International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure and Privacy for Internet of Things data Modelling and Evaluation using Consortium-based Blockchain Consensus Methods

[1]Jaimin Shroff, [2]Jigna Jadav, [3]Nakul Dave, [4]Avani Dave

Submitted: 04/02/2024 **Revised**: 12/03/2024 **Accepted**: 18/03/2024

Abstract: Over the last 20 years, IoT networks have undergone tremendous development. A major issue with this development is the massive amount of data generated by nodes, even though these devices often have limited memory, resources, and computing power. There, cloud computing comes into play by providing a place to store data. The centralization and robustness of a large network that uses cloud computing can make it susceptible to attacks. On top of that, devices might be vulnerable to attacks because access control settings aren't strong enough. Nonetheless, cloud computing offers a foundation for the implementation of such a security system. According to these standards, mobile and edge devices aren't part of a centralised, secure infrastructure. Because of this, many are beginning to doubt the reliability of cloud intermediaries as a whole, which can lead to security and privacy breaches. With an eye towards the Internet of Things (IoT) and cloud-native infrastructure, this study will examine the issue of blockchain architecture's consensus algorithms as they pertain to the Quorum and MultiChain variations. Keeping decentralisation, security, and public verifiability intact while scaling the core layer is a noteworthy problem. One way to speed up blockchains is to use consortium blockchain frameworks, which do away with smart contracts running in parallel. The difficulties of integrating blockchain technology into the Internet of Things (IoT) setting are better addressed.

Keywords: *Internet of Things (IoT), cloud-native infrastructure, consensus algorithms, blockchain architecture, MultiChain, Quorum, decentralization, security, privacy, trust, smart contracts, scalability,*

Introduction

Blockchain is based on a P2P networking concept, which allows all participants in the use case to trust each other and produce a unanimous ledger state. Although consensus is limited, the entities are pseudonymously unrelated. Bitcoin was a major step forward in the study of digital currency. It has nearly achieved global recognition and has taken advantage of remittances from all over the world. A blockchain that implements bitcoin's rudimentary technology is the next known variation[1]. Figure 1 shows the evolution of trust-based cross-sectoral collaboration networks; this one may or may not be deriving its value from coinage. A new avenue for study has opened up with the advent of blockchain technology[2]. The next step is the implementation of smart contracts, which are essentially self-executing programmes built into the blockchain. As an example of cutting-edge reasoning, consider the Proof of Stake (PoS) consensus, which aims to boost security by doing away with the labor-intensive Proof of Work (PoW). Scaling blockchain for quicker finality on transaction stacks to powerful Internet of Things (IoT) and going head-to-head with banking middlemen like VISA is the latest computing horizon[3].

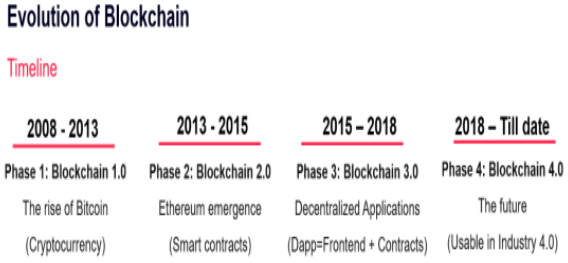

Fig 1 A decade evolution of blockchain

The original idea behind Bitcoin'sblockchain technology which prevents funds from being double-sentedemerged in 2008 as a decentralised, peer-to-peer electronic payment system. Originally developed as a backbone for Bitcoin, blockchain technology has since undergone several iterations, the most recent of which, blockchain

[1]*Assistant Professor, Computer Engineering Department, Vishwakarma Government Engineering College,Chandkheda,Ahmedabad* *jmshroff@vgecg.ac.in*
[2]*Assistant Professor, Computer Engineering Department, Vishwakarma Government Engineering College,Chandkheda,Ahmedabad* *jigna_jadav@vgecg.ac.in*
[3]*Assistant Professor, Computer Engineering Department, Vishwakarma Government Engineering College,Chandkheda,Ahmedabad* *davenakul@vgecg.ac.in*
[4]*Assistant Professor, Computer Engineering Department, Vishwakarma Government Engineering College,Chandkheda,Ahmedabad* *andave@vgecg.ac.in*

3.0, introduced smart contracts and decentralised apps (DApp). Crypto experts predict that a "blockchain of things" will power the blockchain of the future. Originating as a combinatory logic in the multidisciplinary domains of computer networks, distributed computing, cryptography, software engineering, and game theory trade, the idea of blockchain technology was derived from Distributed Ledger Technology (DLT)[3][4][5]. The blockchain protocol ensures the governance of crypto-economic entities and facilitates interactions by running on top of the Internet infrastructure. In addition, digital signatures, hashing functions, asymmetric key cryptography, and data structures like Merkle trees and Merkle Patricia trie fortify and protect blockchain's foundational security features. Hashing entails a collision-resistant one-way mapping from plaintext of variable length to its fixed-length hexadecimal counterpart..

Blockchain Attributes

A distributed ledger with a chronologically interconnected block of transactions is called a "blockchain," which revolves around cryptographic theories towards anti-tampering. The technology moulds without a central administration and instead is managed with consensus among the network nodes. The network has classes of nodes, including full nodes with a copy of the chain and lightweight nodes that depend on full nodes for on-chain data. The chain continuously evolves by annexing new blocks with the approval of all or a majority of nodes to achieve immutability[6]. Once appended to the chain, data manipulation is impossible since the hash of the block changes when any data is prone to be modified. Every block entails a list of committed transactions and corresponding hashes. Each transaction is digitally signed by the payee and verified by the beneficiary. All the committed transactions of the network participants are validated by "consensus algorithms" executed by the "miners" and disseminated across the distributed network

Distributed nature: The data is simultaneously disseminated in different nodes across the network. When a node is broken from the connection or loses its data, the other network nodes retain a copy of the blockchain. The impaired node can recopy the data from other nodes. Hence, the problem of data loss and double-spending is overthrown[7].

Tamper-resistivity: When any block data is modified, it can be recognized by the mismatch in the block hash of the previous and current block. For a malicious activity to succeed, it must be performed on all the blockchain copies residing at all the network computers, which is practically infeasible for an extensive network.

Pseudonymity and back traceability: Pseudonymity is achieved by assigning a public address to a node without revealing its actual identity. A node can generate numerous public-private key pairs; hence, addresses are generated as desired, consenting to the requirement of a degree of pseudo-anonymity. All the activities are transparent as blockchain stores time-stamped data. Hence, the transaction issued by a node can be traced back to its origin address.

Decentralized nature: The blockchain enables components to be autonomous and avoid intermediaries, thus evading the risk of a centralized base. It nontrivially coordinates the heterogeneous actors of cross-domain distributed systems.

Verifiability: The cryptographic artefacts of the blockchain aid in verifying a record in conformance with its authenticity. It is not that simple to accomplish this behaviour in other distributed databases. The cyber-physical systems achieve cybersecurity with external integrity solutions like digital authentication and encryption algorithms.

IoTSecurity Challenges

The Internet of Things (IoT) is gaining widespread recognition as a potentially game-changing technology. This network of networked "smart objects" includes intelligent sensors, embedded devices, personal digital assistants, and cellphones, all of which are able to exchange and report data independently of one another and time zone. It is anticipated that the quantity of data generated by the Internet of Things (IoT) will exceed Zettabytes (ZB) as Internet access keeps expanding at an exponential rate. Because processing and storing data locally on devices increases network complexity, renting space in the cloud makes sense. While there are numerous issues with the cloud, including security, interoperability, data portability, heterogeneous object federation, and restricted network resources, there is still room for growth in this area[8][9]. As far as data privacy and security are concerned, no amount of security laws aimed at strengthening defensive mechanisms for interconnectivity or excellent governance has ever been sufficient. Hacktivists, as they develop expertise, utilise more complex techniques to breach the security of connected devices and steal sensitive data. Therefore, many organisations are starting to consider worries about the IoT's security as a big roadblock to the technology's broad adoption.

Decentralising IoT With Blockchain

In recent years, blockchain has grown more and more dominating in the IoT area as the decentralised nature of the IoT draws nearer to DLT. Internet of Things (IoT) networks are inherently decentralised, making

blockchain, a popular distributed ledger technology (DLT), crucial to the coordination and communication of "things." Without it, there would be no way for peer-to-peer (P2P) transactions to go through[10]. Scalability, reliability, privacy, trust, and time-stamped data are all persistent problems that it fixes. Given blockchain's current prominence in the IoT, its integration with the latter is likely to yield even greater benefits.

Blockchain Consensus and IoT

A disagreement has arisen on the best consensus mechanisms to use depending on the viability of IoT networks, thanks to the explosion of IoT technologies. The convergence of blockchain technology with the Internet of Things raises a number of questions. The intricacy of the block synchronisation models is the main cause for alarm because they demand a lot of hash rate from the restricted hardware resources of the Internet of Things. For what it's worth, the current consensus model is imprecise. Complicating complicated cryptographic analysis is the fact that the standard device setup uses more power for computations and usually keeps back-end storage resources hidden. Authentication and transaction confirmation processes on most blockchain platforms rely on computationally intensive public-key cryptographic algorithms[11][12]. The well-known Arduino Uno board, for instance, has a CPU speed of 16 MHz, which makes it difficult to implement authentication based on elliptic curve cryptography and causes the verification procedure to take more than 8 seconds. In order for the Internet of Things devices to converge on a blockchain and guarantee a maximum level of security, it is necessary to select appropriate cybersecurity. The most popular proof-based consensus method is inefficient for systems with limited resources since it requires a lot of computing power[13].

Throughput Requisites

Internet of Things (IoT) networks need a certain minimum throughput. When it comes to the main use cases for the Internet of Things, popular blockchains like Bitcoin and Ethereum just aren't strong enough. Users' ability to meet their requirements at low throughput is impacted by the double-spending problem, which consensus techniques aim to remove. Ethereum has a throughput of 15 TPS, while Bitcoin is known to have a throughput of 7 TPS[14][7][8]. The high throughput requirements of IoT data are indicated by the sampling interval of IoT sensors, which is typically milliseconds to seconds. It is not desirable to try to improve scalability by increasing throughput in the existing implementations. Consequently, in order to fulfil the high throughput requirements, a consensus model that is well-suited to the Internet of Things should be developed.

Conceptualising Blockchains

The most straightforward technique to improve the transaction processing rate is the divide and conquer approach with a three-tier layered architecture. The prime layer comprises distinctive servers employed with optimization to mitigate network latency and enhance the transaction throughput. The subsequent layers in the existing literature include modified consensus architecture and data structure for core, validation criteria for chain growth, sharding, and federation[15][16]. A recent innovation is a lightning network where the layer with the off-chain channel with protocols restricts theaggregate interactions with the main chain. The benefit of such a perspective is that all transactions published on the main chain are originated within the channel. The meaning is that a transaction clique can be established autonomously of the confirmation time, which dramatically improves the TPS value.

Design Approach Of Blockchain Consensus For Cloud Resource Optimization

The prevailing solutions on blockchain for IoT network security rely on cloud storage (Zhang et al. 2013) as their backend. It primarily involves permissionless types, such as Ethereum, or federated types like Hyperledger. A list of constraints on conditional incentives and penalties with smart contracts can be automatically triggered to enforce stringent rules,. According to etherscan, the network throughput of public blockchains is limited to 18 TPS, which is insufficient for real-time computations. Moreover, the network is urged to execute DApps and perform complete transactions, relying on the cloud to store the transaction movements. Considering all these points, public blockchains possess the ineffectual capability to support data uploading and downloading on time. However, the consortium type of blockchain prevents the time delay noted in public blockchains, but data safety could turn out to be a point of concern[17][18]. Since more than one agent is involved in the consortium network, it cannot provide a fully decentralized environment, keeping the data at risk. In line with all the points of consideration, this research is confined to connect the technological impacts of the consortium chain, file storage, and sharing to arrive at a notion of a two-layered blockchain for IoT and cloud data security.

Blockchain-based distributed cloud storage involves segmented data to form various encrypted, cryptographically linked blocks to pose a more trusted. The segments are distributed within the P2P infrastructure and held by decentralized entities. Strong security is rendered with distributed ledgers, digital signatures for transactions, data encryption with

asymmetric key cryptography, and hashed blocks. When the block size is increased, it allows the network to offer a higher transaction finality pace at the expense of placing more stress on validators, which leads to a centralization risk[4][5][6]. Correspondingly, trade-offs are reported between security and cost. It is noted that Bitcoin-like frameworks hold all transactions in their history at an equal level of irreversibility. It forms an expensive solution to manage and is not suitable for micro-level low-risk transactions in which all participants have shared legal infrastructures to handle fraud. Hence, all these trade-offs should be weighed for each transaction, as they vary widely in utility and risk profile. Ironically, Bitcoin allows for a "one size fits all" approach by definition[7].

As there has arisen a need to manage large-scale data from the evolutionary Internet technologies, the storage has been moved to the cloud. There has been some disagreement with regard to the privacy of the data and the trustworthiness of the third-party cloud service providers. While there are options for enforcing encryption techniques, they do not guarantee the integrity and privacy of the data in transit from a local machine to the cloud and vice-versa. As objects are redundantly stored on distinct devices across multiple sites, blockchain technology can optimize the storage. It can confirm access to a specific piece of information by logging its hash on the blockchain. It also urges the protection of top-secret and mission-critical data through decentralized management and permissioned access to cloud-based systems[9].

Cloud As IoT Data Storage

Cloud migrations take advantage of data centres that are not evenly distributed, even in hyper-scaled cloud bases Cloud data migration causes a shift in the ownership to the third-party vendors and providers. The relative importance of security in the literature on distributed cloud-based storage has been subject to considerable debate,. Several authors have reported the trends in cryptology-based solutions that demonstrate tools and techniques to overcome cyber-risks. However, much uncertainty exists within the cryptographic algorithms regarding their implicit vulnerabilities and key management

P2P Decentralized Cloud Storage

The recent trend of incorporating blockchain into distributed cloud storage creates momentum. The critical task is to enhance the security and reliability of cloud storage services based on the end-user requisites while synchronously boosting the performance of resource allocations and management. The decentralized cloud storage allows for the storage of mission-critical data without jeopardizing its security and the user's ability to orchestrate fine-tuned access control on the data based on its functional requirements. The entities are interconnected by a secure P2P network that strategically combines cryptographical primitives that provide a trusted environment. The self-sustaining nature of blockchain-cloud records complete resource allocation and utilization transactions. The innately verifiable blockchain architecture allows tracing the storage and backup history by querying the system. The decentralized system provides a protected space through a sequentially connected mesh of blocks, storing files and permission properties in the cloud database with a transparent information log

Layering of Blockchain Protocols

A specified set of communication protocols is mapped to track distributed ledger network components called "blockchain protocols." It allows a synergy between fat protocols and thin applications leaning on a distributed network without being concerned about the trust base. The architecture designis geared towards a logical split of four layers represented in Figure 3.3: the resource layer, layers 0, 1, and 2.

Resource Layer: The constrained physical server space swarming across cloud storage platforms provides the infrastructure to run the blockchain. The resource set holds RAM disks, the compute engine, the operating system, the processor core, and the system clock and acts as the substructure's backbone

Private P2P Network Layer: Layer 0 is responsible for laying the groundwork for P2P network components with hardware and the Internet. It develops a base upon which the nodes are interconnected to interact and share the data asynchronously. It realizes a full-term legacy network design that draws together Internet routing with end-to-end logical communication channels.

Main Blockchain Layer: Layer 1 serves as an implementation layer that bootstraps the system with the base permissioned network architecture. This layer sets the network properties and parameters. It forms a tamper-resistant append-only transaction store with interlinked blocks. These blocks are cloned across the network nodes to sustain the global state.

a). Smart Contract: The decentralized mini-application imposes the business logic invoked in response to a request event. It programmatically triggers either a state transition or a microcomputation on processing the resource requests. Resource measurements are represented in a smart contract on the main Ethereum.

b). Consensus model: A block relies on a consensus algorithm for guaranteed security and a mutually agreed consistent shared state. Plasma consensus constructs merkleized proofs in MapReduce format. Side-channel

Layer: The Layer 2 protocol lies on the roof of the Layer 1 network to share the load by allowing the entire blockchain network to scale and be interoperable. It handles the processing of the transactions between the nodes by transferring authenticated data for the sake of the base network. A side-channel is explicitly set as a layer discrete from the chain but tethered to the core network. The transaction processing results are reported to the core chain only in the event of a dispute, with a stipulated condition on the parent chain. The traits of the off-chain lean on the consensus model of the core network. A hybridized scaling solution inherits the property of the state channel in which transactions are privatized among the participants

The Truffle framework is used as a development environment for testing and as a configurable build pipeline for Ethereum (2021) network management. Its scriptable context provides built-in smart contract execution, linking, deployment, and binary management benefits. Node.js scripting is used for an open-source server setting that uses JavaScript on the server. A library compilation with web3.js is adopted to collaborate among the local and remote Ethereum nodes employing HTTP, IPC, or WebSocket. Ganache is fabricated as a private blockchain used to call smart contract codes into operation, deploy applications, and run experiments. The testrpc is a node.js compatible server-based Ethereum client used for this research and analysis. It works on ethereum.js to simulate the complete client behaviour as it has all the accessible RPC functions and events that run in deterministic polynomial time. The two-layer optimism aims to decongest the base layer, confined to its slower transaction finality and network resource exhaustion. Data offloading has been emphasized as a strategy of increasing transaction processing speed to prevent bottlenecks and boost throughput.

Smart Contracts

A smart contract is a self-executing program stored on the Ethereumblockchain that gets invoked whenever the pre-set conditions are encountered. It is a compilation of functions and parameters that remains at a precise address in the Ethereum private network. It automates the execution of the transaction process without intermediaries or time loss. An Ethereumbased smart contract deployment involves submitting a gas-consuming transaction as an asset transfer. The testnet implements a smart contract as anEthereum account, which denotes that the contract account retains a balance. It implies that the contract codes can send transactions across the network. Even though the contracts are network deployed, these special accounts are not user-controlled; instead, the code executes as programmed. The user accounts are allowed to interact with the smart contract by issuing transactions that evoke a function written on it. Although the state of the code is transparent on the ledger, the users' privacy is preserved. Smart contracts avoid intermediate layers that reduce the operation and processing time and are conflict-free.

Solidity

Ethereum-based smart contracts are implemented with an objectoriented language called Solidity. It is a Java-based programming language that incorporates C++, Python, and JavaScript concepts into object-oriented programming (OOPs). Solidity targets the Ethereum Virtual Machine (EVM) and holds the inheritance model to execute in the Remix IDE. The Solidity compiler translates the source code into bytecode on the EVM. The solidity execution environment is set up through the Node Package Manager (npm) for Node.js. Once the contract is deployed, no new features or updates can be made. It can be revisited at run-time rather than at compilation. Plasma smart contract enforces the time to live concept by defining an agreed-upon dispute time. When this time gets elapsed with no fraud-proof issued on the main chain, the request is rendered.

Layered Consortium Blockchain For IoT Consensus

IoT network has come a long way in usability, with use-cases like smart homes, smart healthcare, and intelligent vehicles. It is a wide-area network with distributed processors, communicating devices, and hardware interfaces that send and receive data from their context, thereby generating a large volume of heterogeneous data. Considering the characteristics of IoT, blockchain, a cryptographically distributed tamper-proof database when blended with IoT, allows smart device data volume to be archived and exchanged as P2P transactions more privately. Blockchain technology is a significant shift that drives peer transactions with the traits of decentralization, autonomy, pseudonymity, openness, and tamper-resistivity. Recently, researchers have shown increased attention to the applicability of blockchain for IoT security. It is a distributed data management model that embeds only confirmed transactions, formed as a hash-linked chain of time-ordered blocks. Transaction-level integrity is enforced with a digital signature and clustered as a Merkle tree that holds transaction histories. The newly generated blocks are pooled and validated by solving a compute-intensive but verifiable cryptographic puzzle. Some cryptocurrencies, such as Bitcoin, can be viewed as an open-ended and growing record of financial transactions on the blockchain. The primecomponents of the blockchain are hash pointers and transaction blocks, where the hash points to the previous block, and the data field holds the Merkle tree root hash organized with time stamped transactions. Even for the globe that is sceptical of the advantages of cryptocurrency, blockchain offers

much hope for diversified application domains. Reconsidering this cybersecurity, blockchain can be leveraged with the IoT.The application of blockchain technology to IoT necessitates the problem of consensus agreement to be addressed. Because of the CAP theorem, which asserts that it is hard to ensure consistency, availability, and partition tolerance concurrently, the scalability trilemma evolves. Contradictorily, increasing the volume of on-chain transactions could increase the number of resources associated with executing a full node. It urges more nodes to operate lightweight clients that mark relatively low trustworthiness on the honest-majority consensus process for block validity. When the blockchaintrilemma is resolved at the protocol level, it typically centralizes the system. Increased transaction volume frequently necessitates increased autonomy on specific nodes, raising the degree of centralized control. An alternative solution to the consensus problem addresses the network bottleneck by embedding a trust layer

Conclusion

Consortium-based blockchain frameworks offer a decentralized and trustless environment for IoT data modeling and evaluation, reducing reliance on centralized intermediaries and mitigating the risks of data manipulation and unauthorized access. By distributing authority among a consortium of trusted entities, these frameworks ensure transparent and tamper-resistant data transactions, enhancing data integrity and auditability in IoT environments.However, deploying blockchain technology for IoT data modeling and evaluation also presents several challenges and considerations. Scalability, interoperability, regulatory compliance, and energy consumption are among the key challenges that must be addressed to realize the full potential of blockchain in IoT applications. Additionally, ensuring the resilience and robustness of consortium-based blockchain networks against malicious attacks and consensus failures remains a critical area of research and development.

References

[1] Al Omar, A, Bhuiyan, MZA &Basu, A 2018, 'Privacy-friendly platform for healthcare data in cloud based on blockchain environment', International Journal of Information Security, vol. 95, pp. 511-521.

[2] Alessi, M, Camillo, A, Giangreco, E, Matera, M, Pino, S &Storelli, D 2018, 'Make users own their data: A decentralized personal data store prototype based on ethereum and ipfs', 3rd International Conference on Smart and Sustainable Technologies (SpliTech), pp. 1-7. IEEE.

[3] Ali, MS, Dolui, K &Antonelli, F 2017, 'IoT data privacy via blockchains and IPFS', In Proceedings of the Seventh International Conference on the Internet of Things, pp. 1-7.

[4] Aljarbou, YS 2019, 'Large File Transfer Using Multicast and P2P for Error Checking and Correction', 2 nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-3.

[5] Alphand, O, Amoretti, M, Claeys, T, Dall'Asta, S, Duda, A, Ferrari, G, Rousseau, F, Tourancheau, B, Veltri, L &Zanichelli, F 2018, 'IoTChain: A blockchain security architecture for the Internet of Things', IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6

[6] K. Ingole and D. Padole, "Design Approaches for Internet of Things Based System Model for Agricultural Applications," 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151606.

[7] Chen, X, Zhang, K, Liang, X, Qiu, W, Zhang, Z &Tu, D 2020, 'HyperBSA: A High-Performance Consortium Blockchain Storage Architecture for Massive Data', IEEE Access, vol. 8, pp. 178402-178413.

[8] Dorri, A, Kanhere, S, Jurdak, R &Gauravaram, P 2019, 'LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy', Journal of Parallel and Distributed Computing, vol. 134, pp. 180-197.

[9] Garay, J &Kiayias, A 2020, 'Sok: A consensus taxonomy in the blockchain era', In Cryptographers' Track at the RSA Conference, Springer, Cham., pp. 284-318.

[10] Goyal, S, Sharma, N, Kaushik, I &Bhushan, B 2021, 'Blockchain as a solution for security attacks in named data networking of things', Security and Privacy Issues in IoT Devices and Sensor Networks, pp. 211-243.

[11] Kang, J, Xiong, Z, Niyato, D, Wang, P, Ye, D & Kim, D 2019, 'Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks', IEEE Wireless Communications Letters, vol. 8, pp. 157-160.

[12] Kumar, R, Marchang, N &Tripathi, R 2020, 'Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain', International Conference on COMmunication Systems &NETworkS (COMSNETS), pp. 1-5

[13] Li, J, Guo, D &Ren, L 2021, 'Close latency-security trade-off for the Nakamoto consensus', Proceedings of the 3rd ACM Conference on Advances in Financial Technologies.

[14] Li, W, Feng, C, Zhang, L, Xu, H, Cao, B & Imran, M.A 2021, 'A scalable multi-layer PBFT consensus for blockchain', IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 5, pp. 1146-1160. 60.

[15] Li, X, Jiang, P, Chen, T, Luo, X & Wen, Q 2020, 'A Survey on the Security of Blockchain Systems', Future Generation Computer Systems, vol. 107, pp. 841-853.

[16] Liu, H, Han, D & Li, D 2020, 'Fabric-iot: A Blockchain-Based Access Control System in IoT', IEEE Access, vol. 8, pp. 18207-18218

[17] Mahapatra, S, Singh, BK & Kumar, V 2020, 'A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges', Arabian Journal for Science and Engineering, pp. 1-30.

[18] Malhotra, A, O'Neill, HM &Stowell, P 2021, 'Thinking Strategically about Blockchain Adoption Risks and Risk Mitigation', Business Horizons, vol. 65, pp. 159-171