transaction data for this program. By decrypting and verifying the plaintext of the received message, the correct and complete transaction data is obtained.

3. Blockchain (Transaction Record): This article's blockchain is a decentralized wallet. The nodes of the blockchain in our system include network routing, Full Blockchain Database, Miners and Wallets. The network routing module is responsible for discovering and maintaining the connection of peers, as well as broadcasting and accepting new blocks. The Full Blockchain Database Module is responsible for preserving the complete and up-to-date blockchain data. On Bitcoin's blockchain network, mining modules are tasked with creating new blocks in a competitive manner by executing POW consensus algorithms on some special hardware device. The wallet module completes the management of user keys, assets, transactions and other information.

4. Decentralized exchanges (Transaction data sharers): OTC (Over the Counter) trading is a peer-to-peer transaction outside the exchange, guaranteed by a third party. Responsible for the initial registration of the transaction user, generating the system parameters and the key of the trading user at the same time, and sending it to the trading user through a secure channel, generally defaulting to a trusted authority.

Fig. 4 shows the blockchain-based online financial transaction ring signature scenario model. There are n trading users in ring L, $L = \{id_1, id_2, \cdots, id_n\}$, suppose that user A in the ring signs message m on behalf of all users in the ring. After acceptance, the validation program verifies the correctness of this signature. After confirmation, this information is transmitted to the recipient user B. Afterwards, user B obtains the relevant information by comparing the results of the transaction.

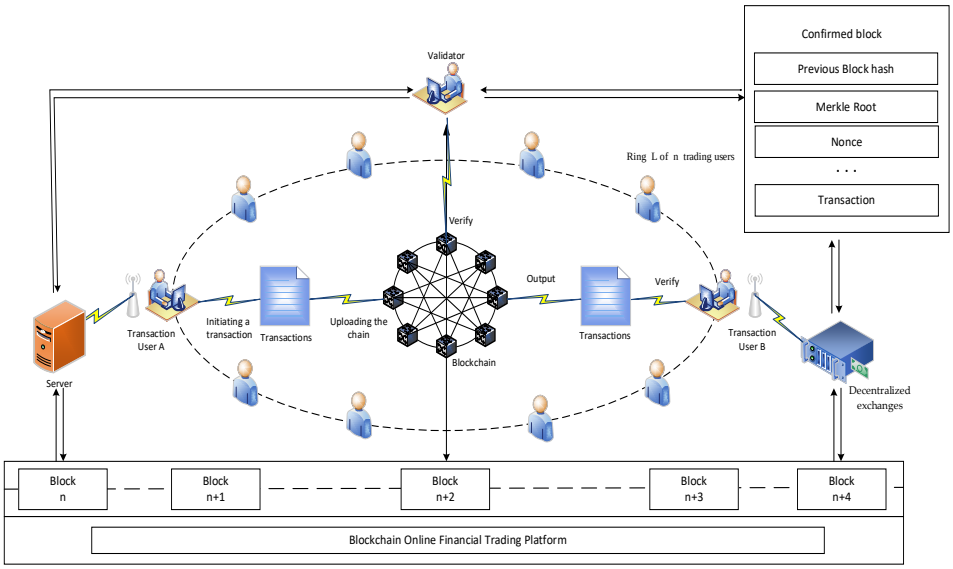

Fig. 4. Blockchain-based Online Financial Transaction Ring Signature Model

4.2 System security goals

1. Unconditional anonymity: In a ring, both the sender and the recipient are anonymous, and only when necessary can the receiver and the sender be able to trace the sender's real identity.

2. Verifiability: We can verify the validity of the membership of nodes in the network, the validity of the trace markers, the integrity of the message passed and the ring signature.

3. Anti-forgery: An adversary cannot forge the identity of the signer for communication transactions, nor can it forge the ring signature to pass the recipient's verification.

4.3 Scheme Description

Step 1: Data Generation

1. Identity Registration. User A publishes the resulting identification information to the entire network. After having been verified by the network, their personal information is compressed into a single file, which is then registered.

2. System Initialization. The additive loop group with the order q is the prime number, and the generator of G_1 is P, and G_2 is a group of multiplicative loops of the q same order. Select a generator P for G_1. Choose a bilinear map $e: G_1 \times G_1 \to G_2$. Choose two anti-collision hash functions: $H_1: \{0,1\}^* \to G_1, H_2: G_2 \to \{0,1\}^1 \times G_1 \to Z_q^*$. Enter a security parameter k, the security parameters k is a large enough prime number, and $q > k$.

3. Key Generation. The external exchange is responsible for the initial registration of the trading user, while generating the system parameters and keys of the trading user and sending them to the trading user through a secure channel. The transaction originator id_i selects a

random number $s \in Z_q^*$ as the master private key, and calculates the system public key $PK_0 = sP$ and $Q_i = H_1(ID_i), i = 1,2,\cdots,n$.

4. The originator id_i arbitrarily selects $x_i \in Z_q^*$, and then calculates the originator's private key $SK_{id_i} = x_i \cdot psk_{id_i} = x_i \cdot s \cdot Q_i$ and public key $PK_{id_r} = (X_i, Y_i) = (x_i Q_i, x_i PK_0)(i = 1,2,\cdots,n)$ according to his identity id_i. The identity of the receiving user is id_k.The user id_k randomly selects $x_k \in Z_q^*$, and the receiver's private key $SK_{id_k} = x_k \cdot s \cdot Q_k$ and public key $PK_{id_k} = (X_k, Y_k) = (x_k Q_k, x_k PK_0)$ are calculated.

Step 2: Data Generation

The user A initiates a transaction and generates a smart contract for signature, the signing process is as follows:

1. We set the signatory user's serial number to r and the key pair to （PK_{id_r}, SK_{id_i}）, and select any N user identities on the exchange to form the set $L = \{id_1, id_2, \cdots, id_n\}$, including the signer id_r.

2. The message to be signed is clearly m. And randomly select $\alpha_i \in Z_q^*$, $\alpha_s \in Z_q^*$, $\alpha \in \{0,1\}^*$, and calculate $R_i, h_i, R_s, h_s, V, T, t, L$. Finally, generate a ring signature $\sigma = (m, R, R_1, \cdots, R_n, V, t, C)$.

3. The user A turns the transaction data and signature into a message (m, σ) encrypted with the user B's public key, and sends it to User B.

Step 3: Data sharing

1. Transaction Generation. User A generates $n - 1$ multiple transactions with the same amount value as the output of the transaction, and mixes the transactions to user B in all output transactions without the participation of others, hashed the transaction and constructs the address image of the transaction $Y = E_{PK_{id_s}}(hash(b))$ and the related witness. Then, run the ring signature algorithm to sign the hash value h to generate a ring signature σ.

2. Transaction Node. Each transaction user in the network has a communication sensor that interacts with other users, and the transaction user can communicate or trade with other users through 4G/5G. User A encapsulates a smart contract containing access control, cryptographic hash index, private key and decryption in a block.

3. Verification Unit. The decentralized exchanges mainly responsible for checking the address image, verifying the validity and correctness of the ring signature containing the transaction, and if the verification passes, it will be sent to the receiving user.

4. Transaction Verification. First, the authenticator checks the address mirror to see if the sender spends the same account twice. The verification algorithm verifies that the signature σ of the transaction is correct. The proposed signature scheme is verified, and if all the verifications pass, the scheme is shown to be correct, and then packaged and encapsulated in a new block. Otherwise, the transaction will be deemed null and void.

Step 4: Transaction Confirmation.

1. Signature verification. After the receiving user id_k receives the ring signature σ, verify its legitimacy. If the signature is valid, the verifier will accept it. Otherwise, the verifier rejects the ring signature.

2. Signer Authentication. When the message recipient discovers that the signer sent illegal information, he can apply to Decentralized Exchange to trace the true identity of the message sender. The receiving user can confirm the identity $t = H_2(T, V, X_S, Y_s, \alpha)$, $e(Y_s, T) = e(P, V)$ of the true signer of the signature by verifying that the equation is true. If the equation is true, the signature can be considered valid and the true signer can be confirmed id_r. If not, it means that the signature was not signed by a genuine signer and is invalid.

3. User B checks multiple transaction outputs for comparison, extracts the target value from these transactions and calculates $Y' = E_{PK_{id_s}}(hash(b))$. If $Y' = Y$, proves that the transaction was sent to user B by user A. So, accept the output of the transaction and put Y and record keeping the (PK_{id_s}, SK_{id_s}).

4.4 Proposed Verifiable Ring Signature Algorithm

1. System Initialization. System parameter generation algorithm: The additive loop group with the order q is the prime number, and the generator of G_1 is P, and G_2 is a group of multiplicative loops of the q same order. Select a generator P for G_1. Choose a bilinear map $e: G_1 \times G_1 \to G_2$. Choose two anti-collision hash functions: $H_1: \{0,1\}^* \to G_1, H_2: G_2 \to \{0,1\}^1 \times G_1 \to Z_q^*$. Enter a security parameter k, the security parameters k is a large enough prime number, and $q > k$. The sender id_i selects a random number $s \in Z_q^*$ as the primary private key, and calculates system public key $PK_0 = sP$ and $Q_i = H_1(ID_i), i = 1,2,\cdots,n$. Therefore, the system exposes parameters is $Params = \{q, e, G_1, G_2, H_1, H_2, P, PK, PK_0\}$.The message space is $m \in \{0,1\}^*$.

2. User Authorization. The user id_i initiates a request authorization operation, the Key Generation Center (KGC) calculates a portion of the user's private key $psk_{id_i} = s \cdot H_1(ID_i) = sQ_i$, after authentication of the user's identity ID. Then, KGC computes part of its private key and transmits it to the user over a secure channel id.

3. Key Generation. First, after the user id_i gets part of the private key, enter the $Params$. Pick a random number $x_i \in Z_q^*$ as its secret value. Then, the KGC calculates the public key PK_{id_i} of the receiving user and will (Q_i, psk_{id_i}) sends to the user id_i: $PK_{id_r} = (X_i, Y_i) = (x_i Q_i, x_i PK_0)(i = 1,2,\cdots,n)$. Second, the user id_i enters the system master private key s to generate its own complete private key: $SK_{id_i} = x_i \cdot psk_{id_i} = x_i \cdot s \cdot Q_i$.

4. Signature Generation. Suppose there are n trading users in the ring L,their identities are set for $L = \{id_1, id_2, \cdots, id_n\}$. The corresponding public key set is $C = \{PK_{id_1}, PK_{id_2}, \cdots, PK_{id_n}\}$. The message is clearly written m and signer is id_r. Enter the exposed $Params$, public and private keys PK_{id_r}, SK_{id_r}:

(1) For any $i \in \{1,2,\cdots,n\}$,if $i \neq s$,then randomly select an integer $\alpha_i \in Z_q^*$, and compute: $R_i = \alpha_i X_i, h_i = H_2(m, R_i, L)$.

(2) If $i = s$.then randomly select an integer $\alpha_s \in Z_q^*$, and compute the following:

$$R_s = \alpha_s X_s - \sum_{i=1, i\neq s}^{n} (\alpha_i + h_i) X_i \quad (1)$$

$$h_s = H_2(m, R_s, L) \quad (2)$$

$$V = (h_s + \alpha_s) \cdot SK_{id_s} \quad (3)$$

(3) For any $\alpha \in \{0,1\}^*$, calculate the trace key:

$$T = (\alpha_s + h_s) Q_s \quad (4)$$

$$t = H_2(T, V, X_S, Y_s, \alpha) \quad (5)$$

(4) Generate Signature: Ultimately, sends the generated ring signature σ to the receiving user id_r.

$$\sigma = (m, R, R_1, \cdots, R_n, V, t, C) \quad (6)$$

5. Signature Verification. After receiving the ring signature σ, the receiving user id_r verifies its legitimacy by doing the following for all $i \in \{1,2,\cdots,n\}$.

(1) Verify equation (7) is true. If not, the public key is not legitimate. Conversely, if the equation holds, it is calculated: $h_i = H_2(m, R_i, L, Y_i)$.If the equation holds, the public key is valid. Otherwise, the public key is invalid.

$$e(X_i, PK_0) = e(Q_i, Y_i) \quad (7)$$

(2) Verify the equation (8) is true. If the equation is true, the above signature is valid and the verifier accepts it. Otherwise, the validator rejects the ring signature.

$$e(PK_0, \sum_{i=1}^{n}(R_i + h_i X_i) = e(P, V) \quad (8)$$

6. Signer Authentication. The receiving user can pass the authentication equation: $t = H_2(T, V, X_S, Y_s, \alpha)$, $e(Y_S, T) = e(P, V)$. Whether it is true or false, it is necessary to verify the authenticity of the signature. If the equation is true, the signature can be considered valid, and the true signer can be confirmed. If not, it means that the signature was not signed by a genuine signer and is invalid. **Fig. 5** shows the specific ring signature implementation steps.

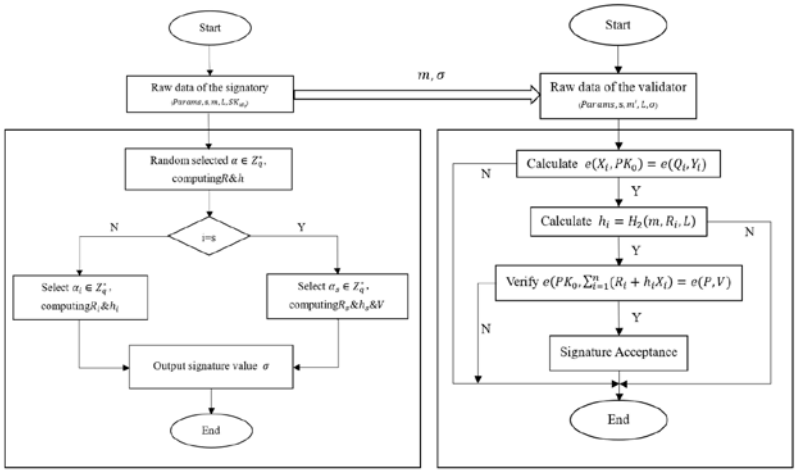

Fig. 5. Ring Signature Algorithm Flowchart

5. Security Analysis

5.1 Unconditional Anonymity

This security nature is mainly guaranteed by the anonymous authentication mechanism of the scheme. In ring signature $\sigma = (m, L, R, R_1, \cdots, R_n, V)$, $V = (h_s + \alpha_s) \cdot SK_{id_s}$, $R_i = \alpha_i X_i$, $R_s = \alpha_s \cdot X_s - \sum_{i=1, i \neq s}^{n}(\alpha_i + h_i) X_i$.These are randomly selected by the signer. The result of this choice is that the $\sigma = (m, L, R, R_1, \cdots, R_n, V, t, C)$ appear evenly distributed in G.

In the ring signing algorithm, when the message receiver performs the authentication operation, it enters the identity set L. To the receiver, each user in the identity collection may be the legitimate sender of the clear text of the message. Therefore, the receiver cannot determine who is the real sender, thus ensuring the privacy nature of the sender's identity on the basis of authentication.

5.2 Verifiability

First of all, the signature's private key consists of a random secret value selected by the signer and a portion of the private key produced by an external transaction, which is synthesized by the signer. At the time of registration, the authenticity of the identity of the transaction initiator can be verified by the external exchange, and the transaction initiator can use the part of the private key sent by the external exchange.

After receiving the ring signature, We can verify the correctness of the user key by the following equation $e(X_i, PK_0) = e(Q_i, Y_i)$, which is proved as follows: $e(X_i, PK_0) = e(x_i Q_i, PK_0) = e(Q_i, x_i PK_0) = e(Q_i, Y_i)$.

If the user key is correct, then in the signature verification phase, we verify that the equation $e(PK_0, \sum_{i=1}^{n}(R_i + h_i X_i)) = e(P, V)$ is true. we have ,

$$
\begin{aligned}
e\left(PK_0, \sum_{i=1}^{n}(R_i + h_i X_i)\right) &= e\left(PK_0, \sum_{i=1, i\neq s}^{n}(R_i + h_i X_i)\right) e(PK_0, R_s + h_s X_s) \\
&= e\left(PK_0, \sum_{i=1, i\neq s}^{n}(R_i + h_i X_i)\right) e\left(PK_0, \alpha_s \cdot X_s - \sum_{i=1, i\neq s}^{n}(\alpha_i + h_i) X_i \right. \\
&\left. + h_s X_s\right) \\
&= e(PK_0, \sum_{i=1, i\neq s}^{n}(\alpha_i \cdot X_i + h_i X_i) + \alpha_s X_s - \sum_{i=1, i\neq s}^{n}(\alpha_i + h_i) X_i + h_s X_s) \\
&= e(PK_0, \sum_{i=1, i\neq s}^{n}(\alpha_i + h_i) X_i + \alpha_s X_s - \sum_{i=1, i\neq s}^{n}(\alpha_i + h_i) X_i + h_s X_s) \\
&= e(PK_0, \alpha_s X_s + h_s X_s) = e(sP, (\alpha_s + h_s) X_s) = e(sP, (\alpha_s + h_s) x_s Q_s) \\
&= e(P, (\alpha_s + h_s) s \cdot x_s \cdot Q_s) = e(P, (\alpha_s + h_s) SK_{id_s}) = e(P, V)
\end{aligned}
$$

If any of the items are tampered with during the ring signing process, the verification will not be passed.

Secondly, in the process of confirming the identity of the real signer, it is necessary to verify that the equation $e(Y_s, T) = e(P, V)$ be valid, which is proved as follows: $e(Y_s, T) = e(x_s \cdot sP, (\alpha_s + h_s) Q_s) = e(P, V)$.

Where the calculation of the value T uses Q_s, the purpose of binding the identity of the real signer, a process that indicates that the signature satisfies the verifiability.

5.3 Unforgeability

Assuming that an attacker id_k attempts to forge the signature id_r of a real signer, a valid signature can be constructed directly using the signer's private key, but this process cannot be completed in this scenario.

Because in the above scenario, the private key of id_r is defined as $SK_{id_r} = x_r \cdot s \cdot Q_r$. Therefore, the attacker id_k must know two important parameters x_r and s. However, since $x_i \in Z_q^*$ is randomly selected by the signer, there is no way for id_k to obtain the private key SK_{id_r} of id_r in the completely unknown case. Thus, in this case, there is no way to forge the valid signature.

6. Benchmark Test

This part simulates a verifiable ring signature algorithm and compares it with other methods for performance and functionality. The experimental running configuration is:I5-1135G7 @ 2.40GHz, 8GBRAM on the HUAWEI desktop, running on Windows 11, Eclipse development environment, using JAVA version 1.8.0 and JPBC version 2.0.0, in an implementation of the library Type-A-Class curves to form a symmetric first-order bilinear group.

6.1 Calculate overhead analysis

In this paper, the effectiveness of this scheme is evaluated by computational cost, the evaluation results are analyzed, and the computational overhead of several traceable ring signature schemes is compared [37-40]. **Table 1** illustrates the meaning represented by the arithmetic symbols. A comparison of the performance of the various methods is given in **Table 2**. **Fig. 6** shows how long the various methods take when n varies from 100 to 1000. For a clearer comparison, we specifically list the performance of total operations when n=1000, as shown in **Fig. 7**.

Table 1. Description of the symbols and different operation times

Symbols	Meaning
OM	The time for one multiplication operation,1OM≈0.35ms
OP	The time for one bilinear pairing operations,1OP≈2.21ms

Table 2. Performance Comparison with Other Schemes

Schemes	Total Cost
Shen et al. [37]	7nOP
Gayathri et al. [38]	6nOP +7nOM
Wu et al. [39]	nOP+7nOM
Cui et al. [40]	3nOM+2nOp
Ours	2nOM+nOP

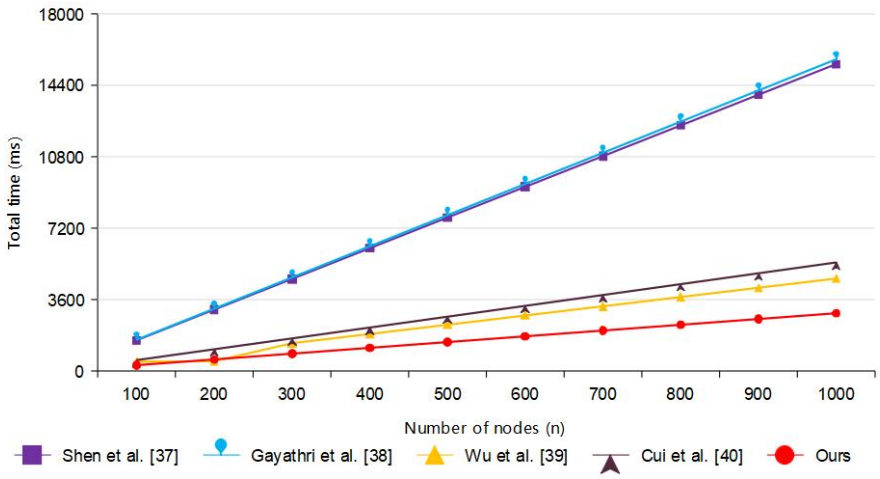

Fig. 6. Comparison of Total Cost

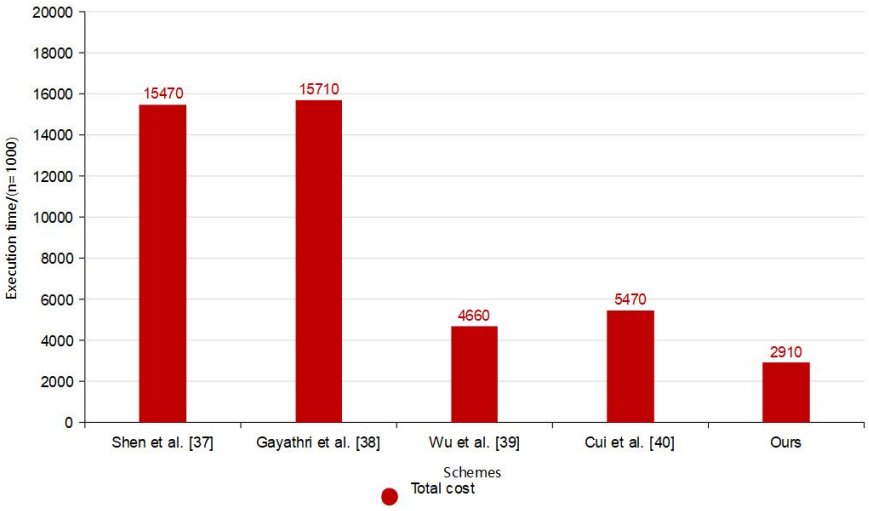

Fig. 7. Comparison of Total Cost (n=1000)

Regarding the whole cryptographic operation, we will find that Shen et al. [37] is 7nOP, Gayathri et al. [38] is 6nOP +7nOM, Wu et al. [39] is nOP+7nOM, Cui et al. [40] is 3nOM+2nOp, and ours are 2nOM+nOP. It can be seen that the scheme in this paper is more efficient and has a shorter overall length compared to those schemes in the literature.

7. Conclusion

In this paper, we construct a blockchain online financial transaction privacy protection protocol based on ring signatures. To achieve the hiding of transaction user information in the ring signature transaction protocol, we first design a verifiable ring signature scheme based on difficult problem assumptions, which is unforgeable, anonymous and verifiable. Secondly, our paper aims to build a scenario for blockchain online financial transactions using the high integrity of blockchain and the unconditional anonymity of ring signature, supplemented by smart contract technology, and proposes a privacy protection protocol for blockchain online financial transactions based on ring signature, which saves signature execution time and storage space, has lower complexity, shorter signature length and lower overhead, and can effectively improve the efficiency of signature and better protect the privacy of users in the transaction process.

In summary, this paper can achieve anonymity, verifiability and unforgeability of online transactions of digital assets with the help of blockchain and ring signature function, which is a secure and efficient ring signature scheme.

Acknowledgement

This research was supported in part by Shaanxi Provincial Social Science Foundation (2022D161), Shaanxi Province Philosophy and Social Sciences Major Theoretical and Practical Problems Research General Project (SX-318), Communications Soft Science Project of the Ministry of Industry and Information Technology (2021-R-44) and Shaanxi Province Soft Science Project (2023-CX-RKX-024). The authors express their gratitude for the support received.

References

[1] L. Wang, X. F. Liu, and X. D. Lin, "A fair and privacy-preserving image trading system based on blockchain and group signature," *Security and Communication Networks*, vol. 2021, pp. 1-18, Oct. 2021. Article (CrossRef Link).

[2] C. Rupa, D. Midhunchakkaravarthy, and M. K. Hasan, "Industry 5.0: Ethereum blockchain technology based DApp smart contract," *Mathematical Biosciences and Engineering*, vol. 18, no. 5, pp. 7010-7027, Aug. 2021. Article (CrossRef Link).

[3] Y. L. Wu, H. N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300-2317, Feb. 2021. Article (CrossRef Link).

[4] R. T. Ren and J. Q. Su, "A security-enhanced and privacy-preserving certificateless aggregate signcryption scheme based artificial neural network in wireless medical sensor network," *IEEE Sensors Journal*, vol. 23, no. 7, pp. 7440-7450, 2023. Article (CrossRef Link).

[5] S. Tadelis, "The Economics of Reputation and Feedback Systems in E-Commerce Marketplaces," *IEEE Internet Computing*, vol. 20, no. 1, pp. 12-19, Feb. 2016, Article (CrossRef Link).

[6] R. Guo, G. Yang, H. X. Shi, Y. H. Zhang, and D. Zheng, "O^3-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System," *in IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8949-8963, June. 2021. Article (CrossRef Link).

[7] E. F. Cahyadi, T. W. Su, C. C. Yang, and M. S. Hwang, "A certificateless aggregate signature scheme for security and privacy protection in VANET," *International Journal of Distributed Sensor Networks*, vol. 18, no. 5, May. 2022. Article (CrossRef Link).

[8] R. T. Ren, J. Q. Su, B. Yang, R. Y. K. Lau, and Q. L. Liu, "Novel Low-Power Construction of Chaotic S-Box in Multilayer Perceptron," *Entropy*, vol. 24, no. 11, pp. 1552, Oct. 2022. Article (CrossRef Link).

[9] H. T. Nie and N. Li, "Protection of trade secrets of financial transactions under big data: dilemma and countermeasures," *Technology and Law*, pp. 31-37, 2020. Article (CrossRef Link).

[10] J. Q. Su, R. T. Ren, Y. H. Li, R. Y. K. Lau, and Y. K, Shi, "Trusted Blockchain-based Signcryption protocol and data management for Authentication and Authorization in VANET," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–14, Jan. 2022. Article (CrossRef Link).

[11] W. B. Shi, N. Kumar, P. Gong, N. Chilamkurti, and H. Chang, "On the security of a certificateless online/offline signcryption for Internet of Things," *Peer-to-Peer Networking and Applications*, vol. 8, no. 5, pp. 881-885, Jan. 2015. Article (CrossRef Link).

[12] W. B. Shi, J. Q. Wang, J, J. X. Zhu, Y. P. Wang, and D. M. Choi, "A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation," *Intelligent Automation and Soft Computing*, vol. 25, no. 1, pp. 171-181, 2020. Article (CrossRef Link).

[13] J. J. Li, Y. Yuan, and F. Y. Wang, "Analyzing Bitcoin transaction fees using a queueing game model," *Electron Commer Res*, vol. 22, pp. 135–155, March. 2022. Article (CrossRef Link).

[14] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 2016, no. 4, pp. 2292-2303, May. 2016. Article (CrossRef Link).

[15] W. Cui, Y. Pan, and Z. D. Ai, "A blockchain-based transaction system for private data sharing and trading," *Control Theory and Technology*, vol. 20, no. 3, pp. 291-302, May. 2022. Article (CrossRef Link).

[16] D. Roman and K. Vu, "Enabling Data Markets Using Smart Contracts and Multi-party Computation," in *Proc. of Business Information Systems Workshops*, pp. 258-263, Jan. 2019. Article (CrossRef Link).

[17] M. I. Pramanik, R. Y. K. Lau, M. S. Hossain, M. M. Rahoman, S. K. Debnath, M.G. Rashed, and M. Z. Uddin, "Privacy Preserving Big Data Analytics: A Critical Analysis of State-Of-The-Art," *WIREs Data Mining and Knowledge Discovery*, vol. 11, no. 1, Oct. 2020. Article (CrossRef Link).

[18] M. Q. He, G. X. Zeng, J. Zhang, L. R. Zhang, Y. C. Chen, and S. M. Yiu, "A New Privacy-Preserving Searching Model on Blockchain," in *Proc. of ICISC 2018 Information Security and Cryptology – ICISC 201*8, pp. 248-266, Jan 2019. Article (CrossRef Link).

[19] B. Bhushan, P. Sinha, K.M. Sagayam, and A. J, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Computers & Electrical Engineering*, vol. 90, March. 2021. Article (CrossRef Link).
[20] X. Sun, P. Kulicki, and M. Sopek, "Logic Programming with Post-Quantum Cryptographic Primitives for Smart Contract on Quantum-Secured Blockchain," *Entropy*, vol. 23, no. 9, p. 1120, Aug. 2021. Article (CrossRef Link).
[21] Z. Peng, J. L. Xu, X. W. Chu, S. Gao, Y. Yao, R. Gu, and Y. Z. Tang, "VFChain: Enabling Verifiable and Auditable Federated Learning via Blockchain Systems," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 173-186, Feb. 2022. Article (CrossRef Link).
[22] H. N. Dai, Y. L. Wu, M. Imran, and N. Nasser, "Integration of Blockchain and Network Softwarization for Space-Air-Ground-Sea Integrated Networks," *IEEE Internet of Things Magazine*, vol. 5, no. 1, pp. 166-172, March. 2022. Article (CrossRef Link).
[23] E. Zaghloul, T. T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10288-10313, Oct. 2020. Article (CrossRef Link).
[24] N. Andola, Raghav, V. K. Yadav, S. Venkatesan, and S. Verma, "Anonymity on blockchain based e-cash protocols—A survey," *Computer Science Review*, vol. 40, May. 2021. Article (CrossRef Link).
[25] S. S. M. Chow, S. M. Yiu, and L. C. K. Hui, "Efficient Identity Based Ring Signature," in *Proc. of International Conference on Applied Cryptography and Network Security*, pp. 499-512, 2005. Article (CrossRef Link).
[26] Y. Q. Chen, W. Susilo, and Y. Mu, "Identity-based anonymous designated ring signatures," in *Proc. of the 2006 international conference on Wireless communications and mobile computing*, pp. 189-194, July. 2006. Article (CrossRef Link).
[27] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and sustainable energy reviews*, vol. 100, pp. 143-174, Feb. 2019. Article (CrossRef Link).
[28] Y. Guo, and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, Sep. 2016. Article (CrossRef Link).
[29] K. F. Zhang, Z. Qiu, T. Chen, J. L. Lin, Y. S. Lian, and Z. R. Yang, "Research and improvement of blockchain DPoS consensus mechanism," in *Proc. of the 12th International Conference on Computer Engineering and Networks*, pp. 1284–1292, Oct. 2019. Article (CrossRef Link).
[30] Y. M. Zhang and C. Z. Zhang, "Improving the application of blockchain technology for financial security in Supply Chain Integrated Business Intelligence," *Security and Communication Networks*, vol. 2022, pp. 1-8, May. 2022. Article (CrossRef Link).
[31] A. Q. Zhang, P. Y. Zhang, H. Q. Wang, and X. D. Lin, "Application-Oriented Block Generation for Consortium Blockchain-Based IoT Systems with Dynamic Device Management," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7874-7888, 15 May15, 2021. Article (CrossRef Link).
[32] O. Owe and E. Fazeldehkordi, "A lightweight approach to smart contracts supporting safety, security, and privacy," *Journal of Logical and Algebraic Methods in Programming*, vol. 127, pp. 100772, June. 2022. Article (CrossRef Link).
[33] L. J. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, and Y. F. Suo, "Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet," in *Proc. of 2017 IEEE International Conference on Energy Internet (ICEI)*, pp. 176-181, 2017. Article (CrossRef Link).
[34] R. Guo, L. Xu, X. Li, Y. H. Zhang, and X. L. Li, "An Efficient Certificateless Ring Signcryption Scheme with Conditional Privacy-Preserving in VANETs," *Journal of Systems Architecture*, vol. 129, Aug. 2022. Article (CrossRef Link).
[35] F. L. Chen, Z. H. Wang, and Y. M. Hu, "A New Quantum Blind Signature Scheme with BB84-State," *Entropy*, vol. 21, no. 4, p. 336, March. 2019. Article (CrossRef Link).
[36] J. H. Chen, J. Ling, J. T. Ning, E. Panaousis, G. Loukas, K. Liang, and J. G. Chen, "Post quantum proxy signature scheme based on the multivariate public key cryptographic signature," *International Journal of Distributed Sensor Networks*, vol. 16, no. 4, April. 2020. Article (CrossRef Link).

[37] L. M. Shen, J. F. Ma, Y. B. Miao, and H. Liu, "Provably Secure Certificateless Aggregate Signature Scheme with Designated Verifier in An Improved Security Model," *IET Information Security*, vol. 13, no. 3, pp. 167-173, May. 2019. Article (CrossRef Link).
[38] N. B. Gayathri, T. Gowri, and P. V. Reddy, "Secure and Efficient Certificateless Aggregate Signature Scheme from Bilinear Pairings," *Information Security Journal: A Global Perspective*, vol. 28, no. 6, pp. 149-163, Nov. 2019. Article (CrossRef Link).
[39] G. Wu, F. Zhang, L. M. Shen, F. C. Guo, and W. Susilo, "Certificateless Aggregate Signature Scheme Secure Against Fully Chosen-Key Attacks," *Information Sciences*, vol. 514, pp. 288-301, April. 2020. Article (CrossRef Link).
[40] M. M. Cui, D. Z. Han, J. Wang, K. C. Li, and C. C. Chang, "ARFV: An Efficient Shared Data Auditing Scheme Supporting Revocation for Fog-Assisted Vehicular Ad-Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15815-15827, Dec. 2020. Article (CrossRef Link).

Jinqi Su received the Ph.D. degree in systems engineering from the Northwest Polytechnic University, Xi'an, China. He is an associate professor and dean with the School of Economics and Management, Xi'an University of Posts and Telecommunications. He is the author of more than 20 refereed international journals and conference papers. His current research interests include data mining, knowledge discovery, e-commerce, and digital economy.

Lin He received the B.S. degree in Economics from Xianyang Normal College, China in 2020. She is currently pursuing her master's degree at Xi'an University of Posts and Telecommunications, China. Her current research interests include digital economy, information systems and accounting.

Runtao Ren received the B.S. degree in information security from the Xi'an University of Posts and Telecommunications, Xi'an, China, and the M.S. degree in business and data analytics from the City University of Hong Kong, Hong Kong. He is currently pursuing the Ph.D. degree with the City University of Hong Kong, Hong Kong. He has worked as the research assistant with the Department of Information Systems, City University of Hong Kong, Hong Kong, and the School of Modern Post, Xi'an University of Posts and Telecommunications, Xi'an, China, in 2022. His current research interests include theoretical computer science, information systems, provable security, and digital economy.

Qilei Liu received the Ph.D in Management science and Engineering of Northwestern Polytechnical University, Xi'an, China. He is a lecturer in School of Economics and Management, Xi'an University of Posts& Telecommunications. He has published over 30 academic papers and his current research interests include digital innovation and system engineering.