# PoAh: Proof-of-Authentication for Post-Blockchain Based Security in Large Scale Complex Cyber-Physical Systems

**Dr. K. Sai Manoj**
CEO, Amrita Sai Institute of Science and Technology / Innogeecks Technologies

## ABSTRACT

The internet of things is the network of physical objects which are connected or embedded with sensors, software, and other technologies to exchange data with other device or system via the internet. The blockchain can be used to track the sensor data measurements and prevent duplication with manipulation data. Blockchain enriches the IoT devices to improve and extend security by the means of bringing transparency to the IoT ecosystem. Blockchain is a system of recorded information so it is impossible to change, hack, or cheat the system. But blockchain faces a lot of disadvantages as it uses more energy, it was not distributed among many computing systems, they are not immutable, etc. This research paper is about the post-blockchain structure that integrates a multi-blockchain in one ledger using a directed acyclic graph (DAG) structure called a multi-chain. Blockchain is a DAG that combines the internet of things to make the machine-to-machine transactions more possible. This multi-chain model helps in solving expandability and storage capacity which is the replacement for the old conventional blockchain on the internet of things. This research is proposed with a new framework called the Proof-of-Authentication the PoAh. This helps in improving the latency which is considered as one of the important factors in the internet of things devices. The PoAh is 4000× approximately faster than that of PoW the proof-of-work and it is also faster than that of the PoS the proof-of-stake which is 55× faster approximately.

**Keywords**
Blockchain, IoT applications, Proof-of-work, Proof-of-Authentication, Directed acyclic graph.

*Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020*

## Introduction

[1-3] a blockchain is a system of recorded information so it is impossible to change, hack, or cheat the system. The blockchain allows the interaction by the user or among the user without the involvement of anyone.

There may be a situation of distrust among the business parties or those who are participating in this scenario were blockchain is designed with more transparency, security to avoid cheating or misleading of information, and tracking or tracing of information which will help understand the misleading.

Blockchain has highlighted its strength and capacity in many functional areas and it also plays an important role in IoT. The internet of things is the network of physical objects which are connected or embedded with sensors, software, and other technologies to exchange data with other device or system via the internet.

Some common examples of IoT are the Air conditioner which can be operated and accessed using our smartphones. In smart cars, it is used in providing the shortest route. Our smartwatches which are used to control our daily activities. All these devices use IoT. The devices with IoT reduces human intervention.

Still, certain problems remain unaddressed they are providing security and safety for our data in the devices with the internet of things because the information which is sensitive like about our health, location of our place, etc are collected. But still, the importance of blockchain with the combination of IoT was investigated in order to know the importance of it yet the question remains unanswered.

This research paper tries to showcase the blockchain attribute which would add value or advantages to the internet of things(IoT) applications.

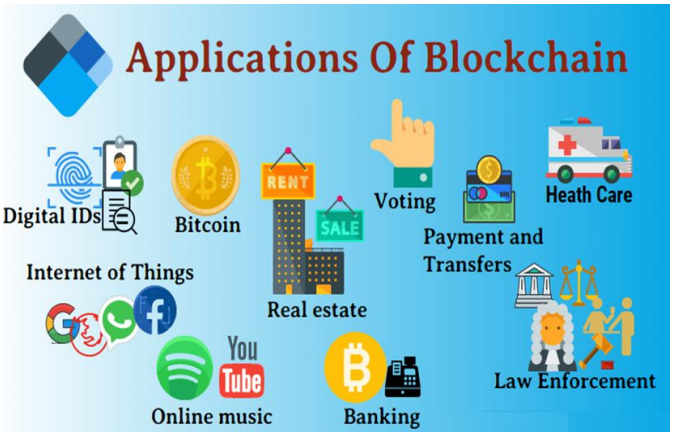



**Figure 1** Applications of Blockchain

The consensus algorithm which includes PoW, PoS, PoA, PoC, PoBT, PoV. Among these consensus algorithm few of them suits with the internet of things constrained device. This research is divided into 6 sections.

## Background

The concept of blockchain and IoT are displayed in further process in this study. For the deep understanding of blockchain and IoT concepts.

### 2.1 Blockchain Overview

the properties of blockchain with 3 known technologies as follows:

1. Cryptography
2. Peer-to-peer networks
3. Consensus mechanics

Cryptography: In the blockchain, a block being referred to the collection of data, records, and the blocks related to the public database are stored in the list. These lists are linked to cryptography making it the most essential and fundamental requirement of creating a blockchain. The blockchain makes use of 2 algorithms of cryptography.
Peer-to-peer network: The P2P network enables all the network together in order to avoid failure from a single point of view and this P2P network which helps in avoiding the help of middleman between the networks.
Consensus mechanics: The consensus network in the blockchain is a procedure through where all the peers of the network reach a common agreement about the DAG. In this, a common agreement is tried to found to in the entire network.
The main aspects of blockchain are:

- The transaction are the one developed by participating nodes in the network which are later broadcasted to the entire network.
- The blocks are considered as the group of transactions which are added to the block after validation.
- The blockchain is considered as the ledger of all the created blocks which helps in setting up the entire network.
- The blockchain depends on public network to connect it with various blocks together.
- The consensus mechanism is the one which makes the decision in adding the blocks in blockchain.

The features of blockchains are decentralization, transparency, data protection, relative user autonomy, and security. For those who have no idea about this present topic it may be not familiar for them to choose the right properties and platform. The most important 3 blockchain platforms are discussed below:

#### 2.1.1 Public Permissionless

The public permission less is a one which creates less trust environment by which anyone can run a node and can be added in the network with these characters :

- The network access is open to all
- All nodes can engage in consensus protocol
- The ledger transcation can be read by anyone.

#### 2.1.2 Public Permissioned

The public permissioned is a hybrid model connecting the less trust environment of public blockchain and highly trusted model in private blockchain.

- The pre-selected node controls the network access.
- The pre-selected node controls the consensus model.
- The right to read is restricted.

#### 2.1.3 Private Blockchains

The participants are added and validated based on the central-based system in the private blockchains. This is similar to the conventional central-based system with cryptography protocol. The characters of private blockchains includes:

- Single system controls the network access.
- Single system controls the consensus protocol
- The right to read is restricted.

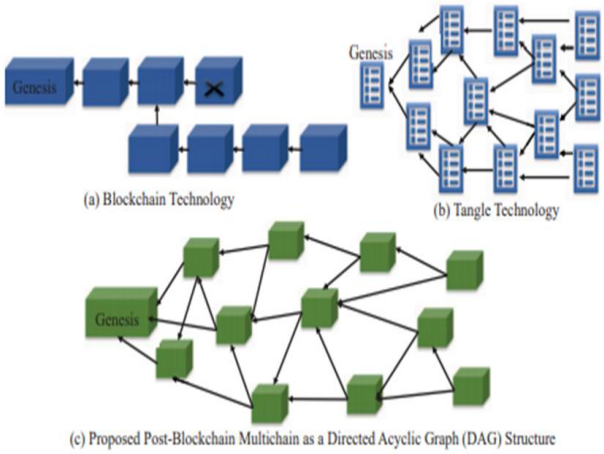



**Figure 2:** Ledger Structure for: (a) Blockchain Technology, (b) Tangle Technology, and (c) the Proposed Post-Blockchain Technology

### 2.2 IoT

The internet of things is the network of physical objects which are connected or embedded with sensors, software, and other technologies to exchange data with other device or system via the internet. The IoT uses M2M interaction between these devices connected with sensors. In this case, human intervention and interaction are avoided easily. The M2M helps the devices to act independently and autonomously.
Some common examples of IoT are the Air conditioner which can be operated and accessed using our smartphones. In smart cars, it is used in providing the shortest route. Our smartwatches which are used to control our daily activities. The communication with one device to the device but trust and relationship is created between these automatic devices. But in recent days with so much up-gradation in devices and technology, we are highly concerned about the security and our data privacy. There is a possibility for us to share our sensitive data like location, health, etc. the large scale must be capable enough of maintaining our data carefully and sustain privacy.

## Blockchain Advantages for IoT

In the present time, the internet of things has chosen client planning with central based trust brokers and with security protocols like SSL protocol and the TLS protocol. This protocol has worked successfully for many years. But the central based cannot keep in watch the data of each and every person. This centrally based system may also fail due to the number of servers connected to the IoT system these days.
But in the case of blockchain, it has showcased its prospective in many fields including the financial sector. We may trust that Internet of things domain can also benefit from blockchain technology in the process of establishing the challenges. There are many security-related problems faced by IoT. In this research paper, we try to focus on a few

challenges by IoT which could be solved with the help of the blockchain mechanism.

### 3.1Confidentiality and Integrity

All the internet of things devices is implemented with sensors one of the tasks for IoT is to collect the data and craft the data related to their environment/surroundings, location, and the state/country. But the conventional IoT was connected with data about our day to day activities.
When we share our data the insecurity about the privacy of those data always arises in the minds of the users. With all these issues the implementation and execution of innovative ideas to protect data at the same time may not reach the spot where it has to be and attention among the users is also not reached. Sometimes the privacy concerns are based on the decision of the users but the sensitive data about health care etc must be given attention in the IoT devices.
When the blockchain mechanism applied with IoT devices it becomes difficult to corrupt our devices and data in it

- The fixed cryptography with the process of data verification can be shared with other members in the network.
- Checking the network transaction before receiving them.

The linked blocks in the blockchain make it harder to break them. When confidential data have shared the blockchains see to the data sent in form of codesor converting the data to prevent them from unauthorized access.

### 3.2 Autonomous Behavior

The IoT devices provide the power of autonomy to its users. By the means of interacting with devices relating to the issue, we face in the device without any human intervention. For developing such a model there must be a lot of integration and up-gradation in the properties of the devices. The autonomous nature of IoT opens up for an extendable platform for several applications such that smart communication and connectivity.
[4,29] even the blockchain plays an important role in giving autonomy to its users through smart contracts. These are the self-executing programs which are operated automatically in the blockchain mechanism. The IoT device can be connected with smart contracts which will enable the interaction with the entire network. Example the details of credits or transactions after payment. The smart contract in the blockchain is highly protected with cryptographic protocols so the data in it cannot be manipulated so easily.

### 3.3 Fault Tolerance

When the devices are hacked on the IoT network the device must be capable enough of securing the data or protecting it. The main function of the blockchain is increasing the fault-tolerance in some case the hacked data may not attack the entire network. The decentralized architecture of blockchain also allows for lighter, faster, more reliable, and secure communication between nodes.

**Table 1:** A Comparative Perspective of Blockchain, Tangle, and the Proposed Multi-Chain.

| Features | Blockchain Technology (for Bitcoin) [6], [14] | Proof of Authentication based Private Blockchain [15] | Tangle Technology (for Cryptocurrency) [8], [16] | HashGraph Distributed Ledger Technology [17], [18] |
|---|---|---|---|---|
| Linked Lists | • Linked list of blocks<br>• Each block contains multiple transactions | • One linked list of blocks<br>• Each block contains multiple transactions | • DAG linked list<br>• One transaction | • DAG linked List<br>• Container of transaction hash |
| Validation | Mining | Authentication | Mining | Virtual voting (witness) |
| Type of Validation | Miners | Trusted Nodes | Transactions | Containers |
| Ledger Requirement | Full ledger required | Full ledger required | Portion based on longest and shortest paths. | Full ledger required |
| Cryptography | Digital Signatures | Digital Signatures | Quantum key signature | Digital Signatures |
| Hash Function | SHA 256 | SHA 256 | KECCAK-384 | SHA 384 |
| Consensus | Proof of Work | Cryptographic Authenti-cation | Proof of Work | Asynchronous Byzantine Fault Tolerance (ABFT) |
| Numeric System | Binary | Binary | Trinity | Binary |
| Involved Algorithms | HashCash | No | • Selection Algorithm<br>• HashCash | No |
| Decentralization | Partially | Partially | Fully | Fully |
| Appending Requirements | Longest chain | One chain | Selection Algorithm | Full Randomness |
| Energy Requirements | High | Low | High | Medium |
| Node Requirements | High Resources Node | Limited Resources Node | High Resources Node | High Resources Node |
| Design Purpose | Cryptocurrency | IoT Applications | IoT Cryptocurrency | Cryptocurrency |

## Novel Contributions of the Current Paper

Blockchain is a system of recorded information so it is impossible to change, hack, or cheat the system. But blockchain faces a lot of disadvantages as it uses more energy, it was not distributed among many computing systems, they are not immutable, etc. In order to over comes the limitations of the blockchain it has been explored to find solution for those. Tangle is considered a successor of blockchain technology
In this research to advance state-of-art of the tangle technology for the purpose of speeding up the post-blockchain mechanism as a multi-chain paradigm.
The contribution of the paper towards multi-chain paradigm:

- The SUIL (secure unique identification list) is used for authenticating all parts of the nodes.
- This proposed protocol uses DBL (Dynamic block list) which speeds up the authentication process.
- All the nodes in this protocol can be broadcasted with authentication of all the transaction this shows the integrity of authority distribution.
- The Dynamic block list is distributed to all the nodes. The DBL will be reduced to the least version.

**Table 2:** Nodes Timing Analysis for PoAh for 5 Nodes.

| Time (ms) | Authentication (ms) | Reduction (ms) |
|---|---|---|
| Maximum | 18.13 | 2381.7 |
| Minimum | 3.77 | 307.45 |
| Average | 20.32 | 723 |

**Table 3:** Timing Analysis for PoAh for 10 Nodes

| Time (ms) | Authentication (ms) | Reduction (ms) |
|---|---|---|
| Maximum | 6.7 | 1570 |
| Minimum | 2.37 | 278.9 |
| Average | 578 | 850 |

**Table 4:** Timing Analysis for PoAh for 15 Nodes

| Time (ms) | Authentication (ms) | Reduction (ms) |
|---|---|---|
| Maximum | 4.85 | 2483.7 |
| Minimum | 2.52 | 278.4 |
| Average | 45.25 | 790.75 |

## Blockchain Technology Versus Tangle Technology Versus Proposed Multi-Chain

This section is here to present the comparison between the blockchain model along with the Tangle and the multi-chain protocol. This comparison is illustrated in the fig 2 and the result of it is summarized in tabulation 1

### 5.1 Blockchain Technology and Limitations

[6,14,34] in blockchain technology, the PoW is considered as an important consensus for the validation of a group of transactions. The blockchain technology is the linked group of blocks in it where the data are distributed to all the blocks. In the linked list the transaction is displayed in a public ledger by the users and the transaction is validated by the miners. The blocks must be displayed in public ledger for 2 reasons: honest publisher and the with consistent order. The current operation faces scalability issues such as cryptocurrency, storage of bitcoin, etc have a direct link with the expansion of ledger. With gradually increases the fees and the cost of operation. This was considered as one of the reasons for a business to avoid the usage of blockchain technology. The proof-of-work has been developed for the technology behind the concept of cryptocurrency because they are not suitable for the application of the internet of things due to the usage of more resources.

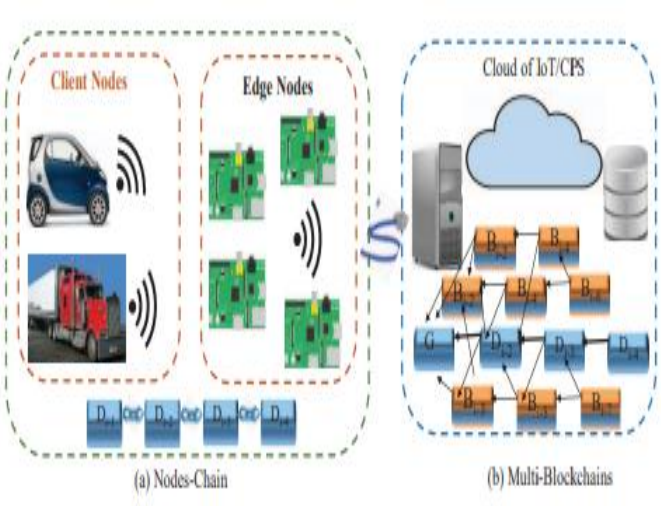



**Figure 3:** Illustration of Post-Blockchain Multi-Chain Technology in a Transportation CPS Infrastructure

### 5.2 Tangle Technology

[8,15,16] tangle is the technology that helps in reducing the cost of the operation in the blockchain. The tangle uses the DAG which is the perfect scalable structure and the one which encourages independent transaction with PoW without the involvement of miners. Many factors are involved with this process such as selecting the algorithm for the location, and the longest and shortest route for ledger minimal version. The tangle model has been liked due to the directed acyclic graph. It removes the involvement of miners in the decentralized structure and it also reduces the cost. This process needs resources to be performed as a complete protocol.

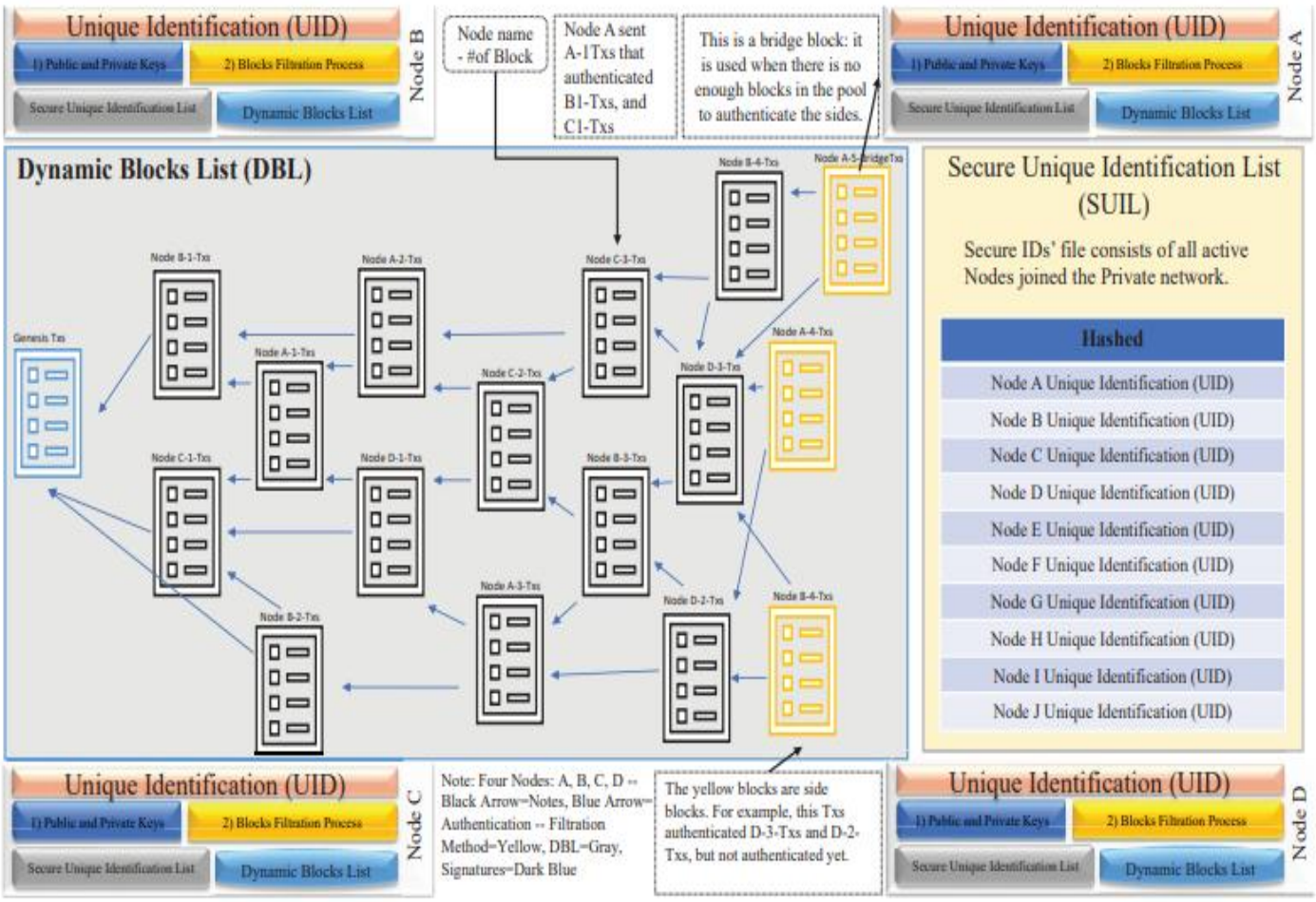



**Figure 4:** A Detailed Depiction of The Proposed Consensus Algorithm Operation in the Multi-Chain Framework.

### 5.3 Proposed Novel Post-Blockchain Multi-Chain Technology

The proposed model for the research the multi-chain technology is illustrated in fig 2.

This model can give a solution to many issues like miners, scalability, and latency which was faced by the conventional blockchain model. The proposed model combines the conventional blockchain model along with the DAG using a unique identification process through a private model for the purpose of authentication of blocks. With this protocol, the cost will be reduced and the involvement of miners will be eliminated. Which will save 50 percent of attack in proof-of-work and the priority in the selection of proof-of-stake is tabulated in 1.

The blocks of the blockchain are strongly connected with the referenced to the previous one instead of the conventional model. These blocks are consistent and can even grow with the existence of malicious blocks illustrated in fig 5. The unauthenticated blocks will be abandoned when the participants de-authenticate it. The abandoned block will not cause any effect on the growth of the ledger.

The topology of the multi-chain model neglects time constraints between the blocks because the time consensus is applied for the side blocks. The preference of the side blocks is based on the time consensus which will always use the median time of the chosen blocks. Before the broadcast, the blocks are identified in the ledger.

.

## Proposed Novel Post-Blockchain - Multi-Chain

The proposed multi-chain algorithm contains 4 important parts the DBL, SUIL, transaction, and the block content.

### 6.1 Dynamic Blocks List (DBL)

The DBL is the structure that stores data in topology order. This has 2 stages. The 1st one is the unauthenticated block and the 2nd one is the authenticated block. The vertices are arranged in perfect order which shows that the ordering of the block is done with complete fairness.

All the blocks reach the genesis block with the space between each vertex. The path of the genesis block is used for the identification of the storage volume of the nodes.

The DBL contains 2 arcs that are attached to all blocks. This used for the authentication of 2 blocks using one block. The speed is improved in this process.

For increasing the speed of authentication more blocks are added to the multi-chain protocol.

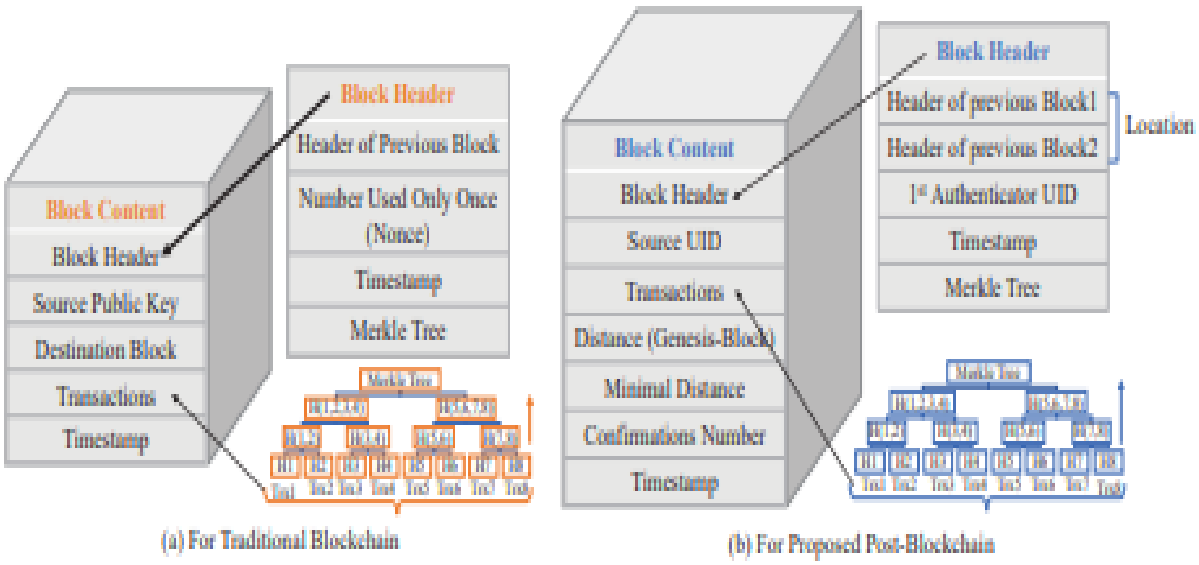



**Figure 5:** The structure of block in the proposed post-blockchain.

### 6.2 Secure Unique Identification List (SUIL)

The secure unique identification is the process of storing unique identification. The UIDs are connected to the nodes in the multi-chain privately. Fig 4 illustrates the SUIL with UID. The unique identification is also responsible for the transaction along with DBL. the idea behind having UID which helps in matching with the points of the UIDs in the block with that of the existing SUIL.

### 6.3 Block content

The block content is illustrated in fig 5 along with the Merkle tree. These blocks contain 4 parts: the header of the block, the source for unique identification, the data, and the timestamp. The header of the block contains header 1 and header 2 of the previous blocks. It also contains a Merkle tree and timestamp.

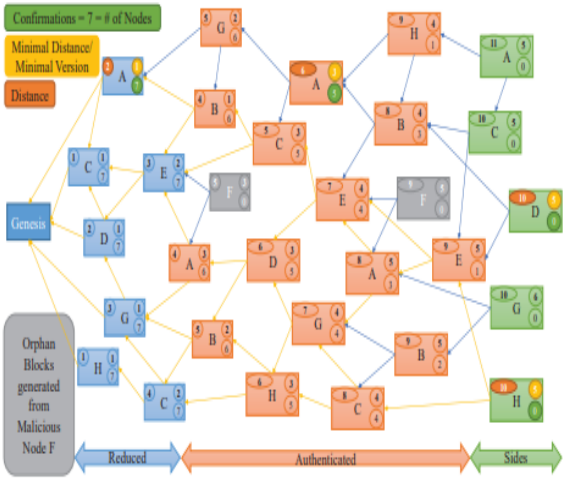



**Figure 6** Illustration of actions of the proposed PoAh Algorithm in post-blockchain.

**Algorithm 1** Proposed PoAh

**Algorithm 1:** Procedure of the Proposed PoAh.

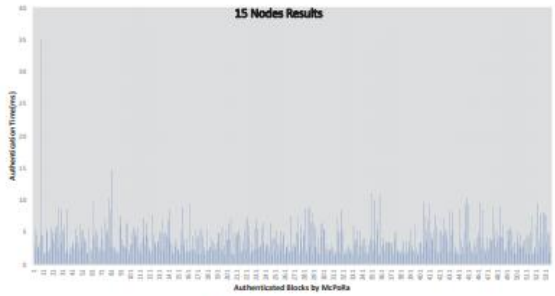
**Inputs :** All nodes in the network follow $SHA-256$ hash. Individual nodes have private $(PrK)$ and public keys $(PuK)$.

**Outputs:** Validated Blocks which are added to the blockchain.

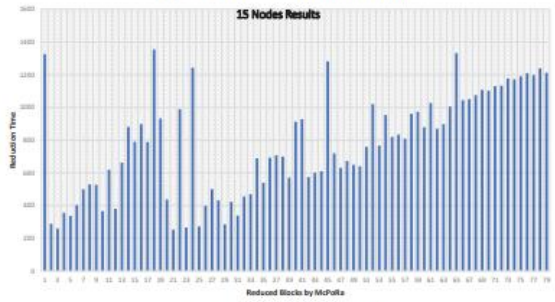
1 $(Trx^{+}) \rightarrow$ blocks; /* Nodes combine various transactions to form the blocks */
2 $(S_{PrK})$(block) $\rightarrow$ broadcast; /* Nodes sign blocks with private key and broadcast to network */
3 $(V_{PuK})$(block) $\rightarrow$ MAC Checking; /* Trusted node verifies signature with source public key */
4 **if** *Authenticated* **then**
5 $block||PoAH(D) \rightarrow$ broadcast; /* Trusted node broadcasts the authenticated block to network */
6 $H(block) \rightarrow$ Add blocks into chain; /* If nodes hear from trusted node, they add block to blockchain */
7 **else**
8 DROP the block; /* If not authenticated, drop the block */
9 GOTO $(Step-1)$ for next block;

### 6.4 Proposed Algorithm and It Operations

The nodes of the protocol are supposed to be predefined and should be granted by Unique identification from the network. After the nodes finished collecting data it forms a block, the DBL is filtered for choosing the location of the newly generated block with the specification of the two sides of the block and then authenticating them. After the block is in the authenticated process of the dynamic block. The algorithm 1 shows the process of data collection from the nodes, and authentication of the earlier blocks and then adding it to the newly generated block for the further step of the un-authentication process in the DBL. the new nodes generated by the new block will also follow the same steps. The proposed algorithm is illustrated in fig 6.




(a) for Block Authentication



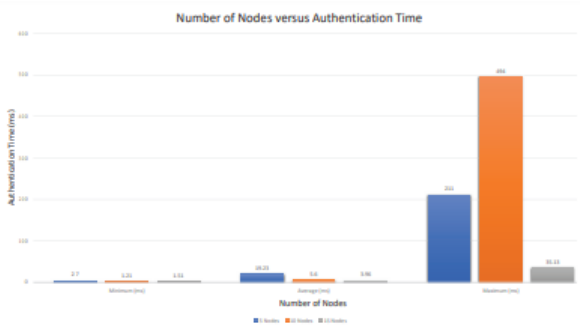

(b) for Block Reduction

**Figure 7:** Time Consumed by PoAh for 15 Nodes

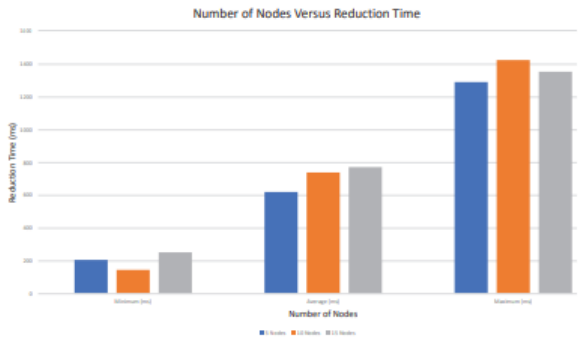
## Experimental Results

The proposed framework is demonstrated and analyzed. The proof of authentication was implemented using python. The peer-to-peer network was created among 15 nodes.

Each node is sending 1024 bytes to the block in each second. The nodes in the private network have the same kind of authority over the entire network. The SQL is used for storing the headers of the block and the collection of data from the nodes. It is also used for the creation of securing unique identification which has the UIDs in the network which is stored in all the nodes. The experiment was conducted for the 5th, 1oth, and the 15th node. The result of the experiments is tabulated in 2, 3. The time taken for authentication of the ledger is illustrated in fig 7. The fig 7 b illustrates the reduction in time for the 15th node.



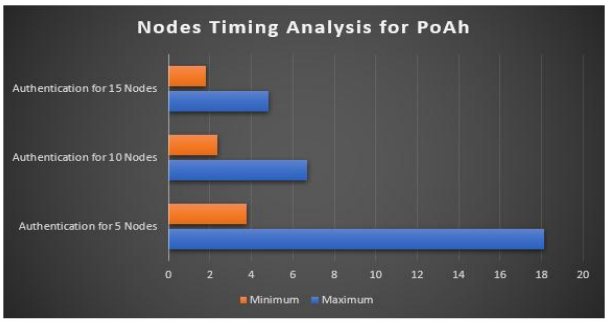

(a) Block Authentication Time.



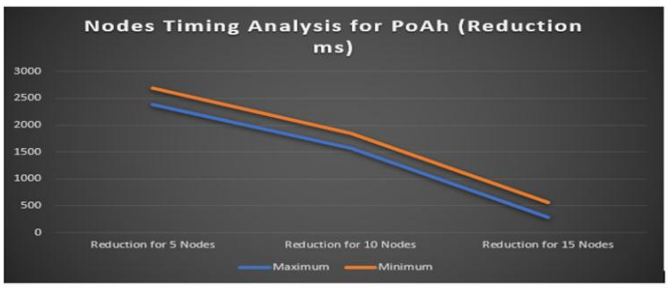

(b) Block Reduction Time.

**Figure 8:** Scalability study in terms of Number of Nodes.

When comparing the 3 scenarios the time taken for authentication is reduced with the increase in the number of participants. The flow in the blocks which shows the network speed and its stability with the increased participants in the multi-chain protocol. In order to reduce the level, the blocks must get authentication which must be equal to that of the number of participants avoiding the source. Fig 8 illustrates the process of authentication and the time reduction over the number of nodes. The proof of authentication neglects the involvement of miner and full ledger.




(a) Based on Authentication




(b) Based on Reduction

**Figure 9** Nodes Timing analysis for PoAh

## Conclusions and Future Directions

This research mainly focused on the integration of the internet of things and the usage of blockchains with IoTs. For attaining effective integration the consensus algorithm must be suitable for the internet of things. The conventional consensus algorithms the proof-of-work is not suitable for IoT because of using more power and time. The multi-chain model is used as the replacement of the conventional blockchain model which helps in eliminating the full ledger for authentication of blocks. In this research, a new protocol was developed which addresses the latency problem of the conventional blockchain. The concept of the post-blockchain ledger as a multi-chain is in progress. Further planning with this model is using this concept with the CPS. The validation of real data in CPS is also planned.

## References

[1] T. M. Fernandez-Caram ´ es and P. Fraga-Lamas, “A review on the use of ´ blockchain for the internet of things,” IEEE Access, vol. 6, pp. 32 979– 33 001, 2018.

[2] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, “When internet of things meets blockchain: Challenges in distributed consensus,” IEEE Network, pp. 1–7, 2019.

[3] A. Rovira-Sugranes and A. Razi, “Optimizing the Age of Information for Blockchain Technology With Applications to IoT Sensors,” IEEE Communications Letters, vol. 24, no. 1, pp. 183–187, Jan 2020.

[4] S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything you wanted to know about smart cities: The internet of things is the backbone,” IEEE Consumer Electronics Magazine, vol. 5, no. 3, pp. 60–70, July 2016.

[5] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, “Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city,” IEEE Access, vol. 7, pp. 18 611–18 621, 2019.

[6] D.Puthal, N.Malik, S.P.Mohanty, E.Kougianos, and G.Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems,” IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6–14, July 2018.

[7] A. Ahi and A. V. Singh, “Role of Distributed Ledger Technology (DLT) to Enhance Resiliency in Internet of Things (IoT) Ecosystem,” in Proc. Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 782–786.

[8] S. Popov, “The Tangle,” Jinn Labs, 2016, version 0.6.

[9] Y. Jiang, C. Wang, Y. Huang, S. Long, and Y. Huo, “A cross-chain solution to integration of iot tangle for data access management,” in Proc. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), July 2018, pp. 1035–1041.

[10] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, “Secured by Blockchain: Safeguarding Internet of Things Devices,” IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 28–34, May 2019.

[11] T. F. Chiang, S. Y. Chen, and C. F. Lai, “A Tangle-Based High Performance Architecture for Large Scale IoT Solutions,” in Proc. 1st International Cognitive Cities Conference (IC3), 2018, pp. 12–15.

[12] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE),” IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 8–16, March 2020.

[13] R. Alexander, IOTA - Introduction to the Tangle Technology: Everything You Need to Know about the Revolutionary Blockchain Alternative. Independently published, 2018.

[14] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Cryptography Mailing list, 2009.

[15] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proofof-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," in Proc. IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1–5.

[16] N. Zivi, E. Kadu ˇ siˇ c, and K. Kadu ´ siˇ c, "Directed Acyclic Graph as Tangle: ´ an IoT Alternative to Blockchains," in Proc. 27th Telecommunications Forum (TELFOR), 2019, pp. 1–3.

[17] L. Baird, "The SwirldsHashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," Swirlds, May 2016.

[18] L. Baird, M. Harmon, and P. Madsen, "Hedera: A Public HashgraphNetwork& Governing Council," Hedera, Aug 2019, last Accssed on 21 Apr 2020. [Online]. Available: https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf

[19] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 2nd ed. MIT Press and McGraw-Hill, 2001, no. pp. 552–557.

[20] "NEM Blockchain Ecosystem," NEM, Feb 2018.

[21] K. Au, "Tracing Back Stolen Cryptocurrency (XEM) From Japan's Coincheck," Forbes.

[22] Parity: Fast, light, robust Ethereum implementation, Parity Technologies, 2017-12-12, retrieved 2017-12-12.

[23] Gavin, Wood (November 2015). "PoA Private Chains". Github., https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper.

[24] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2343– 2355, March 2020.

[25] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and solutions, 2016, arXiv preprint arXiv:1608.05187.

[26] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[27] O. Novo, Blockchain meets IoT: an architecture for scalable access management in ioT, IEEE Internet of Things J. 5 (2) (2018) 1184–1195.

[28] L. Mearian. Ethereum explores a fix for blockchain's performance problem. https://www.computerworld.com/article/3245928/emerging-technology/ ethereum-explores-a-fix-for-Blockchains-performance-problem.html. January 5, 2018.

[29] Z. Chen. How should we regulate blockchain? It depends on which country you ask. http://fortune.com/2018/06/25/Blockchain-cryptocurrencytechnology-regulation-bitcoin-ethereum/. June 25, 2018.

[30] M. Cabrera. Cryptocurrency and blockchain investor gives suggestions to global governments regulating new technologies. https://www.cio.com/article/3263324/Blockchain/cryptocurrency-and-Blockchain-investor-gives-suggestions-to-global-governments-regulating-new-techn.html. March 27, 2018.

[31] A. Kaplan. How alibaba is championing the application of blockchain technology in china and beyond – Tue Jul 10. https://smartereum.com/7630/ how-alibaba-is-championing-the-application-of-Blockchain-technology-in-China-and-beyond-tue-jul-10/ July 11, 2018.

[32] Z. Huang. China's crackdown on crypto hasn't stopped its tech giants from flirting with blockchain. https://qz.com/1256536/baidu-tencentalibaba-bat-are-flirting-with-Blockchain-despite-chinas-ban-on-cryptocurrency/ April 19, 2018.

[33] W. Suberg. Internet giant baidu unveils energy-efficient 'Super Chain' Blockchain Protocol.

https://cointelegraph.com/news/internet-giantbaidu-unveils-energy-efficient-super-chain-Blockchain-protocol. Jun 3, 2018.

[34] A. Levy. Why mark zuckerberg just put some of his best execs on blockchain. https://www.cnbc.com/2018/05/09/zuckerberg-invests-inBlockchain-to-keep-facebook-relevant.html. March 22, 2018.

[35] O. Kharif; M. Bergen. Google is working on its own blockchain-related technology. https://www.bloomberg.com/news/articles/2018-03-21/ google-is-said-to-work-on-its-own-Blockchain-related-technology. May 9, 2018.

[36] Q. Chen. In the world of cryptocurrency buzz, blockchain is the real winner. https://www.cnbc.com/2018/01/10/in-the-world-of-cryptocurrency-buzzBlockchain-is-the-real-winner.html. January 12, 2018.

[37] Markets and Markets, Statista estimates, Market for Blockchain Technology Worldwide (2018). Accessed: Apr. 10https://www.statista.com/statistics/647231/worldwide-blockchaintechnology-market-size.

[38] J. Hu. What are the timetables for the blockchain national standards? http://baijiahao.baidu.com/s?id=1600160721567265567&wfr=spider&for=pc. May 11, 2018.

[39] Y. Yuan, F.-Y. Wang, Blockchain: the state of the art and future trends, ActaAutomaticaSinica 42 (4) (2016) 481494.

[40] Daniel Minoli, Benedict Occhiogrosso, Blockchain mechanisms for IoT security, Internet of Things 1 (2018) 1–13.

[41] L. Atzori, A. Iera, G. Morabito, Understanding the internet of Things: definition, potentials, and societal role of a fast evolving paradigm, Ad Hoc Netw 56 (2017) 122–140. [18] D. Underwood, Industry 4.0, key design principles (April 24, 2017). https://kingstar.com/industry-4-0-key-design-principles/.

## Author profile

Dr. K. Sai Manoj, CEO of Amrita Sai Institute of Science and Technology / Innogeecks Technologies has extensive experience in financial services, IT Services and education domain. He is doing active research pointing to the industry related problems on Cloud Computing, Cloud Security, Cyber security, Ethical Hacking, Blockchain (DLT) and Artificial Intelligence. He obtained PhD Degree in Cloud Computing, M.Tech, in Information technology from IIIT Bangalore. He published research articles in various scientific journals and also in various UGC approved journals with Thomson Reuter id. Also, he presented innovative articles at high Standard IEEE and Springer Based Conferences. He has various professional certifications like Microsoft Certified Technology Specialist (MCTS), CEHv9, ECSA, CHFI, Chartered Engineer (C.Eng.,g from IEI, Paul Harris Fellow recognition by Rotary International and Outstanding Industry and Academic Contributor award from ASSOCHAM . He is currently doing post-doctoral work in Cloud Computing and Cyber Security.