Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Implementation of the BFTIRS Algorithm for Integrating Distributed Ledgers with Supply Chain Network

K. S. Chandrasekaran[1], V. Mahalakshmi[2], M. R. Anantha Padmanaban[3]

[1]Research Scholar, *Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, chandrasekaran-cse@saranathan.ac.in*
[2]*Assistant Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, mahaa80@gmail.com*
[3]*Associate Professor, Saranathan College of Engineering, Tiruchirappalli, India, mrpadmanaban-mech@saranathan.ac.in*

Over the past ten years, blockchain technology has significantly captured interest in various application fields. Originally devised for the Bitcoin peer-to-peer cryptocurrency network, extensive research now explores integrating blockchain with various other service domains. The technology is celebrated for its decentralized structure, robust security, immutability, and transparency. In blockchain systems, consensus algorithms play a crucial role in establishing unanimous agreement among participants within a distributed computing environment, facilitating the addition of new blocks to the blockchain network. The effectiveness and security of the network largely hinge on the performance of these consensus algorithms. However, existing consensus algorithms face challenges with throughput, latency, and communication complexity. To address these issues, an enhanced consensus algorithm known as Intuitive Random Selection based Byzantine Fault Tolerant (BFTIRS) is introduced. This algorithm optimizes the consensus process by selecting a subset of nodes, thereby reducing network complexity and enhancing efficiency without sacrificing security. To tackle scalability issues in blockchains, a hierarchical BFTIRS algorithm that incorporates sharding is developed. This approach segments network participants into local and global consensus groups, each conducting the consensus process independently. Performance evaluations of this algorithm show improvements in both efficiency and security over existing solutions.

Keywords: Blockchain, supply chain, reputation assessment, C-PBFT.

1. Introduction

A blockchain is a decentralised ledger, a digital technology utilised to document transactions among multiple participants in a verifiable and tamper-resistant manner. The ledger can be configured to execute transactions autonomously. The principal function of blockchain in cryptocurrency networks designed to supplant conventional currencies is to enable secure and private transactions among several anonymous entities, eliminating the necessity for a central intermediary. Supply chains employ restricted access to protect corporate operations from adversarial entities and improve overall efficiency. The effective implementation of blockchain technology in supply chains requires the development of private blockchains, the installation of novel protocols for transaction recording, and the formation of new regulations to govern the system. These components are presently under development at varying stages.

The Advantages of Blockchain Technology

During the 1990s, substantial advancements in the dissemination of supply chain information were primarily propelled by companies such as Walmart and Procter & Gamble, through the adoption of enterprise resource planning (ERP) systems. Nonetheless, the challenge of visibility persists in broad supply chains that involve complex operations.

To illustrate the limitations of current financial ledger entries and ERP systems, along with the potential benefits of a blockchain-based environment, we will present a hypothetical scenario: This is a fundamental transaction in which a merchant acquires a product from a supplier, and a bank transfers the requisite payments to the supplier to complete the order. The transaction involves the exchange of information, transportation of merchandise, and transfer of financial assets. It is important to acknowledge that a certain flow does not produce financial ledger entries for all three parties involved. Cutting-edge ERP systems, manual audits, and inspections fail to adequately integrate the three flows, leading to challenges in mitigating execution errors, improving decision-making, and addressing supply chain problems. This Recently, e-commerce has profoundly influenced contemporary economic life as an innovative trading model, expanding rapidly due to its accessibility and efficacy. The expansion has stimulated a rise in the digital economy and increased consumer expenditure, resulting in significant economic advantages for society. Supply chains are a crucial element of e-commerce as they link various entities, including consumers, intermediaries, manufacturers, and suppliers, to facilitate transactions on online platforms. As the number of nodes proliferates, the intricacies of the supply chain escalate, resulting in significant management and maintenance issues. Issues such as information transmission errors or logistical disruptions are exacerbated when one party in a transaction possesses more or superior information than another, complicating product traceability and intensifying the bullwhip effect. This results in losses for consumers and providers, heightens supply and inventory risks, and disrupts supply chain order and marketing management. Blockchain technology has arisen as a prominent framework for decentralised applications owing to its incorporation of distributed ledger storage, consensus mechanisms, and encryption methodologies. The use of blockchain technology into the data-sharing framework enhances administrative efficiency and provides transparent visibility into supply chain information, benefiting all parties involved in the transaction. This integration also alleviates the bullwhip effect by providing steady trade information. Despite these benefits, blockchain's consensus mechanism inefficiency poses significant challenges to supply chain throughput and transaction processing speed. Among the array of blockchain consensus mechanisms, Practical Byzantine Fault Tolerance (PBFT) effectively addresses these issues with a protocol that simplifies agreement among nodes. Nonetheless, PBFT struggles with efficiency under rapid peer expansion. To address PBFT's shortcomings, concurrent PBFT (C-PBFT) has been developed to enhance consensus efficiency, accommodating rapid expansions with low transaction latency and high throughput. However, current research often overlooks the selection of highly reputable primary peers within concurrent consensus clusters. To tackle this, a consensus algorithm incorporating a reputation assessment, named C-PBFT, has been designed to boost blockchain's efficacy in this integration. Key contributions of this work include:

- Developing a framework that merges supply chain and blockchain for efficient management and data transparency.
- Categorizing supply chain peers into clusters based on transaction history analysis.
- Employing reputation assessment methods like the Simple Additive Weighting.

2. Literature of the past findings

With asymmetric and opaque information and complex administration, the e-commerce supply chain is a vast network made up of suppliers, subcontractors, factories, warehouses, transporters, customers, agents, after-sales services, and so forth. The implementation of blockchain technology in the supply chain results in transparent information, easier management tasks, and reliable transactions [1]. The information island phenomenon is effectively resolved and the connections between manufacturing, sales, logistics, and supervision are broken through with the integration of supply chain and blockchain [1].

This study investigates the challenges associated with tracking the supply chain of cannabis and its significance, specifically in terms of verifying the origin to ensure the product's authenticity. The proposal suggests implementing a blockchain strategy using Polygon technology for the cannabis supply chain. This plan would provide enhanced data security, immutability, and decentralized control over cannabis extract goods[2,4].

Research has already been done on the food supply chain with blockchain technology based on the Internet of Things architecture with supply chain security in mind [5]. By utilizing blockchain technology, companies were able to address the problem of drug safety and establish medical traceability [6]. Some researchers propose the automotive supply chain and t01he blockchain-based automotive sector for on-demand supply chain services. They emphasized that in order to reduce transaction fraud, supply chain peers' trustworthiness can be enhanced using blockchain technology. However, instead of taking into account the various supply chains involved in e-commerce, these studies merely apply the blockchain to one [8, 9]. Because different businesses offer different products on an e-commerce platform, the consensus procedures operate poorly in a contemporaneous environment [10,11].

In order to improve the Byzantine Fault Tolerant in cloud computing and reduce delay a novel method to address the inefficiencies of the existing consensus mechanism[12]. One of the most sophisticated consensus algorithms, the SBFT, was demonstrated by Gueta et al. [13Its latency is two-thirds that of the PBFT and its throughput is approximately double that. To improve throughput and decrease transaction latency, a reputation system that runs on the blockchain and is based on the Proof-of-Stake consensus mechanism was introduced. When compared to existing systems, this one provides better privacy guarantees [14]. Using the distributed storage mechanism of blockchain technology, a reliable platform was developed that lowers management costs and enhances data transfer security [15].

Nevertheless, while choosing the principal peer, the current PBFT program does not account for reputation evaluation. Additionally, Sulin and Yongqing looked into how banks make decisions about credit risk [16]. A new credit model known as a negative rating model was suggested by Luo, Jiang, and Zhao [17][21]. Additionally, the creditworthiness of online retailers is assessed using artificial immune technology (negative survey) for the first time. In order to guarantee efficiency and security, Huang et al. introduce a blockchain system with a reputation-based consensus mechanism [18].

This article develops a reputation assessment approach based on past transaction records as the foundation for primary peers, aiming to address the aforementioned issues. Because the primary peers are reliable, there is a significantly lower chance that they will be Byzantine peers, which enhances the stability of the consensus mechanism.

The e-commerce supply chain is a complex and expansive network that includes suppliers, subcontractors, factories, warehouses, transporters, customers, agents, and after-sales services. Integrating blockchain technology into this system enhances transparency, simplifies management, and ensures more reliable transactions. This integration effectively addresses the "information island" issue, creating seamless links between manufacturing, sales, logistics, and oversight.

Researchers like S. Mondal have applied blockchain to specific supply chains like food, utilizing Internet of Things architecture to bolster security. Similarly, Kumar and Tripathi leveraged blockchain to improve drug safety and traceability. Sharma et al. suggested a blockchain-based model for the automotive sector to provide on-demand supply chain services and boost peer trustworthiness, reducing the risk of fraud. However, these studies tend to focus on single supply chain areas rather than the diverse range needed for e-commerce, where different products and consensus processes may interact poorly in simultaneous operations.

To improve Byzantine Fault Tolerance in cloud computing and minimize delays, a new method that overcomes existing consensus mechanism inefficiencies was introduced. The SBFT algorithm, which achieves higher throughput and lower latency compared to PBFT.A blockchain-based reputation system using the Proof-of-Stake protocol to decrease transaction times and increase throughput, offering superior privacy protections was also developed.

However, current PBFT implementations do not consider reputation assessments when selecting a principal peer. Research by Sulin and Yongqing into bank credit risk decision-making and a new negative rating credit model by Luo, Jiang, and Zhao also highlight the importance of assessing the credibility of online retailers. To enhance the efficiency and security of blockchain systems, Huang et al. introduced a reputation-based consensus mechanism.

This article introduces a reputation assessment method based on historical transactions to select dependable primary peers, thereby reducing the likelihood of encountering Byzantine peers and increasing the stability of the consensus mechanism.

3. Proposed Algorithm

Scalability remains the primary obstacle to the widespread adoption of blockchain technology, as noted in reference. The consensus protocol plays a crucial role in how blockchains perform, with the number of network nodes inversely affecting transaction synchronization speeds. Sharding, originally a database technique that distributes data across several servers to boost search speeds, can enhance consensus by dividing transactions among different groups and merging their outcomes. This method integrates sharding into the consensus process by organizing verifier nodes into functional groups that each handle consensus tasks separately. The end result is a blockchain where smaller group outputs are consolidated into the final block. This sharding-enhanced hierarchical BFT_IRS model not only scales and streamlines the blockchain network but also maintains its security and fault tolerance. By fine-tuning the number of nodes involved in consensus, transaction speeds can be increased without sacrificing fault tolerance. Moreover, this proposed Hierarchical BFT_IRS framework offers higher throughput than existing solutions.

Proposed Architecture

The design of the blockchain network in this proposed method is depicted in Figure 1. It consists of verifier nodes organized into two distinct layers namely Local Consensus Group (LCG) and Global Consensus Group (GCG) Within each consensus group, one verifier node is designated as the Primary node, with the remainder serving as backup nodes. These backup nodes have the responsibility of validating the consensus outcomes and logging the data. The BFT_IRS algorithm is implemented at the LCG level, where it processes and consolidates verified transactions into mini blocks. These mini blocks are then collected by the GCG from all the LCGs to form a large block, which is subsequently integrated into the blockchain network

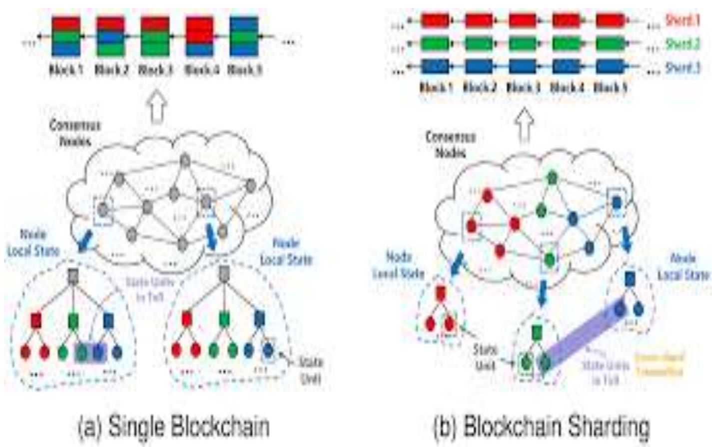

Fig. 1. Sharding-based Layered Blockchain Architecture

Consensus in the Local Consensus Group

The process of reaching consensus within the Local Consensus Group (LCG) begins when a transaction is sent from a client to a backup node, which then assigns it to an LCG. The nodes within the LCG use the IRS algorithm to determine which nodes will participate in the consensus. Both primary and backup nodes carry out the BFTIRS consensus procedure, culminating in the formation of a new mini-block. These mini-blocks are then relayed to the Global Consensus Group (GCG) to assemble the large block that gets added to the blockchain network. The following steps detail the consensus execution within an LCG:

i. The IRS algorithm is run to select verifier nodes. One node is designated as the primary node, while others serve as backup nodes.

ii. The client submits a transaction REQUEST message to a backup node.

iii. This backup node checks the client's signature, assigns a transaction number, and sends out a PRE_PREPARE message throughout the LCG.

iv. The primary node within the LCG validates the signatures of both the client and the backup node, along with the transaction number. It also scans for any conflicting transactions in its local database. If no conflicts are detected, the primary node issues a PREPARE message.

v. The backup nodes verify the PREPARE message. Upon receiving 2f identical PREPARE messages, they broadcast a COMMIT message.

vi. A backup node, upon collecting 2f+1 identical COMMIT messages, processes the client transaction and dispatches a REPLY message.

vii. The primary node, after receiving f+1 identical REPLY messages, confirms that consensus has been reached for the transaction, allowing it to be incorporated into a mini-block.

Consensus in the Global Consensus Group

The Global Consensus Group (GCG) implements the IRS algorithm to select its primary and backup nodes. The primary node in the GCG is responsible for verifying all mini blocks created by various Local Consensus Groups (LCGs) and ensuring their timestamps are correct. It checks the integrity of these mini blocks by verifying signatures and confirming the correct order of transactions. Before the mini blocks can be consolidated into a large block, several conditions must be met by the GCG nodes: They check for any pending transactions that have been verified but not yet included in a mini block. They confirm the authenticity of the signatures from the primary nodes across all LCGs. They verify that the previous hash value of the current large block is accurate. They ensure the correct order of transactions and resolve any conflicts. As outlined in Figure 2, the consensus process within the GCG involves verifying the signatures of both primary and backup nodes. Once these signatures are confirmed, the verifier nodes within the GCG issue a PREPARE message to all LCGs. The primary node in each LCG must receive 2f+1 identical PREPARE messages from the GCG before sending its mini block back to the GCG. The primary node of the GCG then ensures that all mini blocks sharing the same timestamp are collected. Upon successful aggregation, the primary node of the GCG dispatches a COMMIT message to its backup nodes, leading to the final packaging of the large block.

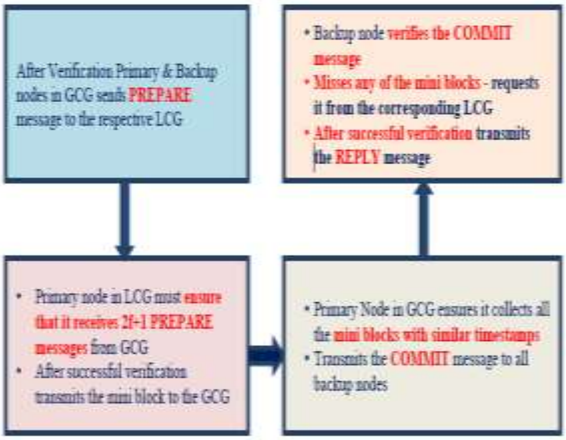

Figure 2 : Consensus at Global Consensus Group

The backup nodes in the Global Consensus Group (GCG) play a crucial role in verifying the COMMIT message and all received mini blocks. Should they discover that a mini block is missing, they request the respective primary node in the Local Consensus Group (LCG) to resend it. After confirming that the transaction order is correct, they send out a REPLY message and proceed to package the large block. The integrity and accuracy of the newly created large block are then verified by the backup nodes. The addition of the large block to the existing ledger occurs only after receiving 2f+1 identical REPLY messages, ensuring that a consensus has been achieved and the transactions are accurately recorded and synchronized across the network

4. Experimental Results

The evaluation is conducted in a Golang command line-based development environment, utilizing the Go programming language. Unique identities are assigned to participants for use during the consensus procedure. Once identities are set, participants are organized based on their geographical proximity. Local Consensus Groups (LCGs) are established by grouping nodes within one-hop communication range. Using selection and election algorithms, various node roles such as candidates, verifiers, and normal nodes are designated. The verifiers within the LCGs select nodes to form the Global Consensus Group (GCG), ensuring equal opportunities for all participants to be included in the GCG.

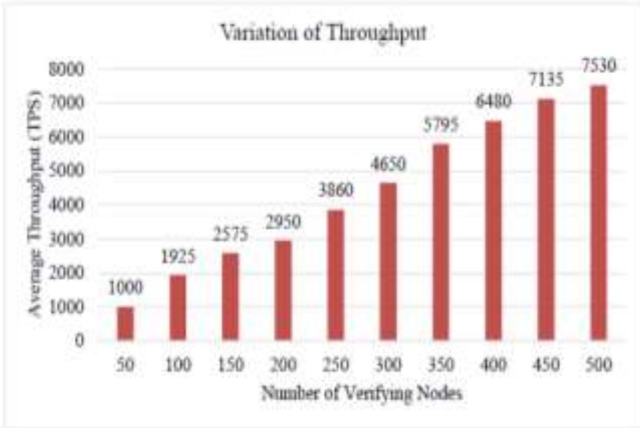

Fig3: Analysis of throughput vs Verifying nodes

The configuration varies with 4 to 12 LCGs, and each LCG consists of 20 to 50 nodes, while the GCG consistently comprises 20 nodes. Each consensus group has exactly 5 verifier nodes. Performance metrics such as query and confirmation latency, throughput, and block creation time are rigorously measured. The size of each large block is standardized at 1 MB. The simulation results, depicted in Figures 3 and 4, show outcomes for configurations with 50 nodes per LCG, where the number of LCGs ranges from 4 to 12. The observed data indicates that query latency ranges from 2.25 to 3.35 seconds, confirmation latency from 6 to 9 seconds, and block creation time from 6 to 8 seconds. Through these configurations, the Hierarchical BFTIRS technique achieves a throughput of up to 7500 transactions per second (TPS).

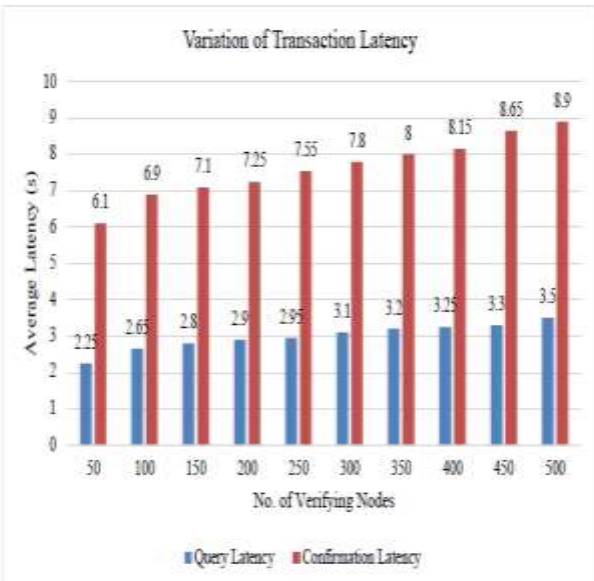

Figure 4: Query and Confirmation Latency Analysis

TABLE I. PERFORMANCE COMPARISON OF THE PROPOSED HIERARCHICAL BFTIRS WITH EXISTING APPROACHES

Parameter	Elasti-co	Omni-Ledger	Monoxi-de	PBFT	BFT IRS (Proposed)	Sharding + BFTIRS
Miner Selection I Consensus	PoW + PBFT	Atomix + PBFT	PoW + Chu ko- nu	State Machin e Based	Intuitive Random Selection	Intuitive Random Selection
Byzantine Fault Tolerance	50%	50%	50%	33%	33%	33%
Node Management	Public	Public	Public	Permis sioned	Permissione d	Permissioned
Block Creation Time (s)	61 – 76	51 – 61	36 - 46	10-16	5-6	6-8
Throughput (TPS)	250 - 2500	300 - 2750	350 - 2900	600 - 4500	800 - 6000	1000-7500
Average Confirmatio n Latency (s)	15 - 30	18 - 25	20-35	11-15	7-8	8-10

The proposed hierarchical BFTIRS algorithm is evaluated against other existing sharding-based approaches, with the comparative results detailed in Table I. The algorithm demonstrates superior performance, achieving higher throughput and reduced latency compared to current solutions. Additionally, it facilitates quicker block creation times and accommodates a larger number of nodes without compromising transaction synchronization speeds. The hierarchical structure of the algorithm allows for dynamic adjustments in the number of nodes within the shards and the total number of groups, based on the overall network node count. This flexibility helps in optimizing the performance of the consensus process while minimizing delays.

5. Conclusion

In this paper, a hierarchical consensus protocol is presented, which integrates the BFTIRS algorithm with the sharding technique. By employing a stratified architecture, this methodology successfully satisfies the require for scalability. The scheme is specifically engineered to allow for the flexible adjustment of the quantity of Local Consensus Groups (LCGs), which effectively regulates complexity and reduces the number of verifier nodes. By increasing throughput without causing significant delays, this functionality optimizes the performance of blockchain systems. Furthermore, a security analysis verifies that despite the existence of malicious nodes, the system continues to function normally, thereby ensuring robust security.

References

1. Xu Zhang, Wenpeng Lu, Fangfang Li, Xueping Peng, and Ruoyu Zhang. 2019. Deep feature fusion model for sentence semantic matching. Comput. Mater. Contin. 61, 2 (2019), 601-616.
2. Piwat Nowvaratkoolchai, Natcha Thawesaengskulthai, Wattana Viriyasitavat and Pramoch

Rangsunvigit, “Blockchain-based Cannabis Traceability in Supply Chain Management” International Journal of Advanced Computer Science and Applications(IJACSA), 15(2), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150210

3. Kai Zheng, Ying Liu, Chuanyu Dai, Yanli Duan, and Xin Huang. 2018. Model checking PBFT consensus mechanism in healthcare blockchain network. In Proceedings of the 9th International Conference on Information Technology in Medicine and Education (ITME'18). IEEE, 877-881
4. Asmaa Aldoubaee, Noor Hafizah Hassan and Fiza Abdul Rahim, “A Systematic Review on Blockchain Scalability” International Journal of Advanced Computer Science and Applications(IJACSA), 14(9), 2023. http://dx.doi.org/10.14569/IJACSA.2023.0140981
5. Saikat Mondal, Kanishka Wijewardena, Saranraj Karuppuswami, Nitya Kriti, Deepak Kumar, and Premjeet Chahal. 2019. Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet Things J. 6, 3 (2019), 5803-5813.
6. Randhir Kumar and Rakesh Tripathi. 2019. Traceability of counterfeit medicine supply chain through Blockchain.In Proceedings of the 11th International Conference on Communication Systems and Networks (COMSNETS'19). IEEE,568-570.
7. Pradip Kumar Sharma, Neeraj Kumar, and Jong Hyuk Park. 2018. Blockchain-based distributed framework for auto- motive industry in a smart city. IEEE Trans. Industr. Info. 15, 7 (2018), 4197-4205
8. Mu-Chen Chen, Yu-Hsiang Hsiao, and Hsi-Yuan Huang. 2016. Semiconductor supply chain planning with decisions of decoupling point and VMI scenario. IEEE Trans. Syst. Man Cybernet.: Syst. 47, 5 (2016), 856-868.
9. Ke Huang, Xiaosong Zhang, Yi Mu, Xiaofen Wang, Guomin Yang, Xiaojiang Du, Fatemeh Rezaeibagha, Qi Xia, and Mohsen Guizani. 2019. Building redactable consortium blockchain for industrial Internet-of-Things. IEEE Trans. In- dustr. Info. 15, 6 (2019), 3670-3679.
10. Daniel Miehle, Dominic Henze, Andreas Seitz, Andre Luckow, and Bernd Bruegge. 2019. PartChain: A decentralized traceability application for multi-tier supply chain networks in the automotive industry. In Proceedings of the IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON'19). IEEE, 140-145
11. Domantas Pelaitis and Georgios Spathoulas. 2018. Developing a universal, decentralized and immutable Erasmus credit transfer system on blockchain. In Proceedings of the Innovations in Intelligent Systems and Applications (IN· ISTA'18). IEEE, 1-6.
12. H. Baghban, M. Moradi, C. Hsu, J. Chou, and Y. Chung. 2016. Byzantine fault tolerant optimization in federated cloud computing. In Proceedings of the IEEE International Conference on Computer and Information Technology (CIT'16).658-661. DOI:https://doi.org/10.1109/CIT.2016.114
13.
14. G. Golan Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. Reiter, D. Seredinschi, O. Tamir, and A. Tomescu. 2019. SBFT: A scalable and decentralized trust infrastructure. In Proceedings of the 49th Annual IEEE/IPIP International Conference on Dependable Systems and Networks (DSN'19). 568-580. DOI:https://doi.org/10.1109/DSN.2019.00063
15. Doaa Mohey El-Din M. Hussein, Mohamed Hamed N. Taha and Nour Eldeen M. Khalifa, “A Blockchain Technology Evolution Between Business Process Management (BPM) and Internet-of-Things (IoT)” International Journal of Advanced Computer Science and Applications(ijacsa), 9(8), 2018. http://dx.doi.org/10.14569/IJACSA.2018.090856
16. Wei Liang, Mingdong Tang, Jing Long, Xin Peng, Jianlong Xu, and Kuan-Ching Li. 2019. A secure fabric blockchain- based data transmission technique for industrial Internet-of-Things. IEEE Trans. Industr. Info. 15, 6 (2019), 3582-3592.
17. Pang Sulin, Liu Yongqing, Wang Yanming, and Yao Hongzhu. 2001. The credit-risk decision mechanism on fixed loan interest rate with imperfect information. J. Syst. Eng. Electron. 12, 3

(2001), 20-24.

18. Wenjian Luo, Hao Jiang, and Dongdong Zhao. 2017. Rating credits of online merchants using negative ranks. IEEE Trans. Emerg. Topics Comput. Intell. 1, 5 (2017), 354-365.
19. Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. 2019. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Trans. Industr. Info. 15, 6 (2019), 3680-3689.
20. Sobia Yaqoob, Muhammad Murad Khan, Ramzan Talib, Arslan Dawood Butt, Sohaib Saleem, Fatima Arif and Amna Nadeem, "Use of Blockchain in Healthcare: A Systematic Literature Review" International Journal of Advanced Computer Science and Applications(IJACSA), 10(5), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100581
21. Prajakta U. Waghe, A Suresh Kumar, Arun B Prasad, Vuda Sreenivasa Rao, E. Thenmozhi, Sanjiv Rao Godla and Yousef A.Baker El-Ebiary, "Blockchain-Enabled Cybersecurity Framework for Safeguarding Patient Data in Medical Informatics" International Journal of Advanced Computer Science and Applications(IJACSA), 15(3), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150381
22. Selvi, S., Revathy, G., & Brindha, P. (2024). Blockchain-Enabled Federated Learning for Secured Edge Data Communication Through a Decentralized Software-Defined Network. In Achieving Secure and Transparent Supply Chains With Blockchain Technology (pp. 128-141). IGI Global.