Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.034115
Article

An Interoperability Cross-Block Chain Framework for Secure Transactions in IoT

N. Anand Kumar[1,*], A. Grace Selvarani[2] and P. Vivekanandan[3]

[1]Department of IT, SNS College of Technology, Coimbatore, Tamilnadu, 641035, India
[2]Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, 641035, India
[3]Department of CSE, Park College of Engineering and Technology, Coimbatore, Tamilnadu, 641035, India
*Corresponding Author: N. Anand Kumar. Email: anandk4455@gmail.com
Received: 06 July 2022; Accepted: 07 November 2022; Published: 26 May 2023

Abstract: The purpose of this research is to deal with effective block chain framework for secure transactions. The rate of effective data transactions and the interoperability of the ledger are the two major obstacles involved in Blockchain and to tackle this issue, Cross-Chain based Transaction (CCT) is introduced. Traditional industries have been restructured by the introduction of Internet of Things (IoT) to become smart industries through the feature of data-driven decision-making. Still, there are a few limitations, like decentralization, security vulnerabilities, poor interoperability, as well as privacy concerns in IoTs. To overcome this limitation, Blockchain has been employed to assure a safer transaction process, especially in asset exchanges. In recent decades, scalable local ledgers implement Blockchains, simultaneously sustaining peer validations of transactions which can be at local or global levels. From the single Hyperledger-based blockchains system, the CCT takes the transaction amid various chains. In addition, the most significant factor for this registration processing strategy is the Signature to ensure security. The application of the Quantum cryptographic algorithm amplifies the proposed Hyperledger-based blockchains, to strengthen the safety of the process. The key has been determined by restricting the number of transactions that reach the global Blockchain using the quantum-based hash function and accomplished by scalable local ledgers, and peer validations of transactions at local and global levels without any issues. The rate of transaction processing for entire peers has enhanced with the ancillary aid of the proposed solution, as it includes the procedure of load distribution. Without any boosted enhancement, the recommended solution utilizes the current transaction strategy, and also, it's aimed at scalability, resource conservation, and interoperability. The experimental results of the system have been evaluated using the metrics like block weight, ledger memory, the usage of the central processing unit, and the communication overhead.

Keywords: Internet of Things (IoT); scalability; blockchain; interoperability; security; ledger size; transaction rate; cross-chain based transaction (CCT); quantum cryptographic algorithm

1 Introduction

The computer-aided business has developed into a smart industry with data-driven decision-making, made possible by revolutionary advances in ICT (Information and Communication Technology) [1]. In this paradigm change, IoT play a crucial role in connecting the physical industrial environments to cyberspaces of computing systems, resulting in the development of CPSs (Cyber-Physical Systems). IoT can support Industrial applications including manufacturing, logistics, food sectors, and utilities. The adoption of IoT is predicted to reach 50 billion devices and billions of transactions per day by 2020 [2]. IoTs are aimed at increasing productivity, reducing machine downtimes, and enhancing product quality. However, several drawbacks are also there in IoTs like decentralizations, poor interoperability, privacy, and security issues.

To strengthen security, Blockchain (BC) is used to protect privacy and to tackle the problem of interoperability in IoTs have been exploited by this study, which utilizes community validation to correlate the components of replicated ledgers over large numbers of users [3]. Blockchain, data records have been archived as blocks and based on the logical connections, they are structured as a list of data blocks that have been linked together [4]. The modifications that were done to the data blocks using the consensus method have been evident in the overall network which leads to attaining a tamper-proof platform to keep and share the data [5]. The involvement of an intermediary entity is no more necessary, as in blockchain the data sharing is completely automatic, which enables a paradigm shift to be converted from centralized to decentralized management. Initially, it is presented to overcome the issue of double spending in Bitcoin but in stationing other applications, like health care, logistic systems, delivery networks, and smart grid, it takes more time [6].

In protecting privacy in a system type of Peer-to-Peer (P2P) assuring the security of the shared data, the blockchain we used to stand as a well-qualified competitor by its nature of decentralization. Still, there are certain features of IoTs make it difficult to exploit the blockchain directly in IoTs or other mobile services, they are; the heavy use of resources during the mining and consensus processes, as well as the inadequate resources of IoTs nodes [7]. Research work has come up with the latest permissioned Blockchain and Hyperledger [8]. The blockchain concept anticipates keeping a ledger of device transaction logs and communications in IoTs. It is a crucial necessity to be aware of the formation of BC networks to unite IoTs and Block chain devices used in IoTs can come in two models:

- In the first model, by applying a peer client on itself, each device in IoTs turns out to be a part of the BC network.
- Considering the second model uses a single peer in the global Blockchain (through a legible model) to stand in for the numerous devices that are combined.

Two significant challenges need to be faced in present BC solutions by combining both the models for devices used in IoTs; Transaction per second (TPS), interoperability, and ledger storage requirements. The approach tends to capacitate Blockchain scalability as regards ledger size, rate of the transaction, and interoperability. To avoid the additional work of millions of local transactions done inside the organizations or home networks, the BC ledger is the ultimate intention.

For IoTs, the strategy called Interoperability Cross-Block Chain (ICBC) has been proposed by this research to ease inter and intra-organizational transactions. Through a process of registration authorized by a local Certification Authority (CA), every device in IoTs is linked with an organization. In the ICBC structure, the Cross-Chain based Transaction (CCT) has been utilized to authorize Interoperability, whereas the interoperability has been executed based on the CCT feature. Furthermore, in contrast to the use of peers in global Blockchain networks, this study recommends handling associated anchor peers in global networks utilizing Local Peer (LPR) structures where quantum hashing ensures security. To complete an intra-organizational transactions, the structures restrict ledger sizes and divide them between

Local and anchor peers throughout peer validations. Only in the event of the data getting perpetrated on the destination chain, the ICBC structure is accepted and acknowledged as successful. Hyperledger Fabric (v1.0.2) has been utilized to simulate the proposed model.

The rest of the paper is structured as follows: a literature review of IoTs for secure transactions is provided in Section 2. Section 3 summarizes the Interoperability Cross-Block Chain (ICBC) Framework for IoTs. The proposed system is detailed in Section 4, and the results of the proposed system are implemented and evaluated using other methods in Section 5. This paper concludes and extends the work discussed in Section 6.

2 Literature Review

Many articles and research papers confer the convergence of blockchain with IoTs as given below:

Dorri et al. [9] got rid of the concepts of POW (Proof of Work) and currencies in their lightweight implementations for blockchain devices using IoTs. Their suggested approach had three main phases for smart home environments namely overlays, cloud storages, and smart houses. All of the smart home tier's fundamental components and activities have been thoroughly explored and exemplified. A very capable gadget known as a "Miner" is in charge of controlling all internal and inter-house communications that will ever be online, as well as equipping every smart home. The Miner has also taken care of a private and much safer BC for handling and analyzing communications. For catering to necessary goals of security including confidentiality, integrity, and availability, the study's recommended blockchain-based smart home structures were fortified. Moreover, the overheads created by their technique in terms of traffics, processing times, and energy usages were minor in comparison to the security and privacy improvements and as demonstrated by their simulation results.

Zhang et al. [10] introduced an inventive renovation on the platform of the Internet which turns into a novel domain for Electric-business. 1) Electric IoTs E-business model was established solely for IoTs based E-business; 2) in existing E-business designs, many elements were restructured; 3) Considering the P2P trades based on Blockchain and smart contracts, smart property transactions and paid data on IoTs are recognized. In addition, comprehensive discussions, as well as the assessment of the designs were also done. Still, specific circumstances of integrating block chain with IoTs (for instance, a smart home application) have been significantly considered in these studies. In recent times, studies on blockchain's convergences with IoTs have increased, besides numerous articles have also been published.

Banerjee et al. [11] studied security in IoTs and the effectiveness of blockchain techniques as possible solutions. The study observed a lack of publicly accessible datasets for IoTs that could be used by academia and professionals. Thus, establishing standards for IoT dataset shares is essential. The study expressed the importance of powerful blockchain technology that is needed for protecting IoT systems and providing secure dataset sharing (e.g., guaranteeing the integrity of shared datasets using blockchain).

Reyna et al. [12] tend to examine the chances and the problems of the research when combining blockchain with IoTs. Based on this approach, the authors examined the limitations in the applications of Block chain IoTs and observed the closely associated work to assess the effective way of enhancing IoTs using blockchain. Ali et al. [13] tend to provide wide-ranging scrutiny on the implementation of blockchain in IoT. Begin with aspects like necessary working principles of block chains and creating block chain-based systems that attain auditable decentralizations with security. Subsequently, the limits provided by current centralized IoT models should be investigated, followed by improvements made in both the physical industry and theoretical research to overcome such limitations and effectively utilize blockchains to deliver a decentralized, safe medium for IoTs.

Novo [14] introduced an innovative way for arbitrating roles and authentications in IoTs. Based on Blockchain methodology, this innovative structure acts as an entirely distributed access control system. Here, evidence of the application of the concept stands as a support to the new structure, and IoTs have been assessed in real-time circumstances. During certain scalable IoT circumstances, this blockchain method can be exploited as an access management system that has established evidence through the outcomes.

Dorri et al. [15] favored an LSB (Lightweight Scalable blockchain) which not only upgraded on IoTs demands but also ensured end-to-end protections. Decentralization of the blockchain was been done by creating overlay networks with high-resource devices handling blockchain collectively. To prevent blockchain throughputs from deviating further from transactions on networks, LSB employed an algorithm known as DTM (Distributed Throughput Management). Because the cluster chiefs are in charge of the public blockchain, the overlay has been arranged as individual clusters to minimize the overheads.

Sharma et al. [16] exploited the DistBlockNetto-based blockchain strategy via distributed secure Software-Defined Networking (SDN) structure for IoTs. The standard procedures for designing a scalable, secure and efficient network structure have been adopted by this method. SDN and blockchain are two promising techniques whose benefits have been combined by the DistBlockNet architecture of IoTs structure. In the absence of a trusted intermediary, blockchain allowed members of dispersed peer-to-peer networks to transact with one another in verifiable manners using the study's revised flow rule tables where versions of the flow rule tables were confirmed, the flow rule tables validated, and most recent flow rule tables were downloaded for forwarding devices of IoTs. The potential of DistBlockNet to identify hazards throughout the IoT network in real-time with decreased performance overheads has been demonstrated by the evaluation results. Also, it converges the design standards necessitated for the future IoT network.

Biswas et al. [17] intended a Scalable Blockchain Framework solution to confront these obstacles by filling the gap with a local peer network using scalable local ledgers without sacrificing peer validations of transactions at local and global levels; it is possible to limit the number of transactions that arrive at the global BC. Experiment results showed a significant reduction in block weight and ledger size compared to global peers. The rate of processing transactions of all peers has also been indirectly augmented by the solution as it includes the process of load distribution.

To address the issue of data vulnerability, Abbas et al. [18] suggested a decentralized data management system for smart and secure transportation that makes use of blockchain technology and the Internet of Things in a sustainable smart city setting. It covers background information before offering a Hyperledger Fabric-based data architecture that underpins a safe, reliable, and intelligent transportation system. The simulation results demonstrate the equilibrium between the amount of time required for blockchain mining and the quantity of newly produced blocks. Using an average transaction delay evaluation approach, the performance of the suggested system is tested. The technology will improve governance by addressing residents' and authorities' concerns about the security of the city's transportation network.

A blockchain-based IoT-based collaborative processing system for managing and scheduling marine transportation flow was proposed by Zhang et al. [19]. To lower the communication costs involved in the consensus communication process on the blockchain, a novel consensus method based on reputation voting and Verifiable Random Function (VRF) is introduced. The proposed technique has been tested in a simulated setting, and the findings show that it has a clear advantage in fending against replay and disguise attacks.

3 Interoperability Cross-Block Chain (ICBC) Framework for IoTs

The Interoperability Cross-Block Chain (ICBC) has been recommended in this research for IoT with intra and inter-organizational transactions. Through a process of registration that has been initiated by a local Certification Authority (CA), every device in IoT is linked with an organization. In the ICBC structure, interoperability has been carried out by the feature of Cross-Chain based Transaction (CCT). The CCT is taken into consideration as the transaction between two separate chains using the same Hyperledger-based Blockchain technology. The basic concept of the proposed ICBC model is that the direct connection of devices in IoTs with peer devices is certainly prohibited. The transaction flow can be controlled through an intermediate entity that connects devices and BC peers. It is mandatory for all devices used in IoT to correlate with an entity. By this organization, Transactions within the network have been separated from those that must be handled by global Blockchain by executing the local peer network. During the implementation of this idea, the network has split into five parts in the proposed method, as represented in Fig. 1.

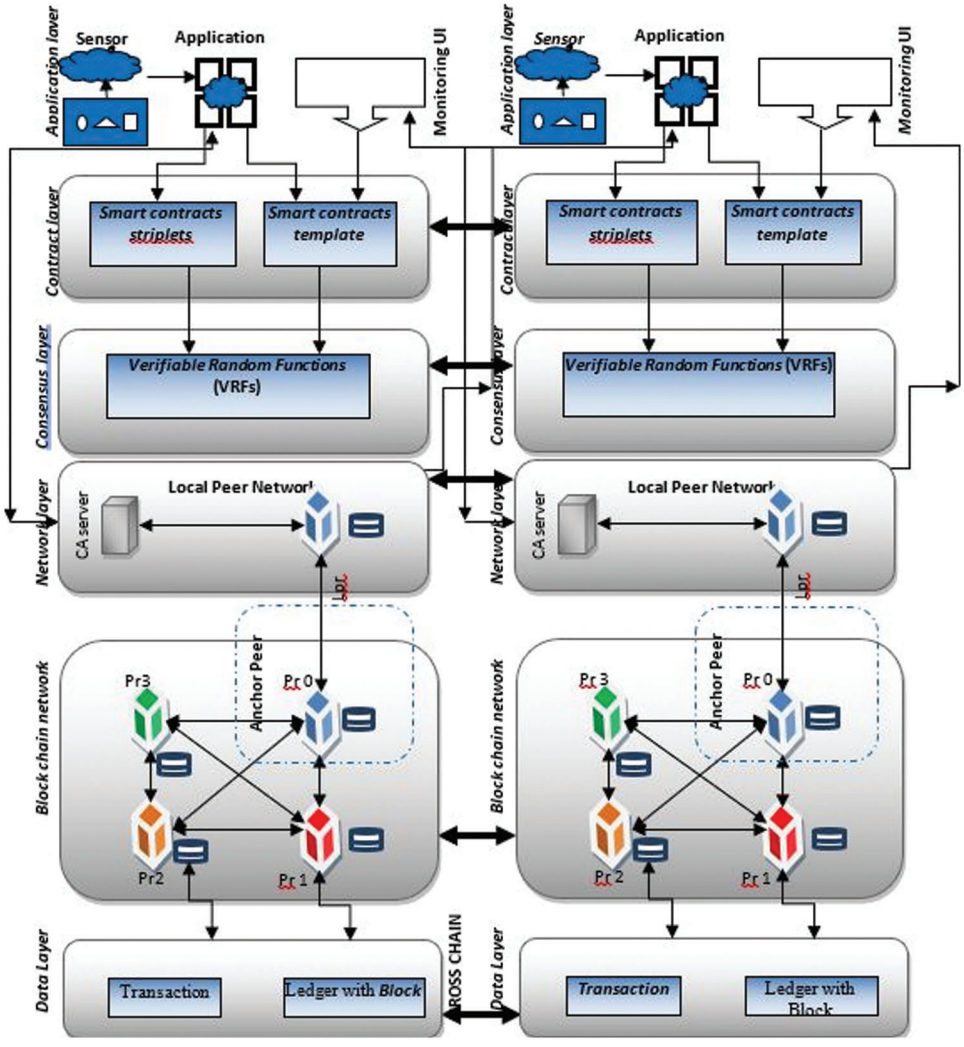


Figure 1: Proposed icbc framework with a local peer-based network model

3.1 Cross Chain in Application Layer

In the global IoTs framework, billions of sensors, actuators, and smart devices used in IoTs are interconnected over the Internet and regulated and managed by applications, which are either firmware or gateway applications. It is assumed by this model that the application stands in for a thing. In this model, front end interaction aided using other network elements has been considered as the responsibility.

3.2 Cross Chain in Contract Layer

To develop the cross-transactions and smart contracts, consider that each application can utilize a Blockchain Standard Development Kit (SDK) since every individual application generates a different format and structure of data. In general, smart contracts are computer protocols that are capable of self-executions and self-verifications as soon as they are implemented. Some of its advantages include real-time updates, precise execution, and reduced human interaction. To broaden contract layers to cross chains, smart contracts need to be initiated from two separate but similar chains. The data is formatted by SDK and cross-transactional information has been taken from various applications by converting them into a standard format to be utilized. Based on a business model and asset definitions, Smart contracts will be applied in the form of chain code. Since the smart contract has referred to global Blockchain networks, it has been utilized in this work [20].

3.3 Cross Chain in Consensus Layer

To assure the stability of states for a blockchain system, the consensus layer is highly significant. Byzantine failures are accompanied by minimal communication cost, for which the author utilized a new Verifiable Random Functions (VRFs)-based method; thereby it can be adopted in the permission-less blockchain [21]. For establishing reliability, Cryptocurrency blockchains have been utilized by applying proof-of-work consensus algorithms. For reinterpreting the consensus protocol, cross-chain interaction has been considered as a verification protocol, thereby the accuracy of the state of a blockchain system can be sustained. The verification protocol plays a vital role to verify whether the data in the source chain has been committed, or the transmitted data has interfered.

3.4 Cross Chain in Network Layer

In the initial phase, the network layer's architectures are intended to provide communications between multiple blockchain system nodes. Blockchains often use the P2P network paradigm to achieve communication decentralization. On recommended Local Peer Networks, Certification Authority (CA) and Local Peer Networks (LPR) are accessible. Several devices are grouped by Lpeer networks, which are employed at organizational levels and based on the application's circumstances. CA verifies and registers network users and/or devices (device certifications and associated smart contracts). Lpeers act as localized peers for organizations and enable communications with Anchor Peers in larger Blockchain networks. It is important to note that Lepers and Anchor Peers are two separate entities with unique roles in the process. The architecture significantly enhanced anchor peer's ledger scalability while also inadvertently increasing cross-transaction rates of peers in Blockchains. Interoperability that connects the cross chains through the passive interoperation has been provided in this layer. Here adopted a Polling-Based Reading (PBR) technique demands the destination chain to consistently try to read information from the source chain repeatedly. Post-completion of a read operation, the destination chain validates the authenticity of the information. Subsequently, the information possessed by the transaction will be proposed to the chain for being committed later. The working phases of the PBR method have been simulated on a virtual machine to assess the I/O overhead. Each virtual machine comprises 1 core of Intel Core i5-4590HQ 2.2 Ghz CPU with 2 GB of RAM, running on Ubuntu 14.04. In the proposed model, divide the local peer into Lpr_0, Lpr_1, to Lpr_N, in which Lpr_0 represents the main instance, to prevent a

single point of failure, the remaining secondary instances are geographically dispersed. If the application needs the consensus of more than one peer for local cross-chain transactions, secondary Lprs may also take part. Ledger replica can also be kept up to date by certain supplementary Lprs. Each device must get registered with Lpr_0, through which each device has been, authenticated through CA and active users' list and their credentials, and smart contracts can be maintained. For reading/writing blocks into the ledger, $Lpr_0$is the only instance admitted and it has the sole responsibility to coordinate with anchor peer, concerning inter-organizational cross transactions.

3.5 Blockchain Network

Because of peer interconnectedness, peers maintain their ledgers and have corresponding smart contracts (chaincodes). In this work's suggested framework, Lpeers communicate with their associated peers in cores (referred to as anchor peers) to support applications (authenticated through CA). There is no change in the process of core Blockchain. For communication with other peers the anchor peer is accountable (and could act as anchor peer for other groups). Pr_0 represents an anchor peer and interacts with Lpr, as illustrated in Fig. 1. The core network of anchor peers performs the inter-organizational transactions. The core Blockchain peer can be connected to clients and can perform as generic peers.

3.6 Cross Chain in Data Layer

In the process of blockchain, data management plays a vital role, by which the data layer can be created along with transaction format, block structure, storage model, etc. [22]. Merging the transaction format would be an uncomplicated and possible idea, for which a generator module has been introduced. And to build a middleware enabling direct communication among blockchains regardless of relay dependency, a data generator has been presented. Further, the most recent blockchain system may simply connect to middleware and use the combined transaction structure. A ledger is a secure, serialized record of every transaction in this tier. Chain code calls performed by members inside the organization produce transactions. Ledger is connected to Lpr_0 the only instance permitted to read/write. If the $Lpeer_0$ is out of service, the self-updating duplicate ledger maintained by Secondary peers has been utilized. In this study, the state database has been utilized by both Lpr and BC for feeding logs to confirm successful transactions.

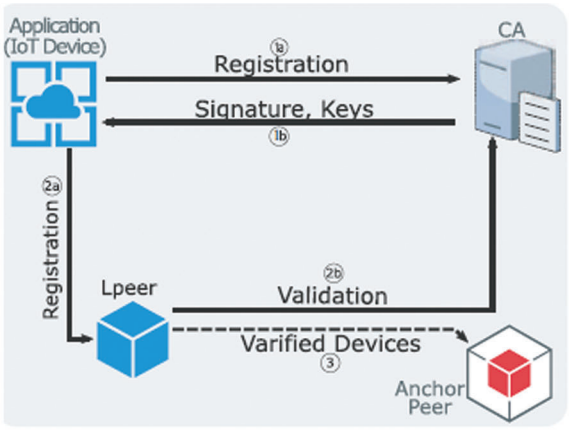
4 Transaction Structure and Processing

The following segments confer the three significant steps involved in the fundamental transaction and processing,

4.1 Device Registrations in IoTs

The sequence of CA and Lpr_0 necessitates every single device used in IoTs to get registered for participating in the process as demonstrated in Fig. 2a. As a first phase, the CA offers an exclusive signature, and the pairs of the encryption key to the devices, as it has the liability to generate and provide the signature, private-public keys, and several certificates, such as eCert, TLS CA, etc., to the device. Subsequently, it registers with $Lpeer_0$, besides the Lpeer0 validates the requester's identity that belongs to CA, during which the $Lpeer_0$ archives the entire credentials (TLS, CA certificates, and signatures) of the device as regards the purpose of future validation. Due to this procedure, the involvement of unauthorized devices used in IoTs have can be prohibited, and only authorized devices used in IoTs can be permitted to be a part of the local Blockchain network, these devices can take part in the global Blockchain network, during which the devices have registered with anchor peer by Lpr_0. Post-acceptance, the CA responds to the device by generating and archiving the signature and cryptographic elements. After the connection of the device de_i with Lpr_0, the registration ID of the device turns out to be Pr_{id}.

De_{id} has preserved to utilize in further steps. Fig. 2b represents the standard formats of Hyperledger and includes a sample for better understanding.



(a)

Transaction from Application to Endorsing Peers

Client ID	Chaincode ID	Trans. Payload	Time stamp	Client Sig.	D Client ID
4ce32c8...	mycc	204c33043d6...	8752475544	0xc421bfc420	2de1f81..
2abc3ef..	mycc1	3045ea3c52..	9924755565	0x24be34c420	2de1f81..

Feed Back from Endorser to Applications

Ep ID	Trans. ID	Chaincode ID	Tr. Cont. Blob	Read set	Write set
8d8a23b...	204c3367b3...	mycc	204c33043d...	1	1
7ebc321e...	125be6183...	mycc	354c33043d...	1	1

Application to Orderer

Seq. No.	Previous Hash	Blob
1	46ee8a063.....	204c33043d...
2	2cd43d22....	3215ef644

(b)

Figure 2: (a) Device registrations in IoTs, (b) Hyperledger's generic transaction format

4.2 Transaction Processing

The Lpr_0 validates the reliability of each transaction by ensuring the transaction is received from a valid user, as depicted in Fig. 2b. The transaction proposal has triggered as a message $TP_{i,j}(Me_{i,j})$ initiated from the device (de_i) to Lpr P_{Lpr}, in which the devices denoted by $i = 1, 2, \ldots, n$; the messages from every de_i signified by $j = 1, 2, \ldots, n$; besides the private and public keys of device de_i indicated by prk and puk, correspondingly. Likewise, a public key of Lpr has been notated as Lp_{puk}, and, the private key of Lpr has been notated as Lp_{prk}. The estimation of the Transaction proposal expressed by,

$$TP_{i,j} = Encr\left(Lp_{puk}\right)\left[Sign(de_i),\ Sign_{Ad}(de_i),\ Hash\left(Me_{i,j}\right)\right] \tag{1}$$

Here, Ad indicates the admin of the device that has connected to the peer. The transaction proposal message $TP_{i,j}$ has been verified and decrypted by peer using the private key. Post-decryption, the entire certificates including the signature of device $Sign(de_i)$ and Lpr admin $Sign_{Ad}(de_i)$ also have been verified by the peer. If each verificationis positive, The Lpr signs and sends a good response to the source application.

The role of the signature has its influence on the secured registration processing mechanism. The following procedure for digital signature generation and verification is as follows. Let the de_i will sign a message $Me_{i,j}$. de_i for creation of one private key integer $de_{prk_i} \in (1,\ n-1)$ and one public key $Q = de_{prk_i} * G$. Here G signifies the elliptic curve generators with large prime order n. de_i select any random integer $k \in (1,\ n-1)$ which is utilized for estimation

$$e = QHash\left(Me_{i,j}\right) \tag{2}$$

and curve point is assessed as

$$(x_1,\ y_1) = k * G \tag{3}$$

where the leftmost part of e is z. The slight alteration of the Quantum Walks (QW) model results in Quantum Hash (QHash) [23]. QHashes are greatly utilized for generating pseudorandom numbers due to their intrinsic

chaotic dynamics. There exist two quantum systems, walker and coin in simple discrete QW [24]. A vector in the Hilbert space is involved in notating the walker-coin system state.

$$H_t = H_p \otimes H_c \tag{4}$$

where the subscripts p and c signify walker and the coin, respectively. The coin state through a conditional shift operator is used to condition the movement of the walk

$$S = \sum\nolimits_x (|x+1,\ 0\rangle\langle x,\ 0| + |x-1,\ 1\rangle\langle x,\ 1|) \tag{5}$$

where the summation symbol represents the sum over all possible positions. The implementation of the total quantum system is accomplished by the global unitary operator repetition.

$$U = S(I \otimes C) \tag{6}$$

where I represents the identity operator and C denotes the coin operator applied on the coin state. Hence the final state $|\psi\rangle_t$ after t steps are articulated by

$$|\psi\rangle_t = (U)^t|\psi\rangle_t = \sum\nolimits_x \sum\nolimits_v |x,\ v\rangle \tag{7}$$

and the probability of locating the walker at position x after t steps is

$$P(x,\ t) = \sum\nolimits_{v \in \{0,1\}} ||x,\ v|(U)^t|\psi\rangle_{initial}|^2 \tag{8}$$

where ψ initial notates the total quantum system's initial state. The coin operator involved in discrete-time QW is made static. The main components in the resulting probability distribution are the original coin state and the step number. Allow the binary string to be, i.e., the message is dependent on the coin operator at each step, and given that construction of a QHash is accomplished, as like preceding work [25]. The constructed QHash inputs are binary strings, i.e., the output hash values are derived from messages $Me_{i,j}$, and resulting probability distributions P (x, t). The control arguments are the state of the coins, hence QHashesd that are created are keyed. The n^{th} step of the walk is managed by the nth bit of the message. The constructions of QHashes are as follows:

- Select parameters (n, (α, β, χ, δ)) and messages $Me_{i,j}$ with arbitrary lengths.
- Run one-dimensional two-particle discrete-time QW on a circle under the control of the message $Me_{i,j}$ and produce the output hash value QHash, i.e., the probability distribution. Here α, β, χ, δ represents the amplitudes of the initial coin state $|v,\ \tau\rangle = (\alpha\ |00\rangle + \beta\ |01\rangle + \chi\ |10\rangle + \delta|11\rangle)$. n denotes the node number of a circle.
- All the values in the resultant probability distribution should be multiplied by 108 modulo 256 to create a binary string that serves as the hash value or secret key prk.

The following conditions have been verified for validation of the hash key function.

Condition 1: The original message $Me_{i,j}$;

Condition 2: Vary the 8th bit from 0 to 1;

Condition 3: Remove the last bit of the message $Me_{i,j}$;

Once the hash values are obtained then compute $r = x_1 \mathrm{mod} n$ and $s = k^{-1}\left(z + rde_{prk_i}\right)$ where $r \neq 0$ and $s \neq 0$. Lastly, the signature is the pair (r, s). Lpr substantiates and consents the signature primarily as valid, if $(r,\ s) = 0$, or else discards.

4.3 Transaction Flow

There involve two sorts of the transaction from device perception in Blockchain-based IoTs. 1) Transactions amid devices enumerated with identical Lpr, and 2) Transactions amid devices enumerated with dissimilar Lprs [26]. The paper describes the two types of transactions elaborately.

5 Implementation and Evaluation

The evaluations are mainly affected due to the rapidly varying architectural platforms. The proposed ICBC is assessed through the probable particulars of the testbed in the forthcoming section. The technical particulars are necessitated for analyzing the performance variation due to the minor configuration variations significantly.

5.1 Hyperledger Testbed Setup

Hyperledger Fabric (v1.0.2) is mainly utilized for the planned ICBC framework along with the prevailing approaches. Test beds encompassed two machines with subsequent conditions for emulating topologies: a) 2.7 GHz, Intel i-7, 16 GB 1600 MHz DDR3, and b) 3.0 GHz, Intel i-5, 8 GB 1600 MHz DDR3. The Lpeer Network has been emulated by the first machine and the global Blockchain is been emulated by the second machine. The peers are run through the Ubuntu container-based virtualization technique. Smart contracts were mainly involved in generations of messages with a JSON payload sent to a local peer continuously who had single orderers, single peer organizations, single channels (lchannels), and single ordering services. Two organizations were in charge of building four worldwide Blockchain network peers, and an ordering service t connected to the Kafka-Zookeeper. The Configtxgen tool was heavily used for constructions of genesis blocks, which were the first blocks of Blockchains without hashes for preceding blocks and one channel which broadcasted transactions to orderers, and one anchor peer alongside Lpeers. All members use the location of the Membership Service Provider (MSP) route. In terms of the number of transactions per block, the maximum size of a block, and the maximum amount of time to wait for transactions, the order describes transaction configuration or structure. Adjust these variables appropriate to the needs of the research in this Lpeer arrangement (described later). Blockchain networks mostly use the Kafka consensus algorithm.

5.2 Block Weight & Ledger Scalability Analysis

The ledger's continuously expanding list of ordered transactions, known as blocks, is significantly dependent on blockchain. The block number is distinct and is distributed in steps starting at zero. Except the genesis block, there is also a connection between the earlier blocks. There are three parts to each block: the header, the transaction details, and the metadata. There are three parts to each block: the header, the transaction details, and the metadata. Blockchain maintains a continuously expanding list of sequential transactions, or blocks, in the ledger. Each block number is unique and is assigned in a straight line starting at zero. Each brick, except the genesis block, is connected to the one before it. There are three parts to each block: the header, the transaction details, and the metadata.

Individual Block Weight: This is a reference to how much RAM is needed to store the block. Block size, which describes the number of transactions included in a block, is different from this. For the block content, the string form of storing is used in addition (i.e., a 4-byte integer may proceed with additional memory after transforming). The actual weight of the ledger kept on the peer nodes in the event of analysis is observed to determine the true memory required. According to several investigations, the average block weight perceived with a single transaction that was approved by a single peer was 4:6 KB. The value of a transaction is strongly influenced by its weight, the number of transactions in a block, and the number of peers supporting it, since all endorsers' signatures are included in transactions, weights increase with counts of endorsing peers.

5.3 Block Weight vs. Concurrent Transactions

Instead of the current bitcoin transactions, devices employed in IoTs enable the production of transactions at a far higher pace. As a result, it is imperative to fully investigate how adding more concurrent transactions from applications may affect block weight. For production-level systems that permit the examination of a greater number of transactions in a block, the batch timeout of the 50 s (block closure time) is seen as being too lengthy. 100 MB of data can be sent in each batch, with a maximum of 2 K messages per batch. The maximum number of bytes for each message is 512 KB. As a result, investigate the impact on block weight as the number of concurrent transactions from applications increases.

In Fig. 3, the block weight is plotted against the number of transactions issued by apps. For comparison, the standard BC, Local Peer-based BC (Lpeer-BC), and ICBC framework are used. The chance of an intra-organizational transaction is 0.7, which is a notable aspect. The block weight of Lpeer-BC and ICBC is increasing, but not at the same rate as conventional BC architecture. Transactions are partitioned among Lpeer-BC and ICBC based on transacting parties, resulting in a decrease in block weights. Furthermore, Lpeer-BC has a higher block weight than ICBC because of the greater number of transactions per block. Even though the ICBC obtains fewer transactions for the development, validation by four peers increases block weights. The block weight for the ICBC framework has increased due to the participation of more peers in production contexts.

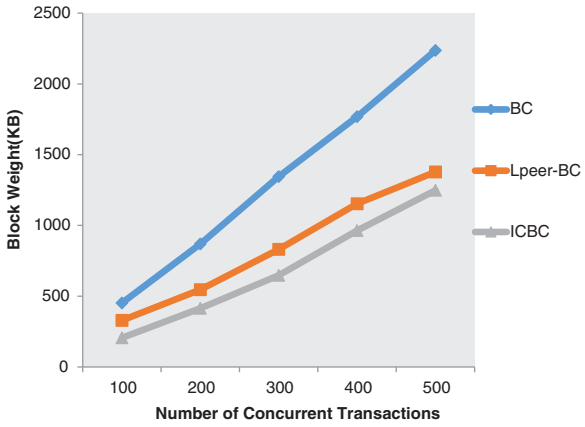


Figure 3: Block weight for concurrent application transactions

Fig. 4 depicts the scalability of the ledger in three frameworks. The sequential ordering of blocks produces block height, which is proportional to counts of blocks added to ledgers, thus memories have cumulative storages. Genesis block (Block 0) receives roughly 12 KB, Block 1 contains only instantiated data covering a single transaction. In the case of a normal BC network, the block size grows dramatically from block 2 to block 11. The proposed ICBC framework ledger demands a reduced quantity of memory resources for an equal number of transactions and blocks. Additionally, because the blockchain network's peers all keep duplicates of the same ledger, total usage is proportional to the counts of peers. Lpeer-blockchain is more scalable across many IoTs domains since there is just one ledger per business.

The interoperability effects are mainly assessed through monitoring of CPU utility in the anchor node for every node. Fig. 5 reveals the average input data sizes obtained through blockchain approaches and also based on the number of destination chains about CPU utility are also exposed. The ICBC method, therefore, produces enhanced scalability with enormous destination chains with a small upsurge in overheads.

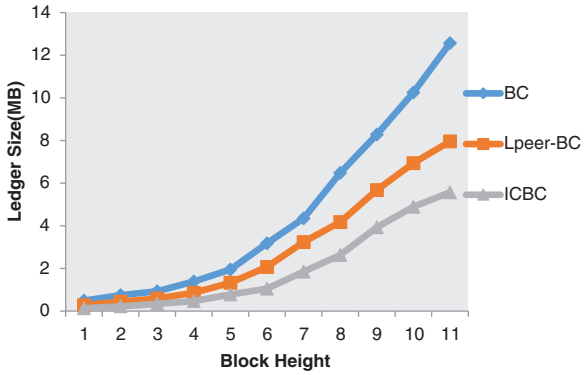


Figure 4: Scalability of ledger memory

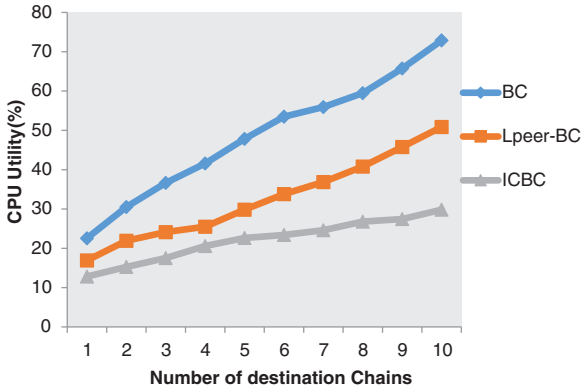


Figure 5: Impact of CPU utility *vs.* block chain methods

Fig. 6 depicts a comparison of current approaches to communication overhead. The communication cost comparison using different approaches is displayed in Fig. 6, along with the total number of devices used in IoTs. The quantity of devices used in IoTs has a direct impact on communication overhead. In comparison to previous approaches, the greater the number of devices used in IoTs, the lower the communication overhead. When devices used in IoTs are upraised, the proposed methodology performs better.

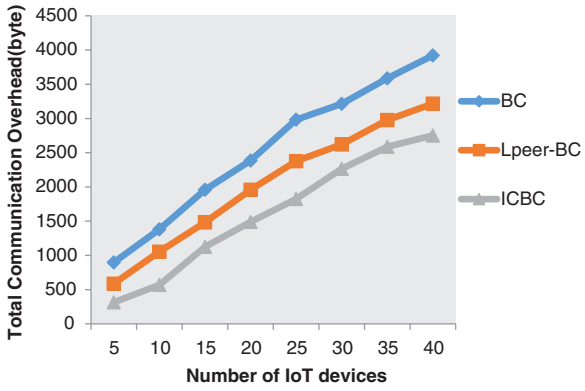


Figure 6: Impact of communication overhead *vs.* block chain approaches

6 Conclusion and Future Work

This research concentrates on inter and intra-organizational transactions encompassed in IoTs background by utilizing the notion of Interoperability Cross-Block Chain (ICBC). A registration process is performed by the local Certification Authority (CA). It is mainly used to interrelate the devices to an organization and all devices used by IoTs. A cross-chain-based local peer network supports greatly permitting the Blockchain ledger to scale through all peers. The interoperability is another support provided by the ICBC notion with two main tasks. The reading overhead is mainly mitigated through the maintenance of interoperation timeliness. Furthermore, Quantum Hash (QHash) function is mainly utilized for the security of proposal transactions amid the device's transaction. Various factors are achieved with betterment results such as ledger weight, CPU utilization, scalability, and communication overhead which are validated by the results. Additionally, greater scalability and interoperability enable large-scale commercial transactions in IoTs, as well as memory necessary to solve issues for block storage. In the future, it may be advised to enable either a uniform transaction arrangement optimized for various types of business chain arrangements through interoperability among diverse chains.

Acknowledgement: We thank the anonymous referees for their helpful suggestions.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. M. Farhan, "Effect of rotation on the propagation of waves in the hollow poroelastic circular cylinder with the magnetic field," *Computers, Materials & Continua*, vol. 53, no. 2, pp. 129–156, 2017.

[2] M. Kubendiran, S. Singh and A. K. Sangaiah, "Enhanced security framework for e-health systems using blockchain," *Journal of Information Processing Systems*, vol. 15, no. 2, pp. 239–250, 2019.

[3] Z. Xiong, Y. Zhang, D. Niyato, P. Wang and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[4] Q. Feng, D. He, S. Zeadally, M. K. Khan and N. Kumar, "A survey on privacy protection in the blockchain system," *Journal of Network and Computer Applications*, vol. 13, no. 1, pp. 45–58, 2018.

[5] H. W. Kim and Y. S. Jeong, "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain," *Human-Centric Computing and Information Sciences*, vol. 8, no. 11, pp. 1–13, 2018.

[6] S. Aggarwal and N. Kumar, "Hyperledger," *Advances in Computers*, vol. 121, pp. 323–343, 2021.

[7] E. Androulaki, A. Barger and E. Bortnikov, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. of Thirteenth EuroSys. Conf.*, Porto, Portugal, pp. 1–15, 2018.

[8] M. Nofer, P. Gomber, O. Hinz and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[9] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. 2017 IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PerCom. Workshops)*, Kona, HI, USA, pp. 618–623, 2017.

[10] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[11] M. Banerjee, J. Lee and K. K. R. Choo, "A blockchain future for internet-of-things security: A position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[12] A. Reyna, C. Martn, J. Chen, E. Soler and M. Daz, "On blockchain and its integration with IoT challenges and opportunities," *Future Generation Computer Systems*, vol. 88, no. 11, pp. 173–190, 2018.

[13] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli *et al.,* "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[14] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[15] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and privacy," *Journal of Parallel and Distributed Computing*, vol. 134, no. 12, pp. 180–197, 2019.

[16] P. K. Sharma, S. Singh, Y. S. Jeong and J. H. Park, "Distblocknet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[17] S. Biswas, K. Sharif, F. Li, B. Nourand and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, 2018.

[18] K. Abbas, L. A. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy *et al.,* "Convergence of blockchain and IoT for secure transportation systems in smart cities," *Security and Communication Networks*, vol. 2021, no. 5597679, pp. 1–13, 2021.

[19] P. Zhang, Y. Wang, G. S. Aujla, A. Jindal and Y. D. Al-Otaibi, "A blockchain-based authentication scheme and secure architecture for IoT-enabled Maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2022.

[20] Y. Gilad, R. Hemo, S. Micali, G. Vlachos and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. of the 26th Symp. on Operating Systems Principles*, Shanghai China, pp. 51–68, 2017.

[21] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi *et al.,* "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[22] I. O. Kennedy, C. K. Lin and V. Venkateswaran, "A cross-layer design and evaluation of IEEE 802.15.4 network with an enhanced sensor gateway: Injecting hierarchy into wireless sensor networks," in *Proc. of IEEE Int. Conf. on Communications*, Budapest, Hungary, pp. 1694–1699, 2013.

[23] S. Elías and V. Andrea, "Quantum walk a comprehensive review," *Quantum Information Processing*, vol. 11, no. 5, pp. 1015–1106, 2012.

[24] D. Li, J. Zhang, F. Z. Guo, W. Huang and Q. Y. Wen, "Discrete-time interacting quantum walks and quantum hash schemes," *Quantum Information Processing*, vol. 12, no. 3, pp. 1501–1513, 2013.

[25] J. A. Izaacand and J. B. Wang, "pyCTQW: A continuous-time quantum walk simulator on distributed memory computers," *Computer Physics Communications*, vol. 186, no. 1, pp. 81–92, 2015.

[26] X. Zhan, H. Qin, Z. H. Bian, J. Li and P. Xue, "Perfect state transfer and efficient quantum routing: A discrete-time quantum-walk approach," *Physical Review*, vol. 90, no. 1, pp. 1–5, 2014.