Ma et al. Cybersecurity (2019) 2:5
https://doi.org/10.1186/s42400-019-0022-2

Cybersecurity

RESEARCH Open Access

The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance

Chaoqun Ma, Xiaolin Kong, Qiujun Lan* and Zhongding Zhou

Abstract

Blockchain technology ensures that data is tamper-proof, traceable, and trustworthy. This article introduces a well-known blockchain technology implementation—Hyperledger Fabric. The basic framework and privacy protection mechanisms of Hyperledger Fabric such as certificate authority, channel, Private Data Collection, etc. are described. As an example, a specific business scenario of supply chain finance is figured out. And accordingly, some design details about how to apply these privacy protection mechanisms are described.

Keywords: Privacy protection, Supply chain finance, Hyperledger Fabric

Introduction

China's small and middle enterprises (SMEs) account for 99% of the total number of enterprises, and provide more than 80% jobs, which is an important part of the national economy. However, due to the lack of sufficient collateral and the opaque information, it is difficult to obtain financial support from financial institutions. The problem of financing difficulties is a huge obstacle to the development of small and micro enterprises (Jiang et al. 2014; Wang 2016). Moreover, SMEs are often in a weak position in the product supply chain. Accounts receivable and advance prepayments occupy most of the liquidity of these enterprises, which undoubtedly would exacerbate their financial strain, increase the risk of capital chain broken, affect their normal operations and greatly reduce their production efficiency (Yao and Liu 2018; Zhu et al. 2016). Supply chain finance service takes the real trade background as the premise and relies on a core enterprise which effectively integrate the capital flow into the supply chain management process (Gelsomino et al. 2016; Lekkakos and Serrano 2016). Supply chain finance as a new way to solve the financing problems of SMEs would revitalize massive "dead" assets such as accounts receivable, prepayments and inventory warehouse receipts. According to the National Bureau of Statistics at the end of 2016, the net amount of accounts receivable of industrial enterprises in China was 12.68 trillion yuan. However, according to China's commercial factoring industry development report, the size of China's commercial factoring markets in 2015 was only about 200 billion yuan, and a large number of "dead" assets were still not fully revitalized. The credibility of commercial bills, core enterprises and supply chain platforms is a key obstacle.

Blockchain technology is a rapidly developing and influential innovation technology. It is an ever-increasing distribute database (DDB), also known as a distributed ledger (Pilkington 2016; Iansiti and Lakhani 2017). The DDB need multiple entities to participate and maintain. Different from traditional bookkeeping technology, it bundles a series of trading records into blocks, which connected and encrypted by cryptographic methods. The Hash value, timestamp, delivery data and other information of the previous block are embedded into the latter block. The participants in the blockchain maintain a growing long chain collectively. What they can do is only adding new records but tampering with records that have occurred. They can reach a consensus without central control. Meanwhile, they use cryptographic mechanism to ensure that transactions cannot be disavowed and tampered, and to protect the privacy of data and records as much as possible (Cachin 2016; Belle 2017). Because of its decentralized, traceable, irrevocable

* Correspondence: lanqiujun@hnu.edu.cn
Business School, Hunan University, Changsha 410082, China

and tampering nature, blockchain is expected to be the cornerstone of the trust economy in the future.

Many countries attach grant importance to the development of blockchain. For example, in May 2018, Xi Jinping, the president of China, clearly stated that "new generation of information technology represented by artificial intelligence, quantum information, mobile communications, Internet of Things, and blockchain accelerates breakthrough applications." In July 2018, the Firecoin Group, one of the world's largest cryptocurrency exchanges, launched a "blockchain+industry alliance" to upgrade and transform real economy projects through blockchain technology, and to promote the blockchain in the physical industry. Blockchain technology and the cryptocurrency economy help companies to effectively solve problems encountered in the actual development process. In this background, "blockchain+-supply chain finance" is highly valued. For example, in 2018, Ping An Group and China Foton Motor Group use the blockchain technology and electronic signatures to improve the financing efficiency of the enterprises. China Tencent Company uses the accounts receivable from the core enterprises as the underlying assets to realize the circulation of the credit certificates through the blockchain. In addition, Huawei, UF, Yixin, Bubi and other well-known Chinese companies have also put forward the "blockchain + supply chain finance" solution, achieving the weak centralization of supply chain finance, data traceable, anti-tampering.

The blockchain technology makes the transaction data credible and shareable, however, it also increases the risk of disclosing the business privacy of the enterprise. Actually, the company does not want competitors to know such information as price, cost, etc., therefore, how to effectively protect various types of data in the blockchain network system is a crucial problem. On the one hand, SMEs need supply chain financial services to solve the problem of financing difficulties and high financing costs. Blockchain technology can make transaction data irreversible, traceable, and reduce credit risk. On the other hand, supply chain financial service providers often need the business information of SMEs when they conduct credit evaluation on SMEs based on blockchain technology. At the same time, the information of each enterprise in the blockchain needs to be shared, In this process, the privacy of SMEs needs to be protected, we need an algorithm to protect privacy. Data sharing is not implemented in the traditional supply chain process. Therefore, the privacy protection requirements are different from those in the supply chain based on blockchain. In the traditional supply chain business process, some methods are used to protect privacy, such as the combination secure multiparty computation cryptography methods with risk identification algorithms from social network analysis, differential privacy, bidirectional efficiency-privacy transferable authentication protocol, public-key cryptography, symmetric encryption, message authentication codes, randomized read access control, etc. The advantages of these methods include strengthening risk identification for the supply chain network, authenticating a batch of tags with less privacy guarantees, reducing trust issues between supply chain owners and tag manufacturers, reducing computational and communication overhead, and reducing computational effort. However, these passive privacy protection methods cannot completely solve the privacy protection based on transaction information sharing (Zare-Garizy et al. 2018; Yao et al. 2016; Qi et al. 2012; Arbit et al. 2014; Lee and Park 2013; Gao et al. 2004). Hyperledger Fabric is a well-known blockchain technology implementation. This paper describes the privacy protection mechanism and their applications in supply chain finance scenarios.

About Hyperledger Fabric

In December 2015, the Linux Foundation and 30 initial companies set up a Hyperledger project to promote cross-industry blockchain technology and provide open source reference implementations for transparent, open, decentralized enterprise-level distributed ledger technology. Hyperledger Fabric has promoted the development of related protocols, specifications and standards of blockchain and distributed ledger. Fabric is one of the first programs added to Hyperledger, it was presented by IBM, DAH and other enterprises by the end of 2015, the positioning of the program is business-oriented distributed ledger platform. Hyperledger Fabric introduced rights management, and its design supports pluggable and expandable. It is the first open source project for the league chain. By August 2018, the Hyperledger has more than 250 members, including Intel, Accenture, Huawei, JD, and other well-known enterprises. Since the fabric 1.2 version already provides a mature and stable privacy protection mechanism, the subsequent solutions in this article are based on this version.

Hyperledger Fabric has a high degree of extensibility and flexibility as it is designed with a modular architecture. From an application perspective, Hyperledger Fabric is divided into four components of identity management, ledger management, transaction management, and smart contracts; from the bottom-up point of view, Hyperledger Fabric is divided into four components of member management, consensus services, chain code services, security and cryptographic services. Security is an enterprise-level blockchain concern, requiring the support of the underlying cryptography. The logical architecture of the Hyperledger fabric is shown in the Fig. 1.

Blockchain network is a typical peer-to-peer network, the peers are directly connected. Organization is the main body of the blockchain network, which includes the corresponding client application, network peer and certificate. The network peer has three categories, the main peer, the endorsement peer and the accounting peer and the sorting service peer should also be included in the network. After a transaction occurs between the network peers, the client application submits the transaction proposal to the endorsement peer, the endorsement peer simulates the execution of the proposal and endorses it, and returns the simulation execution result to the client application; the client application submits a transaction that contains the signature endorsement and the execution result of the simulation transaction to the sorting service peer, the sorting service peer sorts the transactions and generates chunks, and broadcasts the chunks to the master peer, the master peer saves the chunks to the ledger, the peers in the blockchain network except the sorting peer are synchronized according to the master peer. The specific transaction process is shown in Fig. 2.

The privacy security mechanism of Hyperledger Fabric

The privacy protection measures of Hyperledger Fabric include the following four aspects: Firstly, asymmetric cryptography and zero-knowledge proof separate the transaction data from on-chain records, protecting privacy from the underlying algorithm. Secondly, the digital certificate management service guarantees the legitimacy of the organization on the blockchain. Thirdly, the design of multi-channel separates the information between different channels. Finally, privacy data collection further satisfies the need for the isolation of privacy data between different organizations within the same channel.

In the above measures, the two most distinctive methods are the channel and privacy data collection. The channel is dedicated to the blockchain privacy protection, allowing the data on the channel to be isolated separately. The peer on the same channel shares a ledger, the transaction peer needs to obtain the recognition of the channel before it can join the channel and transact with others. The PDC (private data collection) is a collection of organizations that are authorized to store private data on a channel, and the data stored includes: (1) Private data, which implements peer-to-peer communication between authorized organizations through the Gossip protocol. The privacy data is stored in the peer's private database. (2) The hash value of private data. For private data, the peers on the channel use the hash value of the private data when sorting and writing the endorsement, as evidence of the existence of the transaction and for state validation and auditing.

For the processing of privacy data, the Hyperledger Fabric is divided into the following two scenarios: new channels are needed when the entire transaction and ledger must be kept strictly confidential to the outside members of the channel; when the transaction information and ledger need to be shared among some organizations, some of them will be able to see all the transaction data, other organizations need to know the occurrence of this transaction to verify the authenticity of the transaction, a private data collection should be established in this case. In addition, because private data is propagated through peer-to-peer rather than block, the privacy data collection is used when the transaction data must be confidential for the sorting service peer. The blockchain transaction process involving the privacy

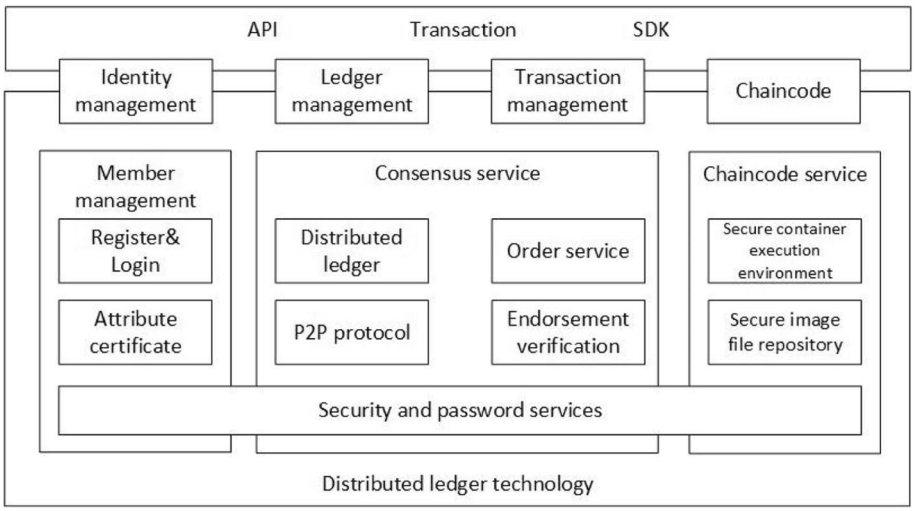

Fig. 1 System logical architecture diagram of Hyperledger Fabric (Zhang et al. 2018)

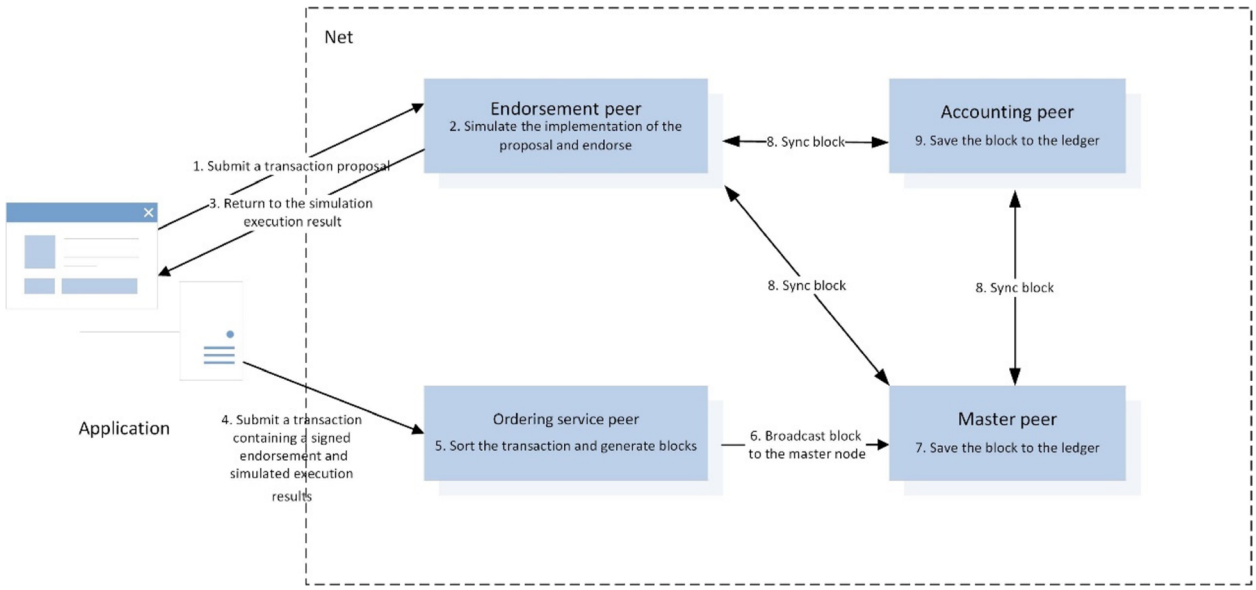

Fig. 2 Schematic diagram of the Hyperledger Fabric trading process (Zang et al. 2018)

data collection is as follows (Hyperledger 2018). Accordingly, Fig. 3 shows this process.

1. The client application submits the offer request to call the chain code function to the endorsement peer of the private data set authorization, and the private data is sent through the provisional domain in the offer.
2. The endorsement peer simulates the transaction and stores the private data in a local temporary repository in the peer. The endorsement peer disseminates the private data to the authorized peer via the gossip protocol.
3. The endorsement peer returns the public data, including the hash value of the private data key-value pair, to the client.
4. The client application submits the transaction to the sorting service peer, and the sorting result is distributed to each block. These blocks containing hash values are distributed to all peers. Each peer above the channel can use the hash of the private data to verify the transaction without knowing the exact private data.
5. When submitting a block, the authorized peer can use the collection policy to determine if it is authorized to view private data. The authorization peer will check the local temporary data store firstly to determine if it has received private data when the chaincode is endorsed. If not, they will attempt to obtain private data from other peers. It then verifies that the hash of the private data and the hash in the block's public information are consistent and commits the transaction and the block. Once authenticated or submitted, the privacy data will be transferred to a copy of the privacy state database and the privacy write repository. Privacy data will be removed from the temporary data store.

When a member of a private data collection shares private data with other organizations, such as when a member of the collection has a dispute or if they want to transfer the asset to a third party. The third party can calculate the hash of the private data and check that the hash value is consistent with the hash on the channel ledger, thus proving the existence of the transaction.

For very private data, after a period of time, the organization that shares the data hopes or requests for timely removal of the data store for policy reasons, leaving only the hash of the data as evidence that the transaction cannot be tampered with. In some cases, private data needs to be stored in the peer's privacy database until it can be replicated to a database outside of the blockchain. This data needs to be stored in the peer until the chaincode business process is used. To support subsequent transactions, once a certain number of subsequent blocks are added to the private database, the previous private data can be purged.

In addition, the Hyperledger Fabric protects privacy data including: within a channel, you can restrict the input data of a chain code to a collection of endorsements, and by using a visual data set, this visibility setting will

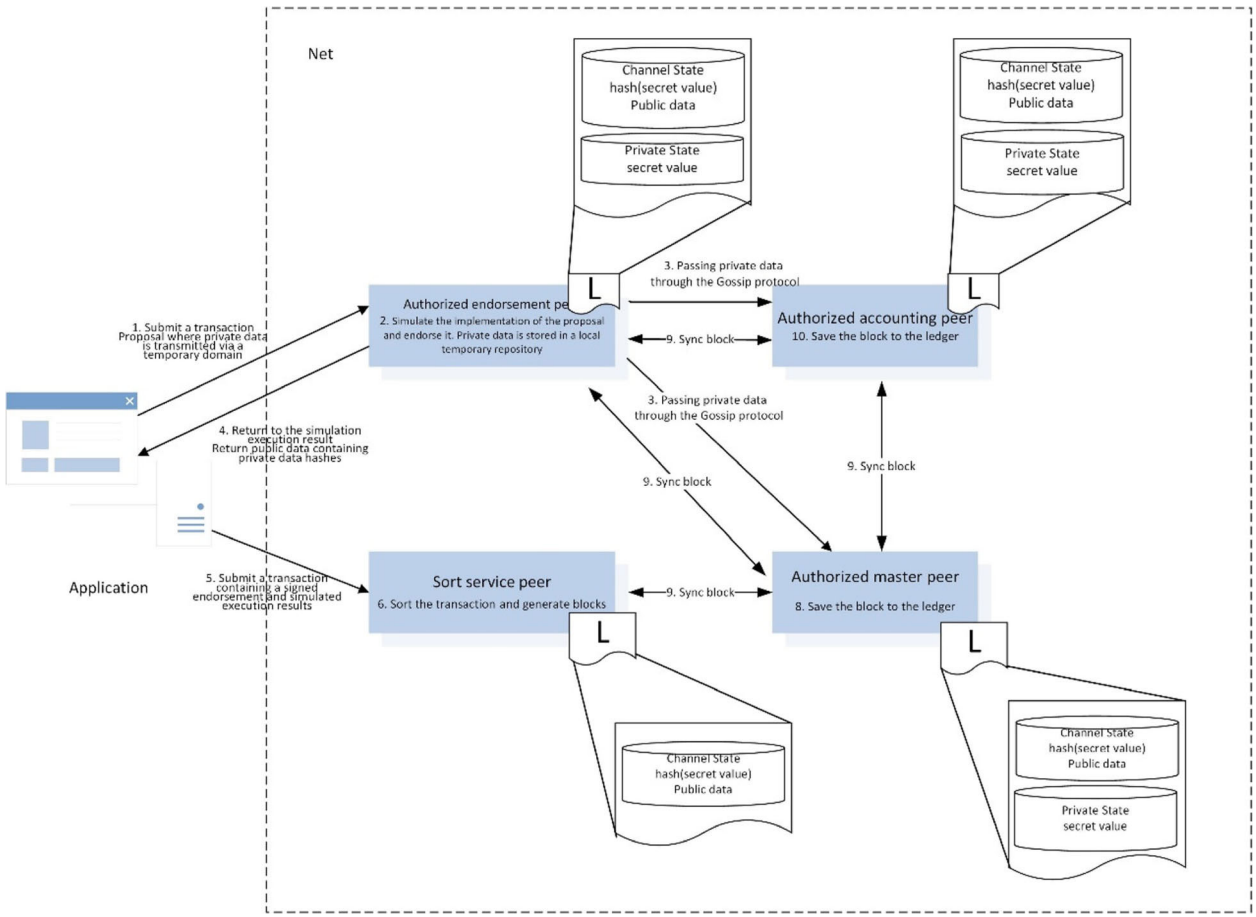

Fig. 3 Hyperledger fabric privacy protection flow

determine whether the input and output chain code data is included in the submission transaction, not just the output data; hashes and encrypts the data before calling the chain code. If the data is hashed, you need to provide a way to share the data source, and if you encrypt the data, you need to provide a way to share the decryption key. By building access control in chain code logic, you can restrict data access to certain roles in your organization; the still encrypted data can be encrypted by the file encryption system on the peer and the data in the transmission is encrypted by TLS.

Applications in supply chain finance

Business scenarios of supply chain finance

Supply chain refers to the core enterprises, starting from the supporting parts, making intermediate products and final products, and finally sending the products to the consumers by the sales network, connecting the suppliers, manufacturers, distributors and end users into one whole functional network chain structure. Supply chain finance is a typical scenario of multi-subject participation, asymmetric information, imperfect credit mechanism and non-standard scene of credit standards,

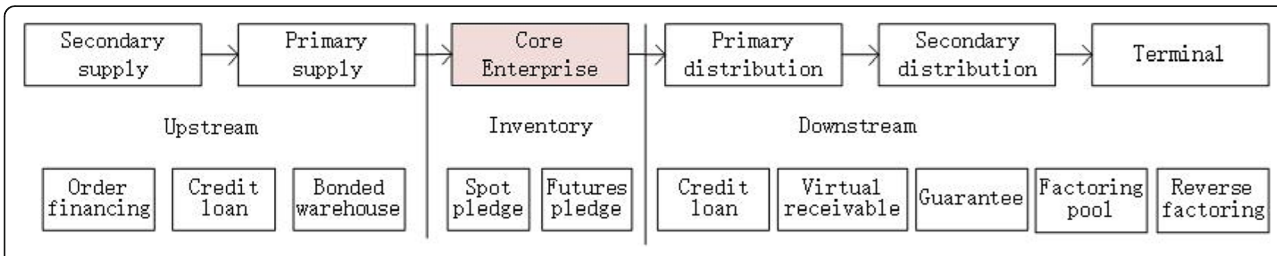

Fig. 4 Supply chain financial business process classification (WelinkData 2017)

and has a natural fit with blockchain technology. The use of blockchain technology to solve the pain in the supply chain financial industry has attracted people's attention. A typical supply chain financial scenario is shown below (Fig. 4).

In the upstream segment of the supply chain, the supplier relies on the transaction relationship with the core enterprise to obtain the credit support, including contract orders and accounts receivable, etc. In the core enterprise interval, logistics finance mainly relies on the credit of the material itself. The credit of the material relates to standardization, fluidity, pledge and salvage value, etc. Therefore, the pledge is the warehouse storage and futures generated in the circulation of bulk commodities. In the downstream section of the supply chain, it includes financial products such as credit loan, receivables pledge and so on. Most of the financial product design in the supply chain needs the documents, transaction records, credit status and other information of the enterprises in the chain. Through the blockchain technology, once the transaction is formed, the relevant data to achieve the distributed storage, which can be traced and verified, so as to alleviate the core enterprise is difficult to self-certification innocence, small and medium-sized enterprises financing difficult financing problems.

Take the example of order financing in the upstream of the supply chain. Manufacturing companies purchase raw materials from upstream raw material suppliers by purchasing and selling contracts with downstream core companies. Manufacturing companies borrow from financial institutions to pay for raw materials, and their finished and semi-finished products are monitored in third-party logistics. Sales revenue to repay bank principal and interest. However, in the actual production and operation activities, the upstream manufacturing companies are far away from the core enterprises in the production process, and it is difficult to obtain commercial papers directly related to the core enterprises. A commercial paper that has not been endorsed by a core enterprise will have the problem of financing difficulties, and the blockchain can solve this problem. Nontamperable and traceable features of data reduce billing costs and reduce financing costs. The financing of financial institutions by means of orders requires the manufacturing companies to provide transaction data, but because of the competitive relationship between manufacturing companies, there is a need for transaction privacy protection. On the one hand, the transaction price between competitors needs to be kept secret; on the other hand, the trading behavior of special industries requires privacy protection, such as military units.

In order to describe the applications of the privacy protection mechanism of Hyperledger in supply chain finance. As an example, Fig. 5 shows a specific supply chain finance scenario. There is a core enterprise, three SMEs (small or middle enterprise), two financial institutions and government departments in the product supply chain. Suppose there are two business processes, the government sector (O1), the core enterprise (O2), the financial institution A (O3), the SME A (O4) and the SME B (O5) belong to the first business process (The information propagation path is indicated by a solid line in Fig. 5); government departments (O1), core companies (O2), financial institutions B (O6), SME A (O4) and SME C (O7) belong to the second business process (Its

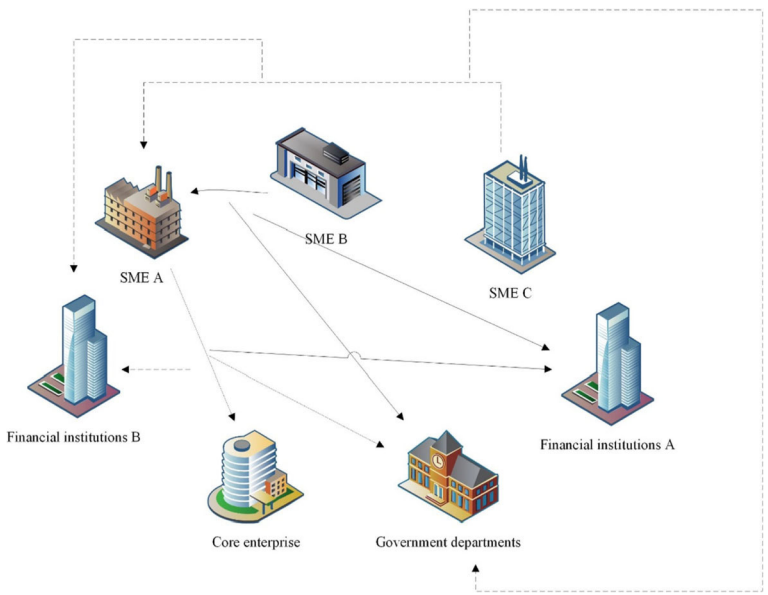

Fig. 5 Supply chain finance business scenario

information propagation path is indicated by a dotted line in the Fig. 5. Two business processes involve the transaction of information between SME A and the core enterprise.

In supply chain finance, due to the long business process and many organizations involved, the following requirements must be met for privacy protection. The business scenario is described as follows: All the above organizations have entered the blockchain network. There are two business processes. In the first business process, transactions occur SME B and SME A, other transactions occur between SME A and the core enterprise. The SME B participating in the transaction did not receive the advance payment after receiving the production order of SME A, and SME A did not receive the advance payment from the core enterprise. SME A and SME B hope to finance through relevant bills, obtain production funds from financial institution A, purchase raw materials for production。In the second business process, SME C also deals with SME A., SME B and SME C are suppliers of SME A, and there is a competitive relationship between SME B and SME C. SME A and the core enterprise generate transactions, and financial institution B provides financing services for the second business process. Government management is responsible for collecting relevant data on a regular basis and exercising statistical and supervisory duties. In summary, the following privacy protection requirements exist in these organizations on the blockchain:

(1) Data transmission is safe and reliable
(2) SME B does not want any transaction behavior between itself and SME A to be known by SME C.
(3) SME B does not want transaction data related to privacy to be passed to financial institution A and government management department in the business process, and hopes to obtain the prepayment of financial institution A by virtue of the provided non-private transaction data, the financial institution needs to obtain relevant Transaction data to determine the authenticity of the transaction and the risk of lending, the government management agencies hope to obtain relevant transaction data in order to grasp the economy.
(4) The core confidential information of each unit needs to be completely confidential.

Privacy protection design of supply chain finance

In response to the above privacy protection requirements, the financial privacy protection design of the supply chain based on Hyperledger Fabric is as follows:

(1) All organizations joining the blockchain must be authenticated at the CA to prevent illegal organizations from joining the network to steal user privacy. The viewing rights of the private data can be further subdivided. In the scenario of the league chain served by the Hyperledger, many organizational relationships on the channel are complex. Therefore, privacy data of different degrees of encryption can be given with different levels according to the nature of the transaction activity and the socio-economic relationship between the organizations. For example, organizations that directly participate in transactions can obtain fully transparent privacy data. Upstream and downstream companies associated with this transaction can obtain private data that is added with less noise. Organizations and industry associations that have little to do with the transaction can obtain statistics on transactions. However, competitors may not be able to have fully access the relevant data of this transaction.
(2) Establish different channels for different business processes. In this case, the two business processes form two channels to ensure complete separation of information between SME C and SME B. Based on the channel formed by the first business process, establish a private data set including SME B and SME A, and a private data set including SME A and core enterprise, and also in the second business process. Establishing similar collections of private data to ensure that private data is only disseminated to both parties to the transaction. Other data is provided to financial institutions for risk assessment and provided to government managements for statistical and regulatory purposes.
(3) For the core confidential information within each organization, the organization performs asymmetric encryption and transmits hash of data to the blockchain. This approach should also be part of the Hyperledger Fabric's privacy protection mechanism. In addition, the storage model for private data should be further designed. At present, Hyperledger's storage of private data is stored in the privacy database of the peer. Once the private data is copied to the database outside the chain, the linked database data will be deleted, leaving only the hash value of the private data to prove the existence of the transaction. However, this approach makes it impossible to fully exploit the traceability of the blockchain, and the final traceability is only the hash of the transaction data, which cannot be verified on the chain. Therefore, the local database should also establish a corresponding hash value of the privacy transaction data and implement mapping with the privacy database on the chain to achieve traceability based on the same hash value.

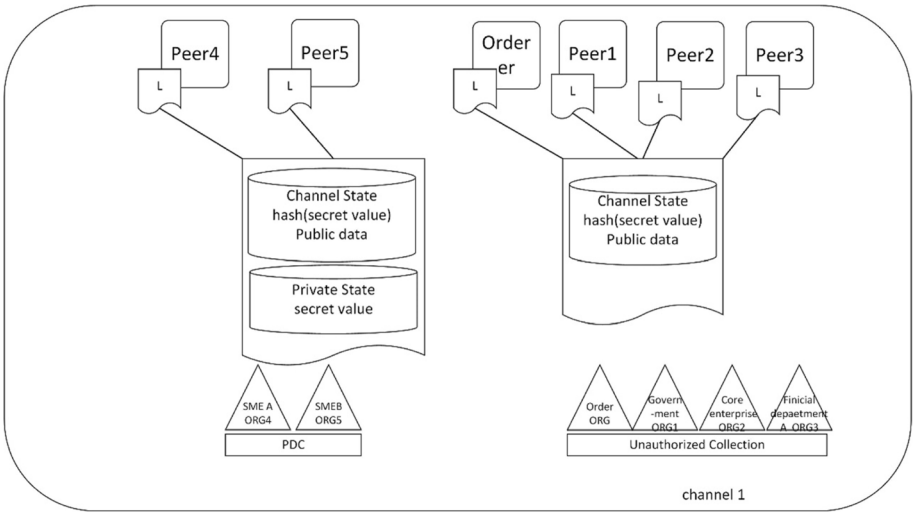

Fig. 6 PDC design in the supply chain finance scenario

(4) The data can be further encrypted according to the attributes of different login users after the privacy data is stored in the database of the organization. Even if the same client of the same organization, the person who manipulates it may be different, so it is necessary to encrypt the data to different degrees according to the attributes of the login user. For example, a supervisor in an organization has the right to view all of the data in the peer database, and visitors in the organization can only see the encrypted data. The permissions of different peers in the same organization to view data should also be different. This is an improvement direction of the privacy protection design on Hyperledger Fabric

The transaction data is divided into two parts, one part is non-confidential transaction information, the other part is the confidential data information, which belongs to privacy data. Organizations with direct production activities on the business process can form a collection of private data that can be authorized to view private data, while organizations that do not belong to the private data collection on the channel cannot see the private data and can only view the hash value of the private data. A peer authorized to obtain private data can compare the hash value of the private data calculation with the public hash value to verify the authenticity of the transaction. Based on this, the privacy data protection mechanism of the Hyperledger Fabric protects the private information in the supply chain. The privacy data collection design of SME A and SME B is shown in Fig. 6.

Compared with the traditional accounting method, the blockchain-based accounting method realizes the distributed storage of the ledger. Each peer stores the same ledger locally, so that the ledger is authenticated by multiple parties. It is difficult to be tampered with the ledger. Therefore, this way achieves decentralization. Hyperledger Fabric achieves the isolation of private data through the method of private data collection and channel. While the traditional accounting method protects the privacy by setting the login password, which has security risks, and the data is not authenticated by multiple parties. The ledger is not necessarily true. Correspondingly, Table 1 lists the differences between blockchain-based accounting method and traditional ledgers.

Table 1 Differences Between Blockchain-Based Accounting Method and Traditional Ledgers

Blockchain-Based Accounting Method	Traditional Ledgers
Decentralized; Distributed storage, each peer has the same ledger	Centralized; Each participant only saves its own ledgers
Traceable, each transaction is recorded	Untraceable, whether the transaction is recorded or not is determined by the participant
Transaction records cannot be tampered after multiple verifications	Each participant is able to modify their own ledgers
Channel and Privacy Data Collections in Hyperledger fabric are designed to protect data privacy	Protecting user's privacy with a login password
Data sharing and privacy protection are both implemented	Data sharing is not implemented

Conclusion

The blockchain has a relatively short development history, it was only used as a technology to support digital currency bitcoin in the very beginning. At present, blockchain technology has been separated from Bitcoin, and has been applied in many fields such as finance, trade, credit, Internet of things and shared economy. In the face of complex scenarios such as the privacy protection challenges of the supply chain financial business scenario, Hyperledger Fabric offers a range of solutions. Flexible combination of these privacy protection mechanisms can meet various privacy security needs.

Supply chain finance involves different participants, with a wide variety of scenarios and complex business processes. This article mainly introduces the privacy protection mechanism of the Hyperledger Fabric, and uses a supply chain financial case to explain. Our next work will be to analyze the specific privacy protection needs of different supply chain financial business scenarios, and improve the privacy protection mechanism of the Hyperledger Fabric, such as setting the viewing permission of hierarchical subdivision, improving the privacy data storage mode, etc.

Abbreviations

CA: Certificate authority; DDB: Distribute database; PDC: Private data collection; SME: Small or middle enterprise; TLS: Transport layer security

Acknowledgements

The authors are indebted to Mr. Wenxuan Long, the Hyperledger China's Community Development Manager, for providing documents on the Hyperledger, and express our gratitude to Dr. Haijie Peng, the engineer of Chuangfa Science & Technology Co., who gave some suggestions on the manuscript.

Funding

This research is supported by National Natural Science Foundation of China (71871090; 71850012) and Hunan Provincial Science & Technology Major Project (2018GK1020).

Availability of data and materials

The authors are indebted to Mr. Wenxuan Long, the Hyperledger China's Community Development Manager, for providing documents on the Hyperledger, and express our gratitude to Dr. Haijie Peng, the engineer of CCS TransFar technology Co, who gave some suggestions on the manuscript.

Authors' contributions

MC, LQ and ZZ conceived and designed the study, KX collected materials, carried out drawing and writing, MC and ZZ reviewed the manuscript, LQ edited the manuscript. All authors read and approved the manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 26 October 2018 Accepted: 15 January 2019
Published online: 30 January 2019

References

Arbit A, Oren Y, Wool A (2014) A secure supply-chain RFID system that respects your privacy. IEEE Pervasive Comput 13(2):52–60
Belle I (2017) The architecture, engineering and construction industry and blockchain technology. Digital Culture 2017:279–284
Cachin C (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol 2016.
Gao X, Xiang Z, Wang H, et al. An approach to security and privacy of RFID system for supply chain in: E-commerce Technology for Dynamic E-business, Beijing, 13–15 SEP, 2004
Gelsomino LM, Mangiaracina R, Perego A et al (2016) Supply chain finance: a literature review. Int J Phys Distrib Logistics Manage 46(4):348–366
Hyperledger (2018) A Blockchain platform for the Enterprise. https://hyperledger-fabric.readthedocs.io/en/release-1.2/. Accessed 5 Sept 2018
Iansiti M, Lakhani KR (2017) The truth about blockchain. Harv Bus Rev 95(1):118–127
Jiang J, Li Z, Lin C (2014) Financing difficulties of SMEs from its financing sources in China. J Serv Sci Manag 7(03):196
Lee Y, Park Y (2013) A new privacy-preserving path authentication scheme using RFID for supply chain management. Adv Electrical Comput Eng 13(1):23–26
Lekkakos SD, Serrano A (2016) Supply chain finance for small and medium sized enterprises: the case of reverse factoring. Int J Phys Distrib Logistics Manage 46(4):367–392
Pilkington M (2016) Blockchain technology: principles and applications. Research handbook on digital transformations 2016:225
Qi S, Lu L, Li Z et al (2012) BEST: a bidirectional efficiency-privacy transferable authentication protocol for RFID-enabled supply chain. Int J Ad Hoc Ubiquitous Comput 18(4):234–244
Wang Y (2016) What are the biggest obstacles to growth of SMEs in developing countries? – an empirical evidence from an enterprise survey. Borsa Istanbul Rev 16(3):167–76
WelinkData (2017) Division of supply chain finance model. http://info.10000link.com/newsdetail.aspx?doc=2017072090035. Accessed 21 Jan 2019
Yao X, Du W, Zhou X, Ma J (2016) Security and privacy for data mining of RFID-enabled product supply chains. In: Proceedings of the 2016 SAI Computing Conference (SAI), London, p. 1037–1046
Yao Y, Liu H (2018) Research on Financing Modes of Small and Medium-Sized Enterprises on the Background of Supply Chain Finance. In: Proceedings of 2018 International Conference on Robots & Intelligent System (ICRIS), Changsha China, 26-27 May 2018.
Garizy TZ, Fridgen G, Wederhake L (2018) A privacy preserving approach to collaborative systemic risk identification: the use-case of supply chain networks. Security and Communication Networks 2018:2018
Zhang Z, Dong N, Zhu X, Chen J (2018) Depth exploration block chain-Hyperledger's technology and application. China Machine Press, Beijing
Zhu Y, Xie C, Sun B et al (2016) Predicting China's SME credit risk in supply chain financing by logistic regression, artificial neural network and hybrid models. Sustainability 8(5):433