Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Enhancing trust transfer in supply chain finance: a blockchain-based transitive trust model

Chang Shu[1], Yuling Chen[1*], Chaoyue Tan[1], Yun Luo[1] and Hui Dou[1]

Abstract

Artificial intelligence and blockchain technology have become indispensable in the era of the digital economy, particularly in the field of financial financing. However, when it comes to supply chain finance (SCF), existing models primarily focus on risk identification and credit evaluation, neglecting the critical aspects of trust transfer continuity and reliability within the chain. To address this issue, this paper proposes a blockchain-based transitive trust model for SCF, which ensures seamless trust transfer from core enterprises to bottom suppliers during financing enterprise credit evaluation. The model utilizes multi-layer metrics to calculate the comprehensive trust value of underlying suppliers, serving as the basis for credit delivery. Additionally, the model stores transitive signature receivable warrants on the blockchain and utilizes splittable delivery of warrants to underlying suppliers. The model's rationality and correctness are verified through experimental analysis, with results demonstrating that the transitive trust model enhances Small and Medium-Sized Enterprises' (SMEs) trust at the bottom of the supply chain, thus alleviating financing difficulties for SMEs.

Keywords Blockchain, Supply chain finance, Transitive signature, Trust evaluation

Introduction

With the advent of Industry 4.0 and the development of digital technology, the intelligence and automation of enterprise production processes are widely used, and this series of technologies is changing the traditional supply chain operation [1]. In traditional supply chain management, enterprises encounter challenges such as information imbalances, restricted capital flow, and operational inefficiencies, which limit their flexibility and competitiveness [2]. SCF serves as a crucial financial tool to address the capital and liquidity requirements within the supply chain. However, as the number of participants in the supply chain increases, a trust gap emerges among enterprises. While first-tier suppliers can leverage the high credit of core enterprises for financing, this creditworthiness does not extend to lower-tier suppliers at the end of the chain, resulting in a breakdown of trust [3]. Therefore, it is of utmost importance to enhance trust among all participants in the supply chain financing network and alleviate the problem of trust deficit within the chain.

Currently, the application of artificial intelligence technology provides more accurate decision support in the field of supply chain financing, and edge computing allows us to push computing power and data processing to the edges of IoT devices and sensors for real-time monitoring and data collection. Wu et al. [4]proposed a popularity-aware and diversity-based Web API recommendation method based on correlation graphs, while Qi et al. [5] introduced a personalized and compatible Web API recommendation method based on correlation graphs. These methods enable personalized

*Correspondence:
Yuling Chen
ylchen3@gzu.edu.cn
[1] State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, Guizhou 550025, China

recommendation services for each participant in SCF, facilitating better matching of funding needs and cooperation opportunities among supply chain parties. Wang et al. [6] proposed an accuracy-enhanced group recommendation method based on DEMATEL, which can achieve more accurate user group recommendation in the SCF platform. Regarding data query and management in SCF, Dai et al. [7] presented a Bloom Filter-based multi-collection membership testing method, Yang et al. [8] employed a deep Q-network for task offloading to enhance the efficiency of multimedia data analysis, and He et al. [9] implemented the EDIndex method for fast data query in an edge storage system. These approaches provide efficient data management support for SCF platforms.In terms of resource management, Xu et al. [10] explored a multimedia vehicle network resource reservation method based on traffic flow prediction, which provides a practical solution for logistics scheduling and resource management in SCF, and Jia et al. [11] proposed a convolutional neural network-based resource optimization method for supply chain management in edge computing environment to improve resource utilization efficiency and performance. Furthermore, Li et al. [12] developed a knowledge-driven anomaly detection framework that helps to improve the security and reliability of SCF systems. Xu et al. [13] used Canopy and K-medoids to initially classify suppliers, and then deployed back-propagation neural networks to evaluate the reputation of suppliers to improve the reliability and efficiency of supply chain by fostering increased trust.

Simultaneously, the advent of blockchain technology has introduced enhanced transparency, trust, and security to SCF. Recent studies have delved into reasonable protocols and attacks in blockchain systems [14], put forth semi-selfish mining techniques based on Hidden Markov Decision Process [15], explored the possibility of undetectable semi-selfish mining [16], and proposed a source location privacy protection scheme using phantom routing of sectors in Wireless Sensor Networks (WSNs) [17]. Hence, the amalgamation of blockchain and supply chain financing not only improves the transparency and integrity of financing transactions but also establishes a more robust credit rating system for the architecture of SCF [18]. Francisco et al. [19] highlight the visibility and auditability features of blockchain, which foster financial collaboration between upstream and downstream entities in the supply chain while reducing the risk of fraud. Cong et al. [20] propose that smart contracts enable effective cash flow management in transactions, thereby facilitating collaboration and cooperation within transaction networks in SCF. The inclusion of blockchain not only facilitates business collaboration among supply chain parties but also enables comprehensive evaluation of these parties through trust assessment. Malik et al. [21] put forward a reputation score-based trust chain to address trust-related concerns regarding the quality of goods and entities recording data on the blockchain. Ma et al. [22]propose a blockchain-based decentralized trust management system for digital copyrights, along with a token-based incentive-driven data consumption approach, aiming to prevent unauthorized dissemination or infringement of high-value data. The fusion of credit assessment and blockchain enhances the trust level among all participants in the SCF network, thereby facilitating financing for SMEs. Chen et al. [23] proposed a federated blockchain and game theory based energy trading scheme to further improve the efficiency and transparency of energy trading in the supply chain. Jiang et al. [24] proposed the use of intuition-based fuzzy entropy-based direct trust and dynamic weight assignment strategy of recommended trust to evaluate the credit of SMEs, however, the proposed strategy has room for improvement in terms of secure authentication.In the field of blockchain and security authentication, Chen et al. [25] present a dynamic multi-key FHE scheme based on the LWE assumption in public key setting. Meanwhile, Ren et al. [26] designed a blockchain-based secure storage mechanism, which adopts an on-chain and off-chain cooperative storage model to alleviate the shortage of blockchain storage capacity. The introduction of these innovative solutions has positively contributed to enhancing the security of blockchain.

Most of the existing models in SCF are designed for simple scenarios, lacking effectiveness in addressing the trust issues among SMEs at the bottom of multi-level supply chain. The transfer of trust between enterprises along the chain is challenging, leading to information asymmetry. To tackle these challenges, this paper proposes a blockchain-based transitive trust model for SCF. By leveraging the distributed characteristics of consortium chains, this model conducts a comprehensive investigation into trust transferability among suppliers in the supply chain while ensuring the security and privacy of SCF.In the proposed model, the trust between suppliers in the supply chain is quantified, and the transitive signature mechanism is employed to ensure more accurate measurement of trustworthiness among underlying suppliers. The key contributions of this paper are as follows:

1. Establishing a general framework of SCF based on the consortium chain. The current SCF faces challenges such as centralized trust and inefficient processes. To overcome these issues, a new general framework of SCF based on the consortium blockchain is proposed in this study. This approach is expected to improve

the efficiency and transparency of SCF and address the issues of centralized trust.
2. Supplier trust value quantification. We use direct, indirect, and incentive trust to quantify the comprehensive trust value of suppliers in SCF. Suppliers with high trust values are chosen to enhance the reliability of resource allocation and improve the overall trustworthiness of suppliers in SCF.
3. This model uses a graph-based signature mechanism to transitive trust between nodes in the supply chain. Financing certificates are stored in the federated chain and their detachability and signature verification enhance trust transferability, ensuring reliable trust transmission from the core enterprise to the bottom supplier.

The rest of this paper is organized as follows. The related work is described in "Related knowledge" section, and the general framework of federation chain-based supply chain financing and the design of transitive trust model are given in detail in "Blockchain-based transitive trust model for supply chain finance" section of this paper. In "Scheme analysis" section, security analysis and experimental analysis are conducted to prove the correctness and feasibility of the model from different perspectives based on our proposed transitive trust model. Finally, in "Conclusion" section, we conclude the paper and the next work outlook.

Related knowledge

This section will provide a detailed introduction to the basics related to blockchain technology and transferable signature mechanism covered in the article in order to more easily understand the model proposed in the article.

Blockchain related technology theory

Blockchain is a technology with characteristics such as decentralization, immutability, and traceability [27]. With the development in recent years, blockchain can be divided into three categories: public chain, private chain, and consortium chain according to its application scenarios and open objects [28]. Among them, private chains are almost indistinguishable from traditional distributed storage solutions, and because private chains are not open and scalable, their use is generally limited to the internal scope of the institution, which holds the writing ability of the whole chain, and the deployment of smart contracts and the reaching of node consensus are only done by the internal members of the institution. The public chain has the characteristics of openness and transparency, but the slow exit block limits its application scenarios. Compared with public and private chains, consortium chains are blockchain systems that are open to specific organizational groups and run nodes in a limited number of institutions that form a federated community. It has more powerful data processing capability, data privacy and scalability of consensus mechanism while being both open. In addition, the nodes in the consortium chain are divided into two categories: full nodes have complete transaction information, while light nodes only keep their own relevant information, which meets the needs of different types of entities. Therefore, this paper adopts the consortium chain to construct a SCF transaction network.

To ensure that the data remains immutable in an untrusted network, the blockchain technology stores the hash value of each block and the previous block in the block. This allows nodes in the network to verify that their own data and the data of the previous block are consistent with the corresponding hash value, ensuring that the data cannot be tampered with. In addition, to address the potential malicious behavior of nodes in an untrusted network, a Byzantine fault-tolerant consensus mechanism is used. This mechanism ensures that even if there are a small number of malicious nodes in the network, the data consistency in the network can still be maintained [29]. Due to these features, the blockchain network ensures fairness, security, and reliability of financing transactions.

Transitive signature

Micali and Rivest [30] introduced the concept of transitive signatures in 2002 with the aim of being able to authenticate the transfer closure $G^{'}=(V,E^{'})$ of dynamically growing graphs $G=(V,E)$ (where V is the set of nodes, E and $E^{'}$ is the set of edges), thus enabling the signing of binary relations with transferable properties, as opposed to standard digital signatures, whose main feature is to reflect the transitivity. A transitive signature scheme generally consists of a 4-tuple (Ks, Kp, M, S)and four algorithms (TKG, $TSign$, TVf, $Comp$), where Ks is the private key space, Kp is the public key space, M is the explicit space (a transitive binary relation on a set), and S is the signature space. The four algorithms are defined as follows:

$TKG : \{0,1\}^k \rightarrow Ks \times Kp$ is a random algorithm used to generate a key, input1^k, output key pair(tsk, tpk), where k is the security parameter, tpk is the public key, tsk is the private key.

$Sign : Ks \times M \rightarrow S$ is a signature algorithm, which can be deterministic or random, input private key tsk and to be signed m, output signature σ_m.

$TVf : Kp \times M \times S \rightarrow \{0,1\}$ is a signature verification algorithm, which is deterministic, input the public key tpk, the signed message m and the signature σ,when σ is a valid signature of m, the output is 1, otherwise the

output is 0. $Comp : Kp \times M \times S \rightarrow \{S, \perp\}$ is a signature synthesis algorithm, which is deterministic, and the public key *tpk* is entered to sign the message m_1,m_2 and the signature σ_1,σ_2. whenσ_1 and σ_2 are valid signatures, the signature σ obtained by the synthesis operation is output, otherwise, $\perp$ is output.

Blockchain-based transitive trust model for supply chain finance

In this section, a specific blockchain-based transitive trust model for SCF is presented. Firstly, a general framework is proposed to use blockchain technology as the basis of trust transfer for all parties in the supply chain. Secondly, the comprehensive trust value of suppliers is calculated to select suppliers with high trust as partners. Thirdly, a transitive signature mechanism is used to ensure that the credit of the core enterprise is reliably transferred to the underlying n-level suppliers.

General framework of supply chain finance under blockchain technology

The decentralization, openness, independence and security features of blockchain provide new ideas for solving SCF. In this paper, we presents an enhanced version of consortium chain, which ensures a high level of control and security by involving suppliers, core enterprises, and financial institutions as active participants. Leveraging the unique characteristics of this consortium chain, it establishes a reliable data exchange and storage system for business and trade data of key subjects, such as core and upstream enterprises in the SCF domain. By combining trust calculation as the foundation for transitive trust, the system calculates the trust value of each supplier. Suppliers with a high trust value are then issued negotiable commercial certificates, using digital creditor credentials as the carrier. To ensure the credibility and legitimacy of these certificates, they are verified by each stage's suppliers through transitive signatures. Additionally, this mechanism implements a verification process for merchant certificates at each stage, ensuring their authenticity and legitimacy through transitive signatures. By employing this trust calculation and transitive signature-based approach, not only can SMEs and financial institutions effectively engage in factoring financing within the SCF, but it also encourages all parties involved to establish a "technological trust" system utilizing blockchain technology. This system guarantees traceability, transparency, and verifiability of transactions

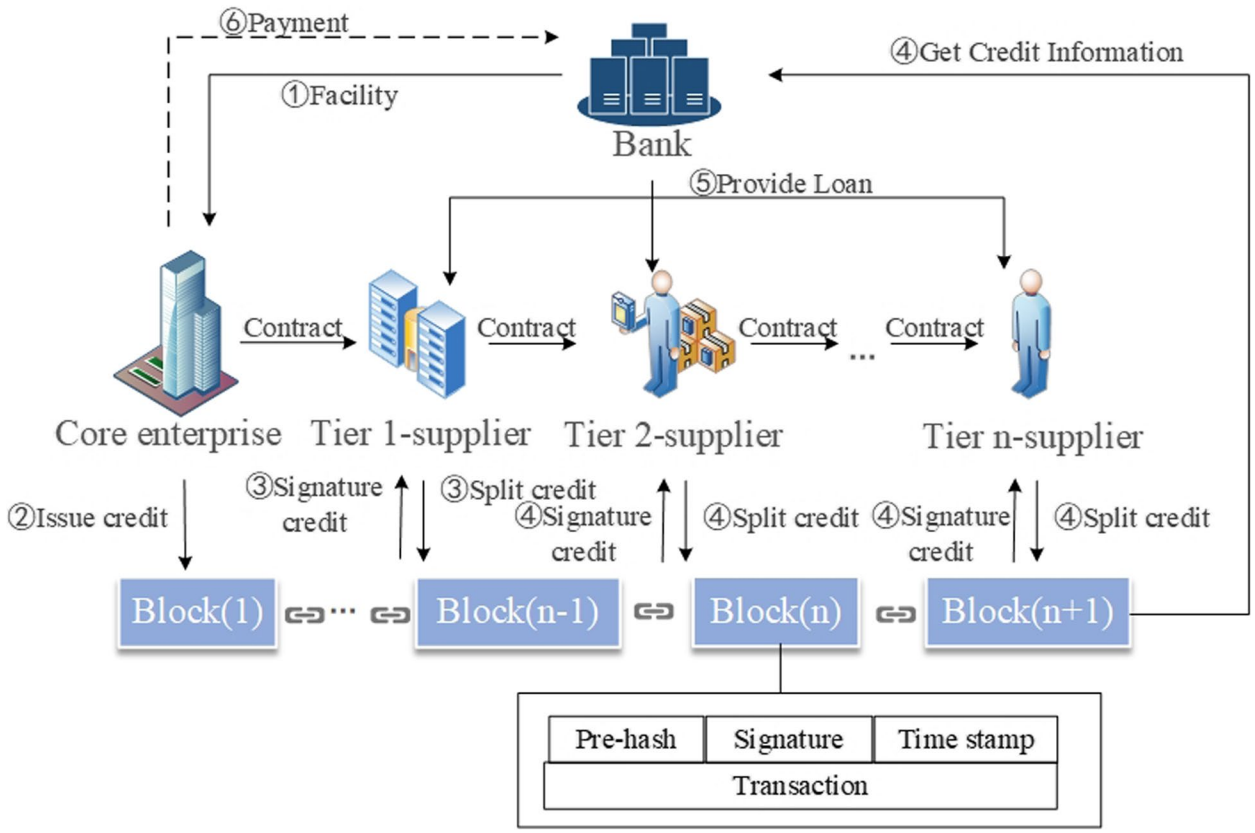

Fig. 1 Blockchain-based SCF general framework diagram

within the supply chain, consequently mitigating potential risks and minimizing instances of fraud. The general framework of blockchain-based supply chain financing is shown in Fig. 1.

The business process of blockchain-based supply chain financing is as follows.

(1) The financial institution grants a reasonable financing amount to the core enterprise.
(2) The core enterprise and the first-tier supplier reach a supply agreement and sign a contract, and the core enterprise electronicizes its accounts payable to form a negotiable certificate stored in the alliance chain with digital debt credentials as the carrier.
(3) The first-tier supplier receives the digital debt voucher from the core enterprise and verifies the authenticity of the voucher with its private key, and after determining that it is correct, it signs on the voucher and splits the merchant certificate and broadcasts it in the alliance chain network.
(4) The secondary supplier then verifies the authenticity of the credential with its private key and signs the credential after being signed and certified by the primary supplier, and keeps repeating this step until the primary supplier.
(5) The financial institution verifies the transaction information of the merchant certificate on the blockchain with its private key and confirms the authenticity before issuing loan operations to each supplier.
(6) The core enterprise and the bank will clear the payment and complete the financing of this supply chain.

The central business entity and the bank collaborate to facilitate payment, thereby finalizing the supply chain finance. The division of merchant certificates and the intricate business processes within the financing procedure are meticulously documented in the blockchain ledger. This results in the establishment of a dependable, traceable, and tamper-resistant accounting model, significantly enhancing the reliability of trust transmission in the realm of supply chain finance.

Trust computing

Within a supply chain network, the trust dynamics between enterprises are subject to numerous influencing factors. Consequently, there arises a need for a fair and impartial measure to reinforce the trust connections among these enterprises. The comprehensive trust evaluation is based on the aggregation of the cumulative evaluation of each enterprise's behavior. The trust model can be used to analyze the trust level of enterprises from multi-dimensional evaluation, and then judge their cooperation possibility and access conditions to the chain. In this way, on the one hand, those enterprises with higher trustworthiness can be motivated to continue their good communication behaviors; on the other hand, those enterprises with lower trustworthiness can be punished to prevent them from continuing their bad communication behaviors. When the overall trust level of an enterprise drops to an extremely low level, it is mandatory to deprive the enterprise of its legal status in the current supply chain network to avoid serious consequences of its malicious behavior.

In the trust network, according to the different interactions between trust nodes, the trust between suppliers can be calculated by direct trust, indirect trust, and incentive trust to obtain the final comprehensive trust value. Among them, the comprehensive trust evaluation (V) model of suppliers is shown in formula (1):

$$V = \mu * DT + \nu * RT + \gamma * ET \tag{1}$$

where DT is the direct trust, RT is the recommendation trust, ET is the incentive trust evaluation part of the first supplier, when the supplier in the first round of trading process to do honest behavior, positive feedback, will get a certain amount of reward trust, when it carries out negative or malicious behavior, will deduct the corresponding trust. The weights of each indicator μ, ν, γ respectively, $\mu + \nu + \gamma = 1$.

Direct trust computing

In the supply chain finance network, the historical behavior of the number of historical transactions between suppliers is statistically significant and has a great impact on the behavior that suppliers may take in the future. Therefore, this paper uses Bayesian Statistics to calculate the direct trust value of suppliers. The trust between suppliers usually obeys *Beta* probability distribution, and the two parameters α and β, respectively the number of successful and unsuccessful transactions between suppliers, can be used for trust value estimation. The distribution can be defined by the function, formula (2) as follows:

$$f(p|\alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1}(1-x)^{\beta-1} \tag{2}$$

From formula (2), we can see that its direct trust value (DT) is the expected value of the *Beta* distribution, that is, formula (3):

$$DT = \frac{\alpha}{\alpha + \beta} \tag{3}$$

Among them, α and β are positive numbers greater than 0 and the initial value is 1, which also means that

when supplier i and supplier j have no historical interaction information, the direct trust degree of the two is 0.5 by default.

Recommended trust computing

Recommended trust refers to the trust generated by the recommendation of others between two non-adjacent nodes, also known as indirect trust. Financial institutions can gain indirect trust in the target company through the recommendation of the core company or other suppliers in the supply chain. Clausius' law of entropy describes the direction in which the energy of a closed system is transformed, i.e., the energy of a closed system can only irreversibly develop in the direction of decay. Entropy is capable of comprehensively considering the uncertainties associated with multiple factors, capturing variations in information distribution, and delivering precise measurements. Its robust interpretability empowers the enhancement of trust management strategies. Hence, the selection of entropy as an evaluation index can furnish a comprehensive, accurate, and highly practical trust metric, thereby fostering the establishment of trust and facilitating trust recommendations. This paper uses entropy as the evaluation index of recommendation trust, as shown in formula (4):

$$H(p) = -plog_2 p - (1-p)log_2(1-p) \tag{4}$$

p represents the probability of mutual trust between suppliers, and the proportion of information gain provided by each layer of nodes as the weight of node recommendation trust. From Eq. (5), the recommended trust (RT) is:

$$RT = \begin{cases} 1 - H(p), 0.5 \le p \le 1 \\ H(p) - 1, 0 \le p < 0.5 \end{cases} \tag{5}$$

Incentive trust calculation

Incentive trust evaluation evaluates the behavior of the node. Based on the behavior of the node in each round of consensus process in the request cycle, combined with the trust degree of the node, the node is evaluated with corresponding rewards and punishments. The incentive evaluation ET of the node can be expressed as formula (6):

$$ET = \begin{cases} sin\frac{(1-V_{k-1})\pi}{2}, Honest \\ sin\frac{(-V_{k-1})\pi}{2}, Negative \end{cases} \tag{6}$$

Among them, V_{k-1} is the trust degree of the node after the last round of transaction. For a node with a high degree of trust, when it does honest behavior, the trust reward it obtains is lower than that of a node with a low trust. At the same time, when a node with a high degree of trust makes a mistake, its trust penalty is greater. Therefore, it can avoid the concentration of power of high-trust nodes and encourage nodes to act honestly.

Vendor receivables merchant certificates based on transitive signature

In the traditional model for accounts receivable financing in the supply chain, the transmission of trust through commercial acceptances, which is the core element, cannot be divided, making it difficult for the commercial credit of the core enterprise to be transmitted. However, the blockchain supply chain financing model allows for suppliers within the same alliance chain to use comprehensive credit calculations to screen out suppliers with high credit. Then, the core enterprise issues accounts payable with a signature broadcast on the whole network. Each supplier in the supply chain gradually verifies and transmits the accounts payable certificates through transferable signatures. Because transactions need to be verified by the entire chain before they can be recorded in the blockchain, the credit certificates are tamper-proof and traceable. If the signature is verified, it is equivalent to obtaining direct credit endorsement from the core enterprise, thereby promoting multi-level supplier financing and broadening the scope of supply chain services while improving the efficiency of whole-chain financing.

Supplier's receivables merchant certificate validation is a graph-based validation structure. Here, we define $G = (V, E)$ as an directed graph, where $V \subseteq N$ is a finite set of vertices and $E \subseteq V \times V$ is a finite set of edges. Based on the equivalence relation, the graph $G = (V, E)$ decomposed into several equivalence classes $D(V) = V_1, V_2, ..., V_m$, where $m = |D(V)|, G = (V, E)$, where $V = V$ and $(i, j) \in E$, denote the existence of V a transfer closure in the path from V_i to V_j. Due to the transferability of the graph ($G = (V, E)$), verification G is equivalent to G validation. Its passable signature algorithm is shown below. The flowchart of the algorithm is shown in Fig. 2.

(1) System parameters and settings.

$TKG : (tpk, tsk) \leftarrow TKG(1^k)$ is given a security parameter 1^k, according to the key generation algorithm (KG) to return a public and private key pair (tpk, tsk).

(2) Signature algorithm.

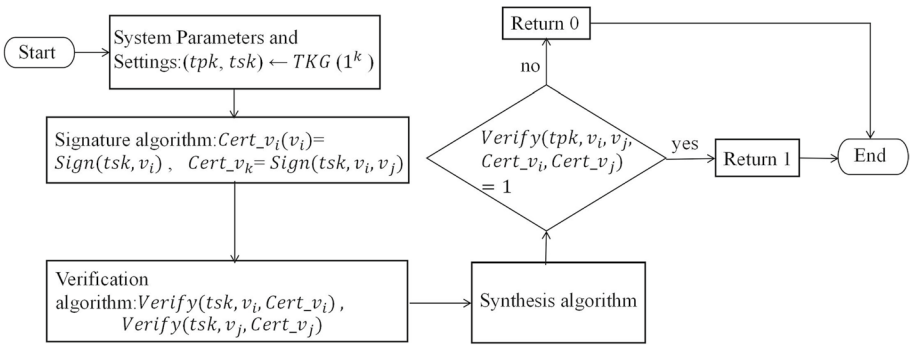

Fig. 2 Flowchart of transitive signature algorithm

Tsign: The signature algorithm includes the following three algorithms: $TAsign-Init$,$TAsign-Node$,$TAsign-Edge$.

1) $Cert(v_i) \leftarrow TAsign-Init(tsk, G)$: The core enterprise signs with the private key *tsk* it owns and the transitive closed graph $G=(V,E)$ where it is located. This signature initialization algorithm ($TAsign-Init$) will return the certificate $Cert(v_i)$,where $v_i \in V, i=1,2,...,N$,$N=|G|$.

2) $Cert(v_k) \leftarrow TAsign-Node(tsk, v_k)$: The next level provider will sign with its private key *tsk* and the provider node v_k, using the signing node update algorithm ($TAsign-Node$) to return the certificate(v_k) of the provider node *k*.

3) $Cert(v_k) \leftarrow TAsign-Edge(tsk, v_i, v_j)$: The private key *tsk* of the underlying provider and the nodes v_i ,v_j, return the updated certificate (v_k) with graph $G=(V,E)$ using the signature edge update algorithm ($TAsign-Edge$), where $v_k \in V_0, k=1,2,...,N, N=|G_0|$.

(3)Verification algorithm.

Given the public key of the core enterprise, vendors v_i ,v_j and the corresponding signatures $Cert(v_i)$,$Cert(v_j)$, this verification (*TAVef*) algorithm returns 1 or 0. If 1 is returned, the nodes v_i,v_j are in the same equivalence class.

(4)Synthesis algorithm.

The accounts receivable merchant certificate passable signature scheme is consistent. The consistency property that *TASign* must be accepted by *TAVef* when and only when the nodes v_i,v_j are in the same equivalence class. That is, $Pr[[TAVerf(tpk, v_i, v_j), TAsign(tsk, v_i), TAsign(tsk, v_j)] = 1] = 1$

Scheme analysis

In this subsection, the proposed model will be analyzed from the safety point of view, and the proposed model will be analyzed by simulation experiments using data to verify the reasonableness and correctness of the model.

Security analysis

For the blockchain-based trust transferable model of supply chain financing proposed in this paper, the transferable signature can efficiently authenticate the dynamically growing graph data, and its security is built on the discrete logarithmic difficulty problem (*DLP*).

Theorem 1 *If it is difficult, then our proposed vendor receivables merchant certificate based on passable signatures is secure under adaptive selection message attacks.*

Proof

Assume that there exists a polynomial-time adversary B attacking a vendor receivable merchant certificate based on a passable signature with advantage $adv_B(k)$ and there is a polynomial-time adversary A with a public key pk that can be exploited to B forge the signature with advantage $adv_A(k)$.The goal of A is to create a valid signature (v_i,v_j),A set one $tpk=pk$,and randomly select a prime number q, and then send (tpk, q) to B. Use $V^{'}=V_1^{'}, V_2^{'}, ..., V_m^{'}$,$M=|V^{'}|$. as the set of vertices for the query,Δ as the set of node signatures storing all queries, and T as the common label table storing all choices. A perform the following operations.

1) If both v_i and v_j are not in $V^{'}$, then $m=m+1, V_{m+1} \leftarrow v_i, v_j$ as well $V^{'} \leftarrow V^{'} \cup V_{m+1}$. Randomly select $x_0 \leftarrow Z_q^*, y_0 \leftarrow Z_q^*$,$v_i$ to obtain the common edges of nodes (x_0, y_0),where $(x_0, y_0) \notin T$. Then update $T \leftarrow T \cup (x_0, y_0)$,randomly select $r_0 \leftarrow Z_q^*$, calculate $x_1 \leftarrow r_0 \cdot x_0 \bmod q, y_1 \leftarrow r_0 \cdot y_0 \bmod q$, and v_j obtain the common edges of the nodes (x_1, y_1).

2) If both v_i or v_j is in $V^{'}$, then $V^{'} \leftarrow V^{'} \cup v_j$ (or $V^{'} \leftarrow V^{'} \cup v_i$). Since v_i or v_j has always been an

equivalent class of $V^{'}$, you can assume that the common edge of v_i or v_j is (x_0, y_0), randomly select $r_0 \leftarrow Z_q^*$, calculate $x_1 \leftarrow r_0 \cdot x_0 \bmod q, y_1 \leftarrow r_0 \cdot y_0 \bmod q$, and obtain the common edge of the node v_i or (v_j) (x_1, y_1).

3)If both v_i and v_j are in $V^{'}$, A search for certificates $Cert(v_i)$ on v_i and $Cert(v_j)$ on v_j from Δ respectively.

4)A return $Cert(v_i), Cert(v_j)$ to B.

Finally, B forge a signature $_{Cert(v_i^*), Cert(v_j^*)}$ on the edge v_i^*, v_j^*. Let $G^{'} = (V^{'}, E^{'})$ be the graph consisting of edge queries and vertex queries from B,and $\widetilde{G^{'}} = (V^{'}, E^{'})$ is the transitive closure of $G^{'}$.$Cert(v_i^*), Cert(v_j^*)$ is considered to a valid signature if the following conditions are met:

1) $TAVef(v_i^*, Cert(v_i^*), Cert(v_j^*)) = 1$, that is: $Verf(tpk, x(v_i^*), y(v_i^*)) = 1$, $Verf(tpk, x(v_j^*), y(v_j^*)) = 1$ and $x(v_i^*) \cdot y(v_j^*) = x(v_i^*) \cdot y(v_j^*) \bmod q$.

2)At least one node is not in $\widetilde{G^{'}}$ between nodes v_i^* and v_j^* ,and then A outputs a solution $(x(v_i^*), y(v_j^*))$ to the A's challenge.

$$Adv_A(k) \geq Adv_B(k)$$

In summary, an attacker cannot forge a signature through computation, and thus cannot forge a new legal signature from an existing signature. With this,we have proved Theorem 1.

Experimental analysis

This section focuses on the blockchain-based trust transferable model for supply chain financing for simulation experiments and tests. The experimental environment is as follows: *Windows*10 operating system, $InterCore - i5CPU$ processor, $8G$ system memory, $1T$ hard disk memory, and *Python*3.6 as the development language.

For the transitive trust model of supply chain financing proposed in this paper, the experiments will use the change of reputation value of suppliers as the basis of transitive trust in SCF, and illustrate the performance of the scheme by adding incentive trust calculation to select more reliable suppliers. To verify the reliability of the integrated trust value calculation, we assume the following scenario: there are 100 suppliers in the whole supply chain and set 5 - 20 low reputation suppliers.

Firstly, we analyzed the initial trust value of suppliers. The initial trust value serves as a fair starting point for all suppliers. When the initial trust value is small, it becomes time-consuming to differentiate between low-credit suppliers and good-credit suppliers. On the other hand, when the initial trust value is large, it takes more time for low-credit suppliers to decrease their trust value, thereby prolonging the identification process for low-credit suppliers. Consequently, setting the initial trust value to 0.5 strikes a balance. It allows suppliers to acquire a certain level of trust initially while facilitating a faster reduction in trust value for low-credit suppliers and providing good-credit suppliers with an opportunity for accelerated trust growth. This approach is better suited for effectively distinguishing between low-credit suppliers and good-credit suppliers. We observe that the change of trust value of low reputation suppliers and high reputation suppliers with the number of interactions is shown in Fig. 3, with the increase of the number of interactions, the integrated trust value of good reputation suppliers keeps increasing and the integrated trust value of low reputation suppliers keeps decreasing.

Secondly, according to the comparative analysis of the comprehensive calculation of supplier trust value, with the increase of the number of interactions, the comprehensive trust value calculated by weighting is higher than the trust value calculated by direct trust and recommendation trust, meanwhile, the incentive trust value calculated by each transaction will increase the trust of suppliers and improve their comprehensive trust value, as shown in Fig. 4. This indicates that the integrated trust can be a better fit for the trust of suppliers and form a positive feedback mechanism. The more the number of interactions among suppliers, the higher the trust degree of mutual cooperation among them, the higher the trust degree of enterprises in supply chain transactions, and the higher the possibility of financial institutions to provide financing support, which is more reliable as the basis for trust transmission.

Finally, compared to the trust calculation proposed in the literature Jiang et al. [24], this paper adds an incentive trust calculation to the integrated trust calculation, so that the model will update the trust value with the performance of the transaction after each interaction, and the integrated trust value is more optimized. In addition, since the model also incorporates a transferable signature mechanism, the trustworthiness of the model is further increased as each vendor will be able to verify the authenticity of the transaction compared to the scheme proposed in Jiang et al. [24]. For generality, 10 supplier nodes with an initial reputation value of 0.5 are taken to simulate a comparative analysis of trust value transfer in the supply chain. As can be seen in Fig. 5, the trust value received by the supplier at the bottom end of the trust is lost to a small extent compared to the original trust value by our model, which is more prominent when the number of supplier nodes increases compared to Jiang et al. [24].

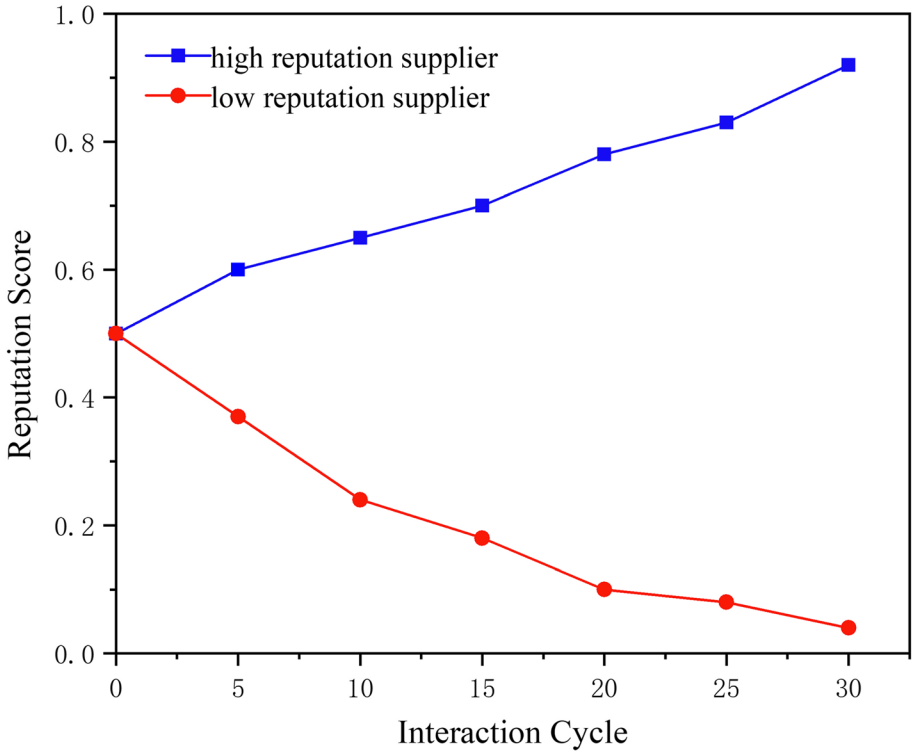

Fig. 3 Changes in supplier reputation with the number of interactions

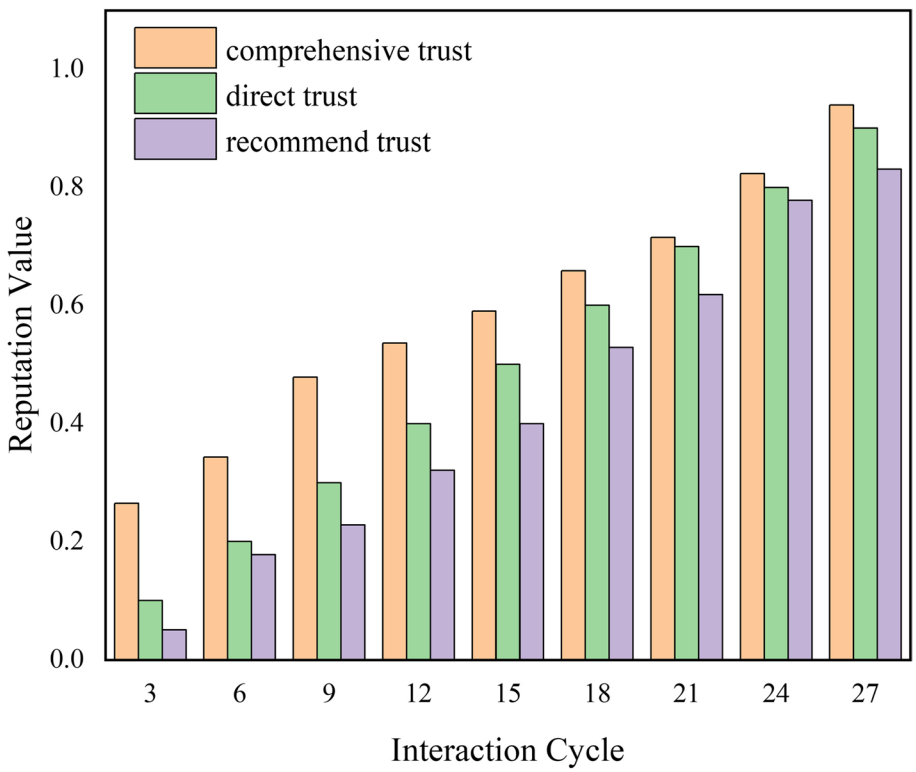

Fig. 4 The change of comprehensive trust value, direct trust value and recommended trust value with the number of interactions

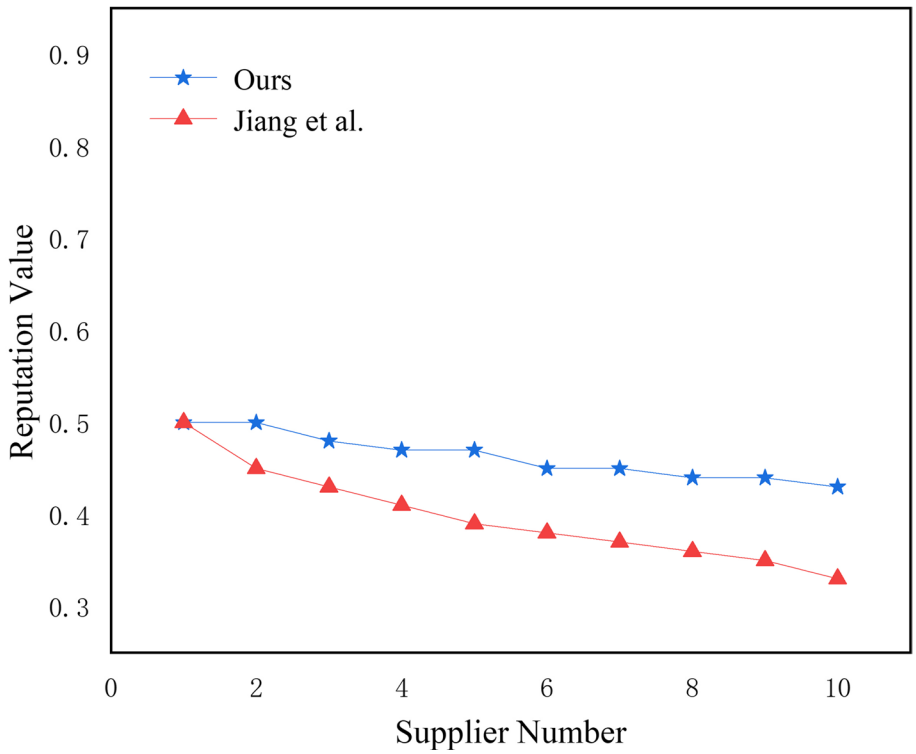

Fig. 5 Trust transfer graph with reputation value increasing with the number of suppliers

Table 1 Performance comparison of different models

Scheme	Trust computing	Trust value transmission ability	Signature security
Jiang et al. [24]	Excellent	Good	Not involved
Ours	Good	Excellent	Excellent

Furthermore, we present the performance comparison of our proposed transitive trust model in Table 1. We analyze the strengths and weaknesses of the transferable trust model from three perspectives: trust value calculation, trust value transmission ability, and signature security. Jiang et al. [24] approach employs fuzzy algorithms, allowing them to achieve optimal performance in certain individual metrics but disregarding other performance aspects. In contrast, our algorithm emphasizes trust transitivity. Although the transitive trust model may fall slightly behind in terms of a single metric, its overall performance remains at a high level. It is noteworthy that the transitive trust model exhibits no apparent drawbacks, leading to its superior comprehensive performance.

Conclusion

We propose a blockchain-based transitive trust model for SCF in this paper. The model quantifies trust transferability by calculating the direct trust value, recommended trust value, and incentive trust value of suppliers in the supply chain, allowing for the selection of suppliers with good credit as the basis for trust transferability in the network. Additionally, the transitive signature mechanism based on graph data optimizes the problem of difficult trust transfer to tail-end enterprises and reduces the number of verification query returns, resulting in fewer network communication interactions. Furthermore, the transitive signature mechanism ensures data integrity by safeguarding it against tampering or damage during transmission through the use of digital signatures. This mechanism facilitates trust transmission and verification, enabling the seamless flow of trust between nodes within the supply chain network. Security and performance analyses indicate the effectiveness and feasibility of the model for transitive trust in SCF.

While the transitive signature mechanism employed in the proposed model can enhance the trust transfer reliability of each participant in the supply chain network, ensuring the privacy of enterprise orders in trusted SCF and promoting mutual cooperation among the chain parties remain important topics that require further in-depth research. These issues represent key research directions for the future.

Acknowledgements
We sincerely thank the people who supported us in doing this work. At the same time, we sincerely thank the editors and reviewers for their constructive comments on this paper.

Authors' contributions
Chang Shu wrote the main manuscript text, Chaoyue Tan and Yun Luo prepared figures, Yuling Chen and Hui Dou provided helpful suggestions and revised the manuscript. All authors reviewed the manuscript.

Funding
This research was supported by Foundation of National Natural Science Foundation of China (61962009 and 62202118), and Natural Science Foundation of Shandong Province (ZR2021MF086), and Top Technology Talent Project from Guizhou Education Department ([2022]073).

Declarations

Competing interests
The authors declare no competing interests.

Received: 16 October 2023 Accepted: 25 November 2023
Published online: 02 January 2024

References

1. Sinha D, Roy R (2020) Reviewing cyber-physical system as a part of smart factory in industry 4.0. IEEE Eng Manag Rev 48(2):103–117
2. Du M, Chen Q, Xiao J, Yang H, Ma X (2020) Supply chain finance innovation using blockchain. IEEE Trans Eng Manag 67(4):1045–1058
3. Ma HL, Wang Z, Chan FT (2020) How important are supply chain collaborative factors in supply chain finance? a view of financial service providers in china. Int J Prod Econ 219:341–346
4. Wu S, Shen S, Xu X, Chen Y, Zhou X, Liu D, Xue X, Qi L (2022) Popularity-aware and diverse web apis recommendation based on correlation graph. IEEE Trans Comput Soc Syst 10(2):771–782
5. Qi L, Lin W, Zhang X, Dou W, Xu X, Chen J (2022) A correlation graph based approach for personalized and compatible web apis recommendation in mobile app development. IEEE Trans Knowl Data Eng 35(6):5444–5457
6. Wang Y, Qi L, Dou R, Shen S, Hou L, Liu Y, Yang Y, Kong L (2023) An accuracy-enhanced group recommendation approach based on dematel. Pattern Recogn Lett 167:171–180
7. Dai H, Yu J, Li M, Wang W, Liu AX, Ma J, Qi L, Chen G (2022) Bloom filter with noisy coding framework for multi-set membership testing. IEEE Trans Knowl Data Eng 35(7):6710–6724
8. Yang C, Xu X, Zhou X, Qi L (2022) Deep q network-driven task offloading for efficient multimedia data analysis in edge computing-assisted iov. ACM Trans Multimed Comput Commun Appl 18(2s):1–24
9. He Q, Tan S, Chen F, Xu X, Qi L, Hei X, et al (2023) Edindex: enabling fast data queries in edge storage systems. In: Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval. Tai Wan, China, p 675–685. https://doi.org/10.1145/3539618.3591676
10. Xu X, Fang Z, Qi L, Zhang X, He Q, Zhou X (2021) Tripres: Traffic flow prediction driven resource reservation for multimedia iov with edge computing. ACM Trans Multimed Comput Commun Appl 17(2):1–21
11. Jia Y, Liu B, Dou W, Xu X, Zhou X, Qi L, Yan Z (2022) Croapp: a cnn-based resource optimization approach in edge computing environment. IEEE Trans Ind Inform 18(9):6300–6307
12. Li Z, Xu X, Hang T, Xiang H, Cui Y, Qi L, Zhou X (2022) A knowledge-driven anomaly detection framework for social production system. IEEE Trans Comput Soc Syst. 2022. https://doi.org/10.1109/TCSS.2022.3217790
13. Xu X, Gu J, Yan H, Liu W, Qi L, Zhou X (2022) Reputation-aware supplier assessment for blockchain-enabled supply chain in industry 4.0. IEEE Trans Ind Inform 19(4):5485–5494
14. Li T, Chen Y, Wang Y, Wang Y, Zhao M, Zhu H, Tian Y, Yu X, Yang Y (2020a) Rational protocols and attacks in blockchain system. Secur Commun Netw 2020
15. Li T, Chen Y, Wang Y, Wang Y, Zhao M, Zhu H, Tian Y, Yu X, Yang Y (2020) Rational protocols and attacks in blockchain system. Secur Commun Netw 2020:1–11
16. Li T, Wang Z, Chen Y, Li C, Jia Y, Yang Y (2022) Is semi-selfish mining available without being detected? Int J Intell Syst 37(12):10576–10597
17. Chen Y, Sun J, Yang Y, Li T, Niu X, Zhou H (2022) Psspr: a source location privacy protection scheme based on sector phantom routing in wsns. Int J Intell Syst 37(2):1204–1221
18. Chen J, Cai T, He W, Chen L, Zhao G, Zou W, Guo L (2020) A blockchain-driven supply chain finance application for auto retail industry. Entropy 22(1):95
19. Francisco K, Swanson D (2018) The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics 2(1):2
20. Cong LW, He Z (2019) Blockchain disruption and smart contracts. Rev Financ Stud 32(5):1754–1797
21. Malik S, Dedeoglu V, Kanhere SS, Jurdak R (2019) Trustchain: Trust management in blockchain and iot supported supply chains. In: IEEE International Conference on Blockchain (Blockchain). Atlanta, p 184–193
22. Zhaofeng M, Lingyun W, Xiaochang W, Zhen W, Weizhe Z (2019) Blockchain-enabled decentralized trust management and secure usage control of iot big data. IEEE Internet Things J 7(5):4000–4015
23. Chen Y, Li Y, Chen Q, Wang X, Li T, Tan C (2023) Energy trading scheme based on consortium blockchain and game theory. Comput Stand Interfaces 84:103699
24. Jiang R, Kang Y, Liu Y, Liang Z, Duan Y, Sun Y, Liu J (2022) A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance. Int J Prod Econ 247:108469
25. Chen Y, Dong S, Li T, Wang Y, Zhou H (2021) Dynamic multi-key fhe in asymmetric key setting from lwe. IEEE Trans Inf Forensic Secur 16:5239–5249
26. Ren Y, Huang D, Wang W, Yu X (2023) Bsmd: A blockchain-based secure storage mechanism for big spatio-temporal data. Futur Gener Comput Syst 138:328–338
27. Cai X, Deng Y, Zhang L, Shi J, Chen Q, Zhen W, Guo M (2021) The principle and core technology of blockchain. Chin J Comput 44(1):84–131
28. Zheng P, Xu Q, Zheng Z, Zhou Z, Yan Y, Zhang H (2021) Meepo: Sharded consortium blockchain. In: IEEE 37th International Conference on Data Engineering (ICDE). Chania, p 1847–1852
29. Li W, Feng C, Zhang L, Xu H, Cao B, Imran MA (2020) A scalable multi-layer PBFT consensus for blockchain. IEEE Trans Parallel Distrib Syst 32(5):1146–1160
30. Micali S, Rivest RL (2002) Transitive signature schemes. In: Preneel B (ed) Topics in Cryptology — CT-RSA 2002, vol 2271. Berlin. https://doi.org/10.1007/3-540-45760-7_16

Publisher's Note