A Blockchain Based Decentralized Transaction Settlement System in Banking Sector

Sincy Joseph, M.Tech Scholar,
Department of Computer Science & Engineering,
Govt Engineering college Wayanad, Mananthavady,
Mananthavady, Kerala, India - 670644
Email Id: sincyjoseph535@gmail.com

Smitha Karunan, Assistant Professor,
Department of Computer Science & Engineering,
Govt Engineering college Wayanad,
Mananthavady, Kerala, India - 670644
Email Id: smithakarunan@gecwyd.ac.in

2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS) | 978-1-6654-4885-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICMSS53060.2021.9673610

***Abstract*— Blockchain, the underlying technology behind Bitcoin, is an emerging technology in industry. Blockchain has the power to reform the existing business processes more democratic, transparent, secure, and efficient. Banking industries are the first movers that capitalize the disruptive potential of this technology. The indian banking system is one of the complex bank payment system in this world. The current infrastructure that is used by indian bank system is real time gross settlement system based and it follows a centralized architecture. Due to this centralized architecture the processing of transactions are slow and cumbersome. It also causes large amount for security and recovery purposes. The real time gross settlement based system demands high need for security, resilience, and performance. Moving from traditional system to blockchain platform is not the prior concern but making a system that provide security, confidentiality, and decentralized money lending mechanism is the core idea. Here proposed a novel system that enable a decentralized Banking system and services based on Ethereum blockchain platform. The system support different services including money deposit, money transfer and loan checking etc. using the distributed ledger technology.**

***Index Terms*—Bitcoin, smart contract, bank, blockchain, decentralization, distributed ledger, ethereum, consensus, real time gross settlement.**

I. Introduction

A. General Background

Blockchain is a compelling technology that is getting into every industry from banking, medicine to government sector. Because of security concern banking domain mostly use blockchain technology. The Indian banking system is the most complicated bank payment system in this world. It is based on real time gross settlement system Which follows a central server mechanism where all the personal information of account holders, bank balance, and all necessary information related to bank are stored. All branches of bank are connected to central server from which every branch retrieves personal information, bank balance and history of a customer from the server itself. Failure or modification in the central server causes all banks to fall down which results in great loss and causing large amount of processing time and cost. Considering all the issues of the current centralized banking system, the proposed blockchain based decentralized mechanism will provide a banking system in a cost efficient and secure way.

TABLE I
COMPARISON OF TRADITIONAL CENTRALISED AND BLOCKCHAIN BASED BANKING SYSTEMS

	Traditional banking	Blockchain banking
Efficiency	Many intermediate link Complex clearing process High latency Low efficiency	Peer-to-peer transmission Decentralised nature Low latency High efficiency
Cost	Manuel operations & paperwork Duplication of tasks & records Higher operational cost Higher administrative costs Higher reconciliation costs	Complete automation Data consistency Lower costs Dis-intermediation
Security	Prone to hacks & failures Easy to leak sensitive information Modifications & risk of fraud Lower security	Unable to hack Cryptographic encryption Fraud proof Higher security Immutable transaction
Experience	Geographically dependent Homogeneous service Limited customer experience	Geographically independent Real time settlement Real time tracking Good customer experience

B. *Blockchain*

Blockchain is a continuous list of blocks linked using cryptographic algorithms [1]. Every block contains previous block hash value, timestamp and transaction data. The database managed by every entity in network. The transaction history are maintained in blocks fore ever and it is not possible to manipulate transactions. Blockchain is classified into three categories [2]:

- Public Blockchain : In this blockchain person having network facility is able to participate in verification process.
- Private Blockchain : It allows one party having full control and they select few nodes which are predetermined.
- Consortium Blockchain : It gives many benefits of private blockchain without consolidating power in one party.

C. Smart contract

Smart contracts is the programs stored on blockchain that run when predetermined conditions are satisfied. It automates the entire process without any intermediary party. It also facilitates, verifies, and enforces transactions in network.

D. Various Consensus

The consensus algorithms act as the the heart of blockchain. The consensus algorithms solve the problem of mutual trust among nodes in distributed networks. Choosing an apt consensus algorithm directly affect the performance of blockchain. The following are the commonly used consensus [3]:

1) Proof of Work (POW): Bitcoin uses pow consensus algorithm [4]. The working of the system is that first the participating nodes calculate the solution of a mathematical puzzle. The first node that get the puzzle solution will create the next block and get some bitcoins as reward.
2) Proof of Stake(POS): Here the participating nodes can mine and verify transactions based on the coins that hold by them. The miner having more coin will be able to participate in mining process.
3) Delegated Proof of Stake(DPOS): In this consensus algorithm, a group of validator is responsible for block creation process and are elected by all participants in the network. If the chosen validator verifies a wrongful transaction or misses his block he gets voted out and replaced by another delegate. The amount of reward that the validators get for their services is determined by the voters. A problem of the algorithm is that mining is only in the hands of a few delegates which reduces the degree of decentralization.
4) Practical Byzantine Fault Tolerance(PBFT): Introduced by Barbara Liskov and Miguel Castro. It is used in asynchronous based system. It has low overhead.
5) Proof of Authority(POA): POA is a modified version of POS. Instead of using stake having monetary value here uses identity as a stake. It has high performance and fault tolerance.

II. Literature Survey

The paper ”inter bank payment system on enterprise blockchain platform” [5] introduces end to end inter bank payment system based on blockchain that uses hyperledger fabric enterprise blockchain. The system enable gross settlement, reconciliation gridlock resolution facility.

The paper ”exploration and practice of inter-bank application based on blockchain” [6] discusses the difference between the traditional transaction structure and blockchain transaction structure. In the blockchain based system participants share a common ledger containing all transactions in the system. But in traditional system the transactions are carried out using a central institution.

The paper ”a blockchain enabled decentralized time banking for a new social value system” [7] introduces a time banking system. The core concept is to exchange the economy not based in money but value everyone contribution on a scale ie, time expended. The blockchain network facilitate members to participate in the service exchange process without depending on centralized third party for maintaining the service time data. The transaction procedure and service time records are trans-coded in a smart contract. The consensus algorithm in the blockchain enable tamper-proof facility for our transaction data in trustless network. The registration, access control, transaction data are the three components in the time banking architecture.

The paper ”blockchain over transaction system” [8] discusses the issues related to current banking system such as wavering interest rates, higher security and privacy risks, high cost for maintenance, failures, longer access times to data, and inconsistent performance etc. It also discusses Some of the benefits that are obtained by the using of blockchain technology in banking sector such as Immutable transactions, mass reduction in errors, automate high volume of data, reduction in turnaround time, Audit trail, User management, cross platform integration and Code independent integration’s etc.

The paper ”decentralized secure money transfer using blockchain” [9] introduced a system that allow users to create wallets with public and private keys using Elliptic-Curve cryptography. It secure the transfer of funds by using digital signature algorithm which prove ownership and allow users to make transaction.

The paper ”performance analysis of ethereum transaction in private blockchain” [10] explained the concept of blockchain. The blockchain is considered as chained blocks appended using cryptographic hash value of previous block. At a time a single block is added. All the nodes in blockchain is connected via peer-to-peer network and everyone in the network can directly interact with each other without the involvement of third party. The node can make series of transaction. Since all nodes store history of every transaction, tampering is not possible in blockchain.

The paper ”technical characteristics and model of blockchain” [11] discusses the blockchain characteristics and models. Decentralization, collective maintenance, openness, security, verifiability, trustlessness, anonymity, untamperability, traceability, verifiability, programmability are the characteristics of blockchain. The models include data, network, consensus, incentive, contract, and application layer.

The paper ”decentralizing privacy: using blockchain to protect personal data” [12] deals with the prevention of attacks, misuse of personal and sensitive data that are handled by third-parties in our current scenario. Without compromising security the users itself own and control their own data. Here the blockchain acts as an access control moderator. Using the decentralized techniques the legal regulatory decision for collecting, storing sharing data is simple. Also, the laws regulations can also be programmed by blockchain. So that it can be enforced automatically.

The paper ”blockchain and smart contracts for digital certificate” [13] introduces an efficient method to share and verify the certificate using ethereum blockchain technology. This reduces expenses and ensures reduction in forged certificates.

The paper ”enhancing breeder document long term security using blockchain technology” [14] deals with the efficient document verification system that prevents quantum attacks.

The paper provides the idea of fingerprint processing and storing data into the blockchain. But the system takes high computation power and is difficult for poor people to familiarize with this technology.

In paper "blockchain platforms:a compendium" [15] compare various blockchain platforms such as ethereum, hyperledger and corda. From this paper here understood that hyperledger is used in application when security privacy is most needed. Ethereum is used in P2P B2C related generalized applications. corda is used in financial industries.

The paper "performance characterization of hyperledger fabric" [16] discusses the overview of hyperledger fabric including it's architecture, transaction flow, ordering and chaincode execution mechanisms etc. The paper also addresses the characterization of latency and throughput of hyperledger platform with controlled workloads.

The paper "performance analysis of private blockchain platforms in varying workloads" [17] explains the analysis of hyperledger fabric ethereum blockchain in varying workloads. In this paper here understood that hyperledger fabric has high throughput low latency compared to ethereum. Average throughput of hyperledger fabric increases faster than ethereum. However ethereum handle more number of concurrent transaction under same computational resources.

In paper "performance analysis of consensus algorithm in private blockchain" [18] provides the performance analysis of algorithm in private blockchain. From this paper here understood that PBFT algorithm have higher performance than pow algorithm. The performance is measured based on average throughput and average delay.

III. Research Problem

- To design, develop and analyse a blockchain based transaction settlement system that can deliver low cost, secure, reliable, and tamper proof services on top of traditional banking system.

IV. Research Objectives

A. General Objective

- To leverage decentralized nature of blockchain technology in banking system, thereby providing a more robust infrastructure for the traditional banking and business processes.

B. Specific Objective

- To identify the challenges, opportunities, scope of implementing blockchain in banking sector.
- To design a blockchain enabled banking system that cut down the need for verification from third parties and thereby reduce the fraudulent actions and beats processing times for traditional bank transfers.
- To develop a system providing security, low cost, tamper-proof services among distributed peers.
- To develop a system providing different services in banking system such as deposit, transfer, check balance, set loanee, get loanee details etc.
- To leverage the distributed verification feature of Blockchain technology in financial institution and smart contracts for secure service management.
- To develop a system that overcome the scalability and security problem of blockchain technology by using off-chain storage of the data/records by using IPFS technology.
- To analyse the proposed system based on various performance characteristics.

V. Proposed System

A. System Description

Today most of the banking transaction taking place are digital, this transition from conventional payment method has opened up for many types of problems. The current payment system is centralized and rely only on a central authority/server to make transactions. This creates single point of failure and due to this centralized architecture insider or outsider attack is possible thereby entire payment system may be compromised. In the proposed model which provide a decentralized banking services. The decentralized banking services which provides secure payment and services. The system depend on cryptographic proof rather than trust allowing two entities to perform transactions without the involvement of central authority. The Stored procedures also known as smart contract executed in Blockchain is used for processing predefined business step without involvement of an intermediary. All the banking transactions such as credit/debit/loan functions can be implemented in blockchain using the smart contract. Through this project, here aimed to bring the technology closer to common people in banking industry as well as society.

B. System Architecture

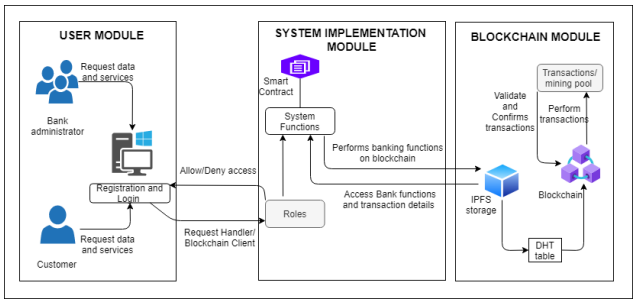

Fig. 1. System Architecture

The fig 1 illustrates system architecture of the system. Here the customer and the bank administrator register through a registration system or portal for accessing different services of a bank. Based on the role of the users interacting with the system the functions are executed. All the services provided by the bank including credit and debit services, loan facilities are provided through smart contract. The smart contract are set of rules that are automatically enforced when some action are occurred. The InterPlanetary File System(IPFS) store transactional data including credit and debit functions,

loan details. The InterPlanetary File System is basically a protocol and peer-to-peer network to store and share data. All the transactional history are stored in blockchain. Once the transactions are in blockchain the customer can access their transaction details from the blockchain.

C. Methodology

The purpose of the system is to build a decentralized application for banking transactions.

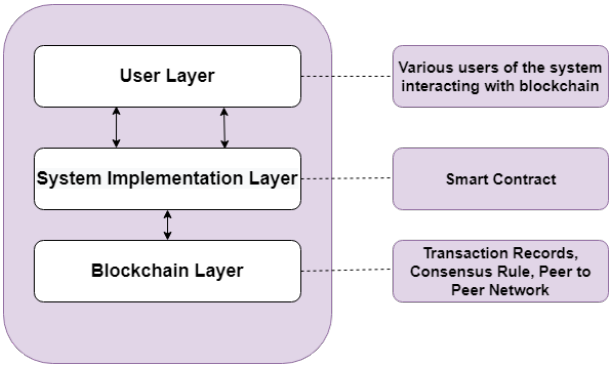

Fig. 2. Modular Design

This system has three modules. User Layer, Blockchain Layer, System Implementation as shown in fig 2. These three module together works for the proper functioning of the system.

1. USER LAYER

The user layer consist of individual nodes that uses the system and resources. The individual nodes are bank administrators, customers who are accessing banking services. The users function is to collaborate with the system and performing tasks in the banking domain such as credit, debit, and loan services. The system functionalities can be accessed by terminal or by browser. In technical term this browser is known as dapp browser. It contains the graphical user interface(GUI) for the dapp.

2. SYSTEM IMPLEMENTATION

The smart contract plays an crucial role in decentralized applications development. The smart contract is gone through 3 stages:

1) Smart Contract Creation
2) Communication Bridge
3) Smart Contract Deployment

1) Smart Contract Creation

In a decentralized system smart contract plays an important role. It is an agreement between two peer nodes in the network. And this agreement is validated by the other participating node through mining process. All the system functionalities such as credit, debit, money lending etc are written inside the smart contract using the solidity code. And this code is complied and generated

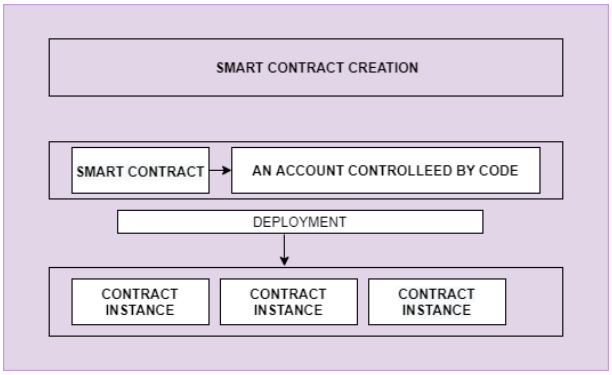

Fig. 3. smart contract creation

abi and bytecode is used for the functioning of the decentralized application.

2) Communication Bridge

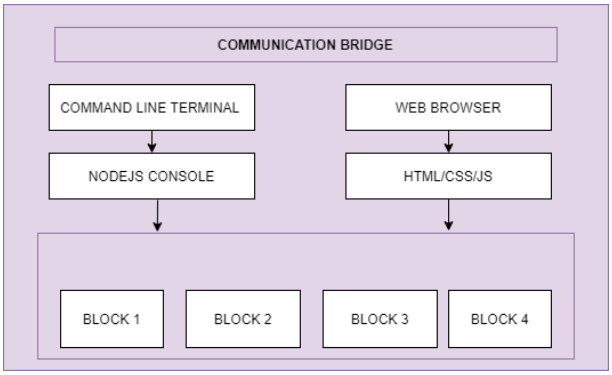

Fig. 4. Communication bridge

The front end and back end communication is needed for the proper functioning of the application. The communication bridge enable this facility in our system. In the communication bridge the multiple layer interaction is taken place. The front-end is made in html, css and javascript that can be accessed using a web browser. The solidity code when compiled generate ABI(Application binary interface) and bytecode which is embedded in html code. And it is used for interacting with blockchain. We can also use command line terminal for interaction with the blockchain.

3) Smart Contract Deployment

The final stage of implementation is smart contract deployment. The smart contract is first compiled using solidity compiler and compiler generate the ABI(Application binary interface) and the byte code. The ABI and BYTECODE is for communication between front and back-end. The smart contract creates the events and through events the communication is taking place. Here the blockchain is running on test network like ganache cli. The gas limits and ether is used for transactions in test networks. The ganache has ten

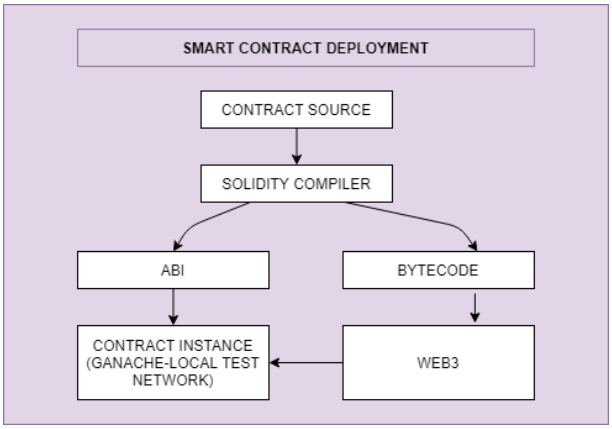

Fig. 5. Smart contract deployment

accounts. The transactions in blockchain is monitored by using web browser extension called metamask. The metamask plugin monitor and record the gas spent and ether used by blockchain for transactions. The application front end is made by html, css, js. The interaction between front end and back end is carried out by web3js.

3. BLOCKCHAIN LAYER

The next layer is the blockchain layer. This layer contains all the code and mechanism for the interaction of user and dapp in the system. The layer comprise three elements in it ie, blockchain assets, governance rule, and network.

1) **Blockchain Assets:** The transactions in ethereum blockchain refer to the change in the state of records or blocks in the blockchain networks. Each and every new change in the records is added as new block in the blockchain. The users can trigger the transactions using the smart contract. All this transactions is refereed as assets in blockchain network.
2) **Governance Rules:** In blockchain technology the governance rules refer to consensus rules. Consensus rules are used for transactions computation and executions in blockchain network. PoW consensus algorithm is the algorithm used in ethereum blockchain. Using this algorithm the blockchain governance is done in trusted manner.
3) **Network:** Ethereum blockchain use peer-to-peer networks for every transactions. Each and every node in this network has equal rights and behaviour. This network provides a decentralized environment of nodes having equal rights.

VI. Results and Discussions

A. Experimental setup

To analyse the system in real life situations here used the apache jmeter tool for performance evaluation. This tool is a desktop performance analysis tool for testing the applications in different situations. Here used apache jmeter (version 5.1.1) & apache (version 2.0).

B. Performance Evaluation

The metrics for evaluation includes execution time, latency and throughput.

1) **Execution Time:** Execution Time is the time difference transaction completion(tx2) and deployment time(tx1) in seconds. Mathematically, it is shown as max(tx2) - min(tx1).
   - Transaction deployment time: It is the time which the transaction is deployed.
   - Transaction completion time: It is the time which the transaction is finished.
2) **Throughput:** Throughput is the amount of data transferred in unit amount of time.
3) **Latency:** Latency is the time difference between the request and response of two system component.

C. Detailed Performance Evaluation

1) **Average Execution Time:** time difference transaction completion(tx2) and deployment time(tx1) in seconds. When the number of transactions are increased the execution time also increases. The transaction here refer the various functions used in the smart contract. If there is a single user using the system functions such as deposit money, transfer money, money lending, loan details. Then it will take 18.291 sec, 1.0 min 48.02 sec and 50.01 sec, 20.02 sec respectively for each functions. The time increases when n users using the system simultaneously.
2) **Throughput:** It is the data transfer in unit amount of time. It is measured in kb/sec. The fig 6. shows the throughput of system. Here jmeter is used to simulate users count from 100 to 500. From the experiment here understand that the when number of user request increase the throughput of the system also increase.

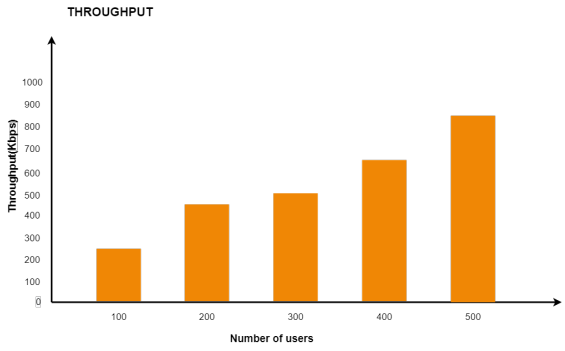

Fig. 6. Throughput of the proposed system

3) **Average Latency:** It is the time difference between the request and response of two system component. Here the latency is measured using jmeter. It is measured in milliseconds. The following Fig 7. shows the average latency of system along with throughput. The latency measured in this experiment is incremental and the highest latency is 14ms.

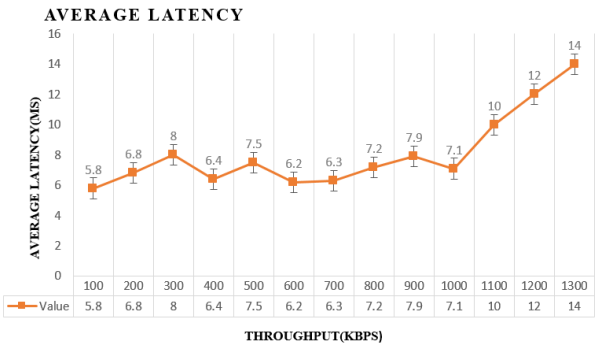

Fig. 7. Average Latency of the proposed system

VII. Limitation and Future Scope

A. Limitations of blockchain

- Higher initial cost: Blockchain saves transaction cost and time but has lots of initial cost. Network size: The need of large number of network participants is also a limitations.
- Limited scalability and storage issues: The blocks in the blockchain grows very rapidly causing storage and scalability issues.
- Un-avoidable security flaws: Miners gaining control of more than half of network computing power is able to perform future confirmations.
- Energy resource consumption: The blockchain network consume lots of resources energy.
- Lack of knowledge and understanding in adopting this technology.

B. Future scope of blockchain

- It is expensive to store data in blockchain so makes better off chain solution to store data and send to blockchain in periodical manner.
- Improves quality of service by adopting new blockchain solution such as corda technologies or any other new technologies.

VIII. Conclusion

Current banking system is based on the centralized architecture which can't handle the digital revolution happening. The proposed method is designed for implementing a decentralized banking system by adopting blockchain on existing banking infrastructure. The blockchain technology has the power to completely revolutionize the way loans function, credit and debit transactions of today's world. It is much better than the traditional centralized system. Blockchain technology provide low cost, high security way of payment transaction that cut down the demand of verification from third parties and reduce processing times for traditional bank transfers. This system completely eradicate the failure of system/data loss/modification of data from the central server. In general the project aimed to provide a more robust infrastructure for the existing banking network using the distributed ledger technology.

References

[1] Blockchain, *https://en.wikipedia.org/wiki/Blockchain*

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[3] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, pp. 2567-2572, doi: 10.1109/SMC.2017.8123011.

[4] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[5] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao and W. Zhao, "Inter-Bank Payment System on Enterprise Blockchain Platform," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 614-621, doi: 10.1109/CLOUD.2018.00085.

[6] T. Wu and X. Liang, "Exploration and practice of inter-bank application based on blockchain," 2017 12th International Conference on Computer Science and Education (ICCSE), 2017, pp. 219-224, doi: 10.1109/ICCSE.2017.8085492.

[7] X. Lin, R. Xu, Y. Chen and J. K. Lum, "A Blockchain-Enabled Decentralized Time Banking for a New Social Value System," 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1-5, doi: 10.1109/CNS.2019.8802734.

[8] A. Vigil, P. Pathak, S. Upadhyay, D. Singh and V. Garg, "Blockchain Over Transaction System," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 1111-1117, doi: 10.1109/CESYS.2018.8723962.

[9] Suganya, T., Vignesh, A., Kumar, V. (2018). "Decentralized secure money transfer using blockchain". IEEE Transactions on Knowledge and Data Engineering, 30, 1366-1385.

[10] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2017, pp. 70-74, doi: 10.1109/ICSESS.2017.8342866.

[11] Y. Xinyi, Z. Yi and Y. He, "Technical Characteristics and Model of Blockchain," 2018 10th International Conference on Communication Software and Networks (ICCSN), 2018, pp. 562-566, doi: 10.1109/ICCSN.2018.8488289.

[12] G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184, doi: 10.1109/SPW.2015.27.

[13] J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

[14] N. Buchmann, C. Rathgeb, H. Baier, C. Busch and M. Margraf, "Enhancing Breeder Document Long-Term Security Using Blockchain Technology," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), 2017, pp. 744-748, doi: 10.1109/COMPSAC.2017.119.

[15] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), 2018, pp. 1-6, doi: 10.1109/ICIRD.2018.8376323.

[16] A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat and S. Chatterjee, "Performance Characterization of Hyperledger Fabric," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 65-74, doi: 10.1109/CVCBT.2018.00013.

[17] S. Pongnumkul, C. Siripanpornchana and S. Thajchayapong, "Performance Analysis of Private Blockchain Platforms in Varying Workloads," 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1-6, doi: 10.1109/ICCCN.2017.8038517.

[18] Y. Hao, Y. Li, X. Dong, L. Fang and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, pp. 280-285, doi: 10.1109/IVS.2018.8500557.