A Trusted Supply Chain Management System Based on Permissioned Blockchains

Rong Wang[1, a], Wei-Tek Tsai [1, a], Juan He[1, b], Can Liu [1, c], Qi Li [1, d], and Enyan Deng [2, e]

[1]Digital Society & Blockchain Laboratory, Beihang University Beijing, China;
[2]Beijing Tiande Technologies No.18 Suzhou Street, Haidian District, Beijing, China.
[a]wangrong@buaa.edu.cn, [b]tsai7@yahoo.com, [c]xiongbao_ft@163.com,
[d]liucan_1115@163.com, [e]liqi7@buaa.edu.cn, [f]deng@tiandetech.com

Abstract. At present, the supply chain system has many problems, such as a large number of scattered participants, which make it difficult to centralize management and operation. Also, it is difficult to integrate data and information, and establish trust relationships between parties. To address these problems, we propose a trusted supply chain management (SCM) system based on permissioned blockchains (BCs) to making the transaction information between alliance companies which is transparent enough to establish mutual trust. We design and develop a supply chain prototype system based on permissioned BCs, smart contract and internet of things (IoT). Use IoT technologies, such as quick response code (QRC), radio frequency identification (RFID) and near field communication (NFC), to realize the automatic upload of entities data of the supply chain. The dual-BCs system architecture is designed to ensure the high throughput and scalability of the system. The smart contracts to making the supply chain system more automated, more secure and credible. Finally, the effectiveness of the design scheme is demonstrated by combining the specific application scenario with the practical case.

Keywords: Supply Chain, Permissioned Blockchains, Smart Contract, IoT.

1. Introduction

In recent decades, as a new organizational management model, the supply chain has attracted the attention of many people in the industry [1]. Supply chain management (SCM) adopts the integrated resource integration concept, using advanced information technology and control technology to manage, coordinate and control the supply chain network from the original supplier to the final customer, improve the satisfaction of the supply chain members, and improve the overall the benefits of the supply chain are maximizing cost-effectiveness and meeting customer needs [2][3]. SCM can track internal processes and inventory and information between enterprises, and integrate all parts of the above supply chain structure chart by improving supply chain linkages, so as to achieve a stable competitive advantage [4]. The SCM system is the automatic tracking IT system inventory and information between the company's internal business processes, and between different enterprises to meet the needs of business entities in the supply chain, so that operational processes and information systems close cooperation, seamless link of all links, forming a logistics, information flow, document flow, business flow and capital flow integration [5]. Realize the overall supply chain visualization, management information, maximize the overall benefits, minimize management costs, and thus improve the overall level. Each link in the chain contains two meanings: supply and demand. For example, a retailer is a supplier of consumption and a demander of a distributor. The supply chain links multiple complex entities (including individuals and businesses) such as product supply, manufacturing, distribution, retail, and customers. The different products of supply chains are bound to be very different. Moreover, the supply chains of complex products may span hundreds of stages, and a cycle will last several months or more, involving multiple geographical locations in the world.

At present, more and more enterprises are building supply chain systems to realize supply chain informatization to meet the business needs of entities in the supply chain, so that operational processes and information systems can be closely coordinated to achieve information sharing among participating entities. Sewing links encourage entities to form a community of interests through the supply chain, and has the incentive to strengthen accountability and supervision; improve overall automated production efficiency, increase profits, and reduce costs. However, the current problems of SCM are as follows:

1.1 Lack of Trust.

Supply chain logistics involves a large number of enterprises and has a large management span. There are situations in which third parties cannot or are not willing to share information in a timely and comprehensive manner. As a result of information asymmetry, the related enterprises will not be able to control the circulation of logistics goods in real time. The situation has made it difficult to integrate information in the supply chain. The information of each link of the participating entities in the supply chain is dispersed and stored within each subject. The information between the subjects is not transparent enough, the information transmission speed is slow, and it is easy to be artificially modified, resulting in lack of trust between the entities [6]. Since suppliers at all levels cannot see the overall information, they can only make demand forecasts based on the situation of neighboring first-tier customers. If each level is added with a 10% insurance factor, the amplitude of the order quantity will increase significantly, resulting in the bullwhip effect. The inaccurate information will cause the fluctuation of product demands, which will be enlarged gradually with the transmission of supply chain. The small fluctuations in product retailing will result in large inventory of distributors, manufacturers and suppliers.

1.2 Lack of Security.

The information of each subject in the supply chain logistics is mutually dispersed, and the data information such as procurement, production, sales, logistics, etc. is also fragmented. There is no platform to systematically store, process, share and analyze such information, which wastes a lot of resources. The data resources, in turn, make a large amount of information in a state that cannot be collected or accessed [7]. At the same time, the security of the information cannot be guaranteed. All the information involved in the entire chain of the supply chain, including customer privacy, has security risks.

1.3 Regulatory Traceability Difficulties.

Supply chain operation usually involves cooperation among several stakeholders. When the chain is long, quality problems will inevitably arise. There is no trust system among the main bodies in the supply chain. Once disputes or quality problems arise, it is inefficient and time-consuming to find out the causes of the problems. Traceability is easy to be interrupted, and it is difficult to obtain evidence and accountability, and it is difficult to supervise traceability [8].

1.4 Privacy Protection.

According to the law, some data of an enterprise need to be provided to the competent authorities and proved to the public and other subjects that it has been submitted; on the other hand, because of business secrets, the enterprise is worried about data disclosure, which makes it difficult to balance data transparency and privacy protection [9].

BC is a new technology system derived from the underlying technology of Bitcoin. The earliest definition comes from the paper published by Satoshi Takemoto in 2008 [10]. BC has many technical characteristics, such as decentralization, impossibility of being tampered with and forged, which makes it have incomparable advantages in ensuring information credibility, security, traceability and other aspects of traditional technology.

The permissioned BC is a BC that is jointly managed by several organizations, which runs one or more nodes [11]. The data in the system only be read and wrote by permissioned organizations. Permissioned BC has the advantages of high transaction speed, good scalability and high security and supporting regulatory [12].

This paper proposes a trusted supply chain management system based on the permissioned BCs. This system keeps all the data of suppliers, manufacturers, transporters, retailers and other suppliers in the supply chain from raw material supply, product manufacturing and processing, logistics and sales to complete records. The recorded data is transparent and traceable. It can't be changed, and the private data is encrypted, which solves the problem of trust between the supply chain subjects, regulatory source tracking and data privacy protection. The content of this paper is organized as follows: Section 2 introduces the related technical background; Section 3 presents a trusted supply chain management system based on the permissioned BCs; Section 4 is system analysis; Section 5 is the summary and the future works.

2. Background

2.1 Permissioned BCs.

The methods and algorithms presented in this paper are based on the permissioned BC. The bitcoin networks are public BC technology, which runs on the P2P network [8]. Every computer on the Internet can participate in activities such as computations and confirmations. But in the actual application process, there are disadvantages of low efficiency and low efficiency. Block and transaction delays, in some cases special applications that are not allowed.

Permissioned BCs refers to a BC that is managed by several organizations, each of which runs one or more nodes [9]. Only nodes are permitted to voting, accounting, and building blocks. Each node in the BC usually has a corresponding entity or organization, participants join the network by authorization and form a stakeholder alliance to jointly maintain the operation of the BC. The data only allows different organizations in the system to read, write and send transactions, and jointly record transaction data. It has the advantages of high transaction speed, no need for mining, low transaction cost, and support for supervision.

Table 1 Differences Between Public Bc And Permissioned Bcs

	Public BC	Permissioned BC
Network	P2P network	Private network
Participate	All nodes	permitted nodes
Number of system	Large	Small
Consensus mechanism	PoW, PoS , DPoS	PBFT, CBFT
Mining	Need	No need
Speed	Slow	Fast
Security	Safety	Safety
Privacy	Anonymity	Good privacy
Transaction data	Plaintext	Plaintext
Cost	High	Low

Permissioned BCs nodes run-in high-speed network, the transmission rate is faster, accounting is more instant and the security is higher [10][13]. In permissioned BCs, the nodes have a certain security guarantee such as authorization. These features ensure that permissioned BCs technology can be used in large-scale transaction processing. The permissioned BC can use the Concurrent Byzantine Fault Tolerance (CBFT) algorithm, which is a Byzantine fault-tolerant algorithm with four communications faces for block building [10]. In the case of hacker attacks, it can guarantee data is difficult to be tampered with to ensure data security. There are many differences between the public BC and the permissioned BCs, which are shown in Table 1.

2.2 Dual-BCs Architecture.

The BC system using dual-BCs architecture has good scalability. The dual-BCs architecture of the BC system is composed of ABCs and TBCs that the TBC is used to process data calculation tasks and the ABC is used to store user data hash [14]. In such system, data processing tasks and users' data hashes are separately stored.

The TBC use for storing transactions reads and writes user data to the maintenance user's BC ABC. For example, a small organization can maintain one ABC, and a larger organization can maintain two or more ABC to prevent some The ABC load is too large and therefore has good scalability. ABC has good privacy only when the data processing needs of the user data is transmitted only after the end of trading TBC does not save user data.

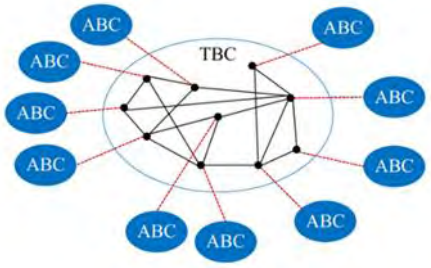

Fig. 1 Dual-BCs Architecture

2.3 Smart Contract.

Smart Contract first is proposed by computer scientists Nick Saab in 1994 [15]. It's a pre-programmed code that identifies and judges the data information obtained and triggers the system automatically, when the conditions set by the program are met, to execute the corresponding contract terms. Smart contracts can export medical data to hospitals, allowing only one-time users of the doctor's identity to read then destroying it to eliminate the hospital's concerns about the safety of its own data and eliminating potential leaks.

BC-based smart contracts, including transactional preservation and state processing, are all done on the BC. The transaction mainly contains the data that needs to be sent, and the time is the description of the data. When the transaction and event information is passed into the smart contract, the resource status in the contract resource set is updated, which in turn triggers the smart contract for state machine judgment [16]. If the event action satisfies the trigger condition, the state machine selects the contract action automatically and correctly according to the participant's preset information.

2.4 IoT Technology.

Under the background of the globalization of production and sales, rapid data acquisition and automatic identification have become the bottleneck of development in the fields of sales, warehouse, logistics, transportation, anti-counterfeiting and identity recognition. The research of data acquisition and automatic identification technology based on QRC, RFID and NFC become more and more important [17].

QRC records data symbolic information with black-and-white graphics which are distributed in the plane according to certain rules by a specific geometric figure [18]. In coding, it ingeniously uses the concept of "0", "1" bit stream, which constitutes the logical basis of the computer, and uses several geometric forms corresponding to the binary system to represent it. Indicate numeric information, through the automatic reading of image input equipment or photoelectric scanning equipment to achieve automatic information processing: it has some common features of barcode technology: each code system has its own specific character set; each character occupies a certain width; has a certain verification function, etc. At the same time, it has the function of automatic recognition of information for different rows and processing of graphics rotation change points.

RFID is a wireless communication technology, which can identify specific targets and read and write related data through radio signals, without establishing mechanical or optical contact between the recognition system and specific targets [19]. RFID is similar to barcode scanning. For barcode technology, it attaches coded barcodes to the target and uses a special scanning reader to transmit information from barcode magnet to scanning reader by the optical signal. For RFID, special RFID reader and special tag can be attached to the target are used to transmit information from the RFID tag to the RFID reader by frequency signal.

NFC as short-range wireless communication, is a short-range high-frequency wireless communication technology that allows non-contact point-to-point data transmission between

electronic devices to exchange data [20]. Like RFID, NFC is also transmitted by electromagnetic induction coupling of the radio frequency portion of the spectrum, but there is still a big difference between them. The transmission range of near-field communication is smaller than that of RFID, and the transmission range of RFID can reach 0-1m. However, due to the unique signal attenuation technology adopted in near-field communication, compared with RFID, near-field communication has the characteristics of low cost, high bandwidth and low energy consumption.

3. A Trusted Supply Chain Management System Based On Permissioned BCs

3.1 Permissioned BCs-Based Trusted Supply Chain Trading Model.

This paper proposes a trusted supply chain management system based on the permissioned BCs, as shown in Figure 2.In this model, data generated in order, purchase, manufacture, logistics, wholesale and retail are uploaded to the Permissioned BCs. Data can be collected by two-dimensional code, RFID and NFC sensors. Data can be transmitted through Bluetooth, WIFI, Zigbee, Ethernet and other communication protocols. The system encrypts public data including company name, company address and randomly generated private data and transmits it to the BC.

In this model, all aspects of the order, procurement, manufacturing, logistics, wholesale, and retail are executed using smart contracts. Smart contracts can represent contracts or ownership, and barcodes or RFID tags represent physical goods. Smart contracts are deployed on BCs and can be used for any transaction between users. The rights and obligations of both parties are clearly defined in the protocol. The actuator of smart contracts periodically checks whether there are relevant events and triggering conditions. Events meeting the conditions will be pushed to the queue to be verified. Verification nodes on the BC first verify the signature of the event to ensure its validity; Then reach a consensus on the event, the smart contract will be successfully executed. Successful execution of the contract will be removed from the block. Unexecuted contracts continue to wait for the next round of processing until they are successfully executed. Through the smart contract, all parties in the supply chain are displayed in the unified BC, so that the parties in the transaction do not have to worry about the loss of benefits caused by one party tampering with the contract or other information asymmetry problems. Moreover, the BC can make the transaction process more transparent, facilitate the supervision of capital and logistics to avoid the occurrence of false transactions.

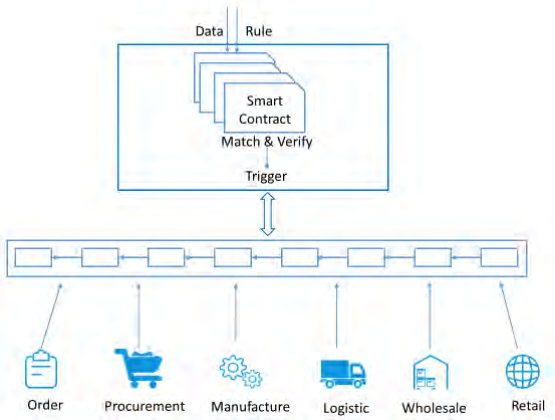

Fig. 2 Permissioned BCs-based trusted supply chain trading model

3.2 System Architecture.

The technical architecture of the trusted SCM system based on the permissioned BCs is shown in the Fig. 3, which is mainly divided into physical layer, communication layer, BC layer and application layer.

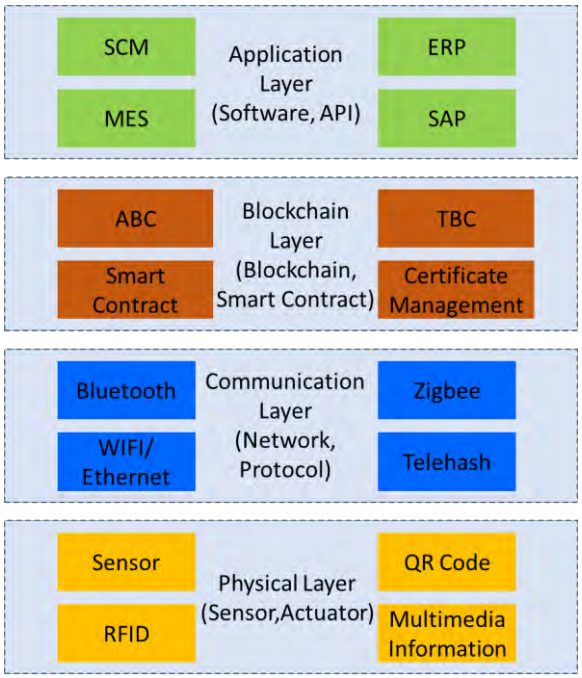

Fig. 3 System technical architecture

The physical layer mainly includes smart sensors and actuators, which are used for data acquisition and forwarding to the upper layer protocol. The process of ordering, purchase, manufacturing, logistics, wholesale, retail, the system collects relevant data by QRC, RFID, NFC and multimedia information. The communication layer mainly includes network structure and protocol. The communication layer of the traditional IoT architecture mainly uses Bluetooth, Zigbee, WIFI, and Ethernet, 3G/4G or other communication mechanisms. After encrypting the private data with public key, the public data and the private data are stored in the BC module through the smart contract module. The BC layer includes BCs and smart contracts. Each record in the BC contains a timestamp and a unique cryptographic signature, and the complete transaction record is available for verification and review by any legitimate user. The information record is open to all nodes in the network, because the ledger is easy to review and has high transparency. Smart contracts are used to perform various supply chain transactions, and smart contracts can represent contracts or ownership. The BC application layer provides various application services, such as DAPP, SCM, ERP, MES and SAP to provide human-computer interaction access.

3.3 BC Architecture.

The architecture of permissioned BC is shown in Fig. 4, which is mainly divided into storage layer, BC core layer, BC service layer and BC interface layer.

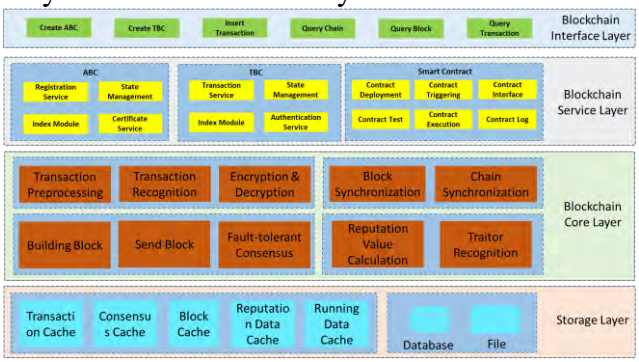

Fig. 4 BC architecture

The storage layer is responsible for various cache data storage and persistent storage of BC data. Support a variety of mainstream databases, such as cache database Redis, relational database MySQL, non-relational database HBase, file storage LevelDB. The core layer of BC is responsible for the core functions of BC, such as consensus mechanism, reputation mechanism, user data, transaction, smart contract, encryption and decryption, signature verification, authentication management, node

management, etc. The BC consensus algorithm adopts CBFT. CBFT consensus algorithm is mainly to make BC nodes reach consensus on block creation, validation and storage, and to ensure the consistency of BC replicas in the system. The service layer includes account BC (ABC) and transaction BC(TBC), ABC is responsible for maintaining account information, TBC is responsible for executing transactions and maintaining transaction history, and ABC stores account information [12]. Smart contracts provide functions such as contract deployment, contract execution, contract triggering and contract testing. The interface layer is responsible for providing the BC platform service interface to the application layer. Through the BC unified interface Open BC Connector (OBCC), the BC service is provided to the application layer.

3.4 Smart Contract Execution.

Smart contracts are composed of script code, algorithm mechanism and smart contract. The smart contract is the core of the contract layer and is implemented by the contract code embedded in the BC. Participants formulate the contract content and trigger mechanism in advance, and embedded the system in the form of code. Once the trigger condition is met, the contract will be executed automatically, and the outside world cannot interfere.

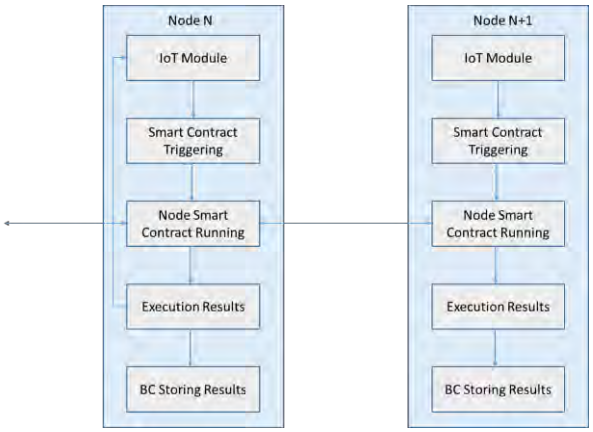

Fig. 5 Smart contract execution

3.5 Application Case.

Take the product traceability application as a case. Firstly, all participants will create a corresponding information file when registering. The file should contain the necessary information such as enterprise information, functions, addresses, and qualifications. After successful registration participants will get a public key and a private key, public key open to all members of the BC, while the private key is the key to verify the identity of the transaction process and information. Each participant can use the registered ID to login to the user interface and enter the designated BC network. The development and maintenance of the software should be carried out by trusted units, and authoritative organizations should assume the responsibilities of the registry. All information is stored in the BC and supported by authorized nodes to access it.

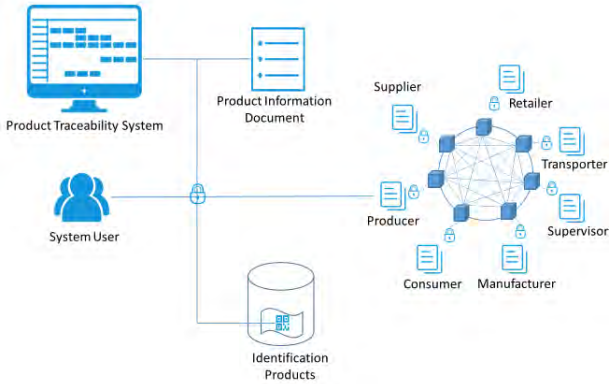

Fig. 6 Product traceability system

When attempting to tamper with the recorded data on the BC, need to modify the duplicate records saved on all nodes. The corresponding RFID tags are written into the relevant attribute information during the production of the products, and the information of the goods is stored in the logistics center database through the control management PC end of the RFID scanner and its connection. After the completion of the contract, through the use of smart contract, commodity information is released in the form of transactions, thus realizing the production of the goods, raw materials, origin, technology, logistics, sellers and other information data chain. Users of the system log on to the product traceability system, and query the commodity information through the system. The system reads the BC information and returns to the front-end interface.

4. System Analysis

This paper uses the features of permissioned BC such as non-tampering, security encryption and fault tolerance to ensure the reliability and robustness of the system. Combining intelligent contract and automation of Internet of Things, the whole SCM is realized. Compared with traditional video surveillance system, the system has many technical advantages. Combined with the automation of smart contracts and IoT technology, the whole SCM is realized. Compared with traditional video surveillance system, the system has many technical advantages.

4.1 Transparency.

The supply chain system based on the permissioned BCs makes the supply chain data more transparent. The enterprises in the supply chain can accurately use end-to-end transparent data. The BC technology can effectively process the transactions of enterprises in the supply chain, and can establish a decentralized and unchangeable record of all transactions, which can realize real-time data sharing and effectively reduce the time cost of data information acquisition.

4.2 Automation.

The use of IoT technology to achieve automated data acquisition and the use of intelligent contract technology greatly simplifies the supply chain business process. Real-time IoT sensors enable automated workflows to be automated through smart contracts (self-executing scripts that can be triggered by BC transactions). The BC network of the IoT accelerates the data exchange in the manufacturing supply chain, thereby improving the operational efficiency.

4.3 Security.

The use of permissioned BCs can improve the security and visibility of supply chain. The distributed and encrypted features of BC allow people to trust each other and conduct point-to-point transactions without the need for third parties. Also, because permissioned BCs using CBFT consensus mechanism has good fault tolerance, which can protect the data from tampering and ensure the security of data, identify malicious or black edge devices in the face of hacker attacks. If any node in the participant network fails, other nodes will continue to run, maintaining information availability and reliability.

4.4 Costs.

Using BC technology to speed up the management of supply chain will automatically reduce the additional costs in the system, while still ensuring the security of transactions. Eliminate intermediaries and intermediaries in the supply chain to avoid risks such as fraud and product duplication. By using BC, customers and suppliers in the supply chain can process payments in a timely manner. In addition, with accurate record keeping, efficiency will increase and the risk of product loss will decrease.

4.5 Scalability

The permissioned BC based on dual-BCs architecture has better scalability. Each participating enterprise can have internal BC and external BC, and can have one or more BCs. Each BC is independent of each other to achieve system expansion. The dual-BCs architecture has the characteristics of load balancing, which can be parallel computing or serial computing, and has good scalability.

5. Summary And Future Works

This paper presents a trusted supply chain management system based on the permissioned BCs. Through this prototype system, the entire supply chain management system is realized. The use of permissioned BC, smart contracts, and IoT technology to solve the problem of trust, supervision traceability, data privacy protection and low automation among the main bodies of the current supply chain management system.

In the future works, we will continue to improve the system function, continue to improve the system performance combined with the specific production environment, and carry out large-scale testing of the system.

Acknowledgments

This work is supported by National Key Laboratory of Software Environment at Beihang University, National 973 Program (Grant No. 2013CB329601), Beijing Municipal Natural Science Foundation (Grant No. 9142012 and 9152009), and National Natural Science Foundation of China (Grant No. 61472032, No. M1450009, No. 71271013 and No. 61462003).

References

[1]. Sell, S. P. D. 1999. Introduction to supply chain management.

[2]. Jung, H., Chen, F. F., & Jeong, B. (Eds.). 2007. Trends in supply chain design and management: technologies and methodologies. Springer Science & Business Media.

[3]. Niranjan, T. T., & Weaver, M. 2011. A unifying view of goods and services supply chain management. The Service Industries Journal, 31(14), 2391-2410.

[4]. Davenport, T. H., & Brooks, J. D. 2004. Enterprise systems and the supply chain. Journal of Enterprise Information Management, 17(1), 8-19.

[5]. Christopher, M. 2016. Logistics & supply chain management. Pearson UK.

[6]. Kwon, I. W. G., & Suh, T. 2004. Factors affecting the level of trust and commitment in supply chain relationships. Journal of supply chain management, 40(1), 4-14.

[7]. Giunipero, L. C., & Aly Eltantawy, R. 2004. Securing the upstream supply chain: a risk management approach. International Journal of Physical Distribution & Logistics Management, 34(9), 698-713.

[8]. Regattieri, A., Gamberi, M., & Manzini, R. 2007. Traceability of food products: General framework and experimental evidence. Journal of food engineering, 81(2), 347-356.

[9]. Li, Y., & Ding, X. 2007. Protecting RFID communications in supply chains. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 234-241). ACM.

[10]. Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system

[11]. Tsai, W. T., Bai, X., & Yu, L. 2017. Design Issues in Permissioned Blockchains for Trusted Computing. In Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on (pp. 153-159). IEEE.

[12]. Tsai, W. T., Deng, E., Ding, X., & Li, J. 2018. Application of Blockchain to Trade Clearing. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 154-163). IEEE.

[13]. Wang, R., Tsai, W. T., He, J., Liu, C., & Deng, E. 2018. A Distributed Digital Asset-Trading Platform Based on Permissioned Blockchains. In International Conference on Smart Blockchain (pp. 55-65). Springer, Cham.

[14]. Tsai, W. T., Blower, R., Zhu, Y., & Yu, L. 2016. A system view of financial blockchains. In Service-Oriented System Engineering (SOSE), 2016 IEEE Symposium on (pp. 450-457). IEEE.

[15]. Szabo, Nick. 1994. Smart contracts. Unpublished manuscript.

[16]. Yu, L., Tsai, W. T., Li, G., Yao, Y., Hu, C., & Deng, E. 2017. Smart-Contract Execution with Concurrent Block Building. In 2017 11th IEEE Symposium on Service-Oriented System Engineering (SOSE) (pp. 160-167). IEEE.

[17]. Brown, K., & Minvielle, E. 2018. U.S. Patent Application No. 15/940,780.

[18]. Liu, Y., & Liu, M. 2006. Automatic recognition algorithm of quick response code based on embedded system. In Intelligent Systems Design and Applications, 2006. ISDA'06. Sixth International Conference on (Vol. 2, pp. 783-788). IEEE.

[19]. Nath, B., Reynolds, F., & Want, R. 2006. RFID technology and applications. IEEE Pervasive Computing, (1), 22-24.

[20]. Yasuda, M., Itoh, K., Natori, M., Yokoshi, M., Yoshimura, O., & Itagaki, T. 2008. U.S. Patent No. 7,336,929. Washington, DC: U.S. Patent and Trademark Office.

[21]. Tsai, W. T., Bai, X., & Yu, L. 2017. Design Issues in Permissioned Blockchains for Trusted Computing. In Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on (pp. 153-159). IEEE.