McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems

Ahmad J. Alkhodair*, Saraju P. Mohanty*, Elias Kougianos†, and Deepak Puthal‡
* Department of Computer Science and Engineering, University of North Texas, USA
† Department of Electrical Engineering, University of North Texas, USA
‡ School of Computing, Newcastle University, United Kingdom
Email: AhmadAlkhodair@my.unt.edu, saraju.mohanty@unt.edu, elias.kougianos@unt.edu, Deepak.Puthal@newcastle.ac.uk

***Abstract*—Internet of Things (IoT) research is in full swing to integrate recent technologies such as the blockchain to enhance system security. However, the blockchain faces many limitations, such as resource demands, energy requirements, scalability, and high latency. This article presents a novel post-blockchain structure that integrates a multi-blockchain in one ledger using a directed acyclic graph (DAG) structure called a multi-chain. The multi-chain structure resolves the issues of scalability and storage and is a candidate to replace the traditional blockchain in IoT applications. This article also introduces a new consensus algorithm called "Multi-Chain Proof of Rapid Authentication" (McPoRA) to improve latency, which is a crucial factor in IoT resource constrained devices. McPoRA is approx. 4000× faster than proof-of-work (PoW) and 55× faster than Proof-of-Authentication (PoAh).**

***Index terms*—** Blockchain, Tangle, HashGraph, Cyber-Physical Systems, Unique Identification, Dynamic Blocks List, Secure Identification List, Block Filtration Algorithm.

I. Introduction

The Internet of Things (IoT) is the interaction and exchange of data between very large numbers of various nodes such as consumer electronics devices, hardware systems, sensors, and buildings. All the devices in the IoT environment are connected through the Internet [1], [2]. The IoT facilitates the exchange of data between the nodes [3], [4]. Privacy and security are challenges for the IoT due to the vast growth of node density [5].

The blockchain is a distributed ledger used to store transactions in a secure, transparent, decentralized, irreversible, and immutable database. Using a technology such as the blockchain in Cyber-Physical Systems (CPS) will improve their efficiency and robustness. However the blockchain faces challenges [6], one of which is scalability [7].

Tangle [8], a new distributed ledger technology has been proposed to replace the blockchain as a faster, and cheaper structure to deal with in an IoT environment. Tangle is a distributed ledger built for micro-payment environments such as the IoT. However, the technology uses the most common and power consuming protocol proposed since the launch of the first cryptocurrency, Proof of Work (PoW). Tangle could be resolving some of the issues of the traditional blockchain, but since it uses PoW, the technology will not be compatible with IoT devices with limited capabilities for data collection and analysis [9].

In this paper, a new protocol is proposed to authenticate data of IoT devices. The protocol uses a Secure Unique Identification List (SUIL) as a file stored in every single node and used to authenticate the previous two side blocks of a directed acyclic graph (DAG) in topological order as prepaid incentive [10]. The approach used speeds up the process of authenticating the data joining the database by just authenticating the source with the predefined ID in the SUIL [7]. The proposed protocol resolves scalability issues such as latency, processing power, and storage in the traditional blockchain [11]. There are several related works developing blockchain consensus for different applications. The major and most widely adopted consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), Proof of Capacity (PoC), Proof of Activity, Proof of Importance, Proof of Block and Trade (PoBT), and Proof of Vote (PoV). However, few consensus algorithms have been developed specific to the IoT for resource constrained devices. The most common are Proof of Authentication (PoAh) and Proof of PUF-Enabled Authentication (PUFChain) [12].

The rest of the paper is organized as follows: Section II summarizes the novel contributions of this paper. Section III presents a comparative perspective of post-blockchain compared to traditional blockchain. Section IV develops the proposed consensus algorithm. Section V provides experimental results and Section VI concludes the paper and presents directions for future research.

II. Novel Contributions of The Current Paper

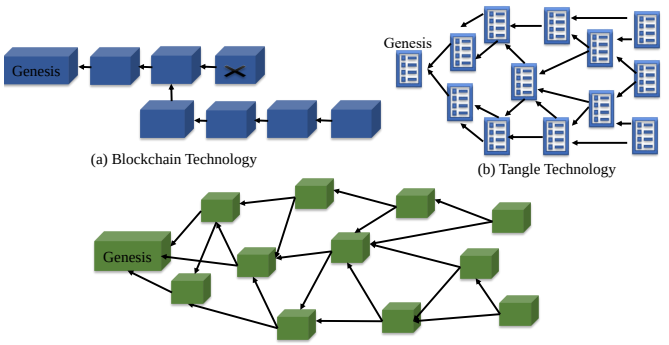
Blockchain technology has been explored for many possible applications but it has several issues such as scalability, energy requirements, resource requirements, and higher latency which are bottlenecks for its application in resource constrained applications [12]. Tangle is considered a successor of blockchain technology [13]. In the current paper we intend to advance

the state-of-art of Tangle technology to build scalable and fast post-blockchain technology as a multi-chain paradigm.

The **novel contributions of this paper** are as follows: (1) To the best of the authors' knowledge, this is the first protocol using a Secure Unique Identification List (SUIL) for authentication that is part of all nodes. (2) The proposed protocol uses Dynamic Block List (DBL), which is a multi-chain as the data structure to store and speed up the process of authentication. (3) In this protocol there are no miners, all the nodes could broadcast and authenticate transactions which indicates fairness in authority distribution. (4) The DBL is distributed over all the nodes and will be reduced to a minimal version.

III. Blockchain Technology Versus Tangle Technology Versus Proposed Multi-Chain

We present comparative perspectives of blockchain technology versus Tangle versus the proposed multi-chain in this section. This perspective is illustrated in Fig. 1 and summarized in Table I.



(a) Blockchain Technology (b) Tangle Technology

(c) Proposed Post-Blockchain Multichain as a Directed Acyclic Graph (DAG) Structure

Fig. 1: Ledger Structure for: (a) Blockchain Technology, (b) Tangle Technology, and (c) the Proposed Post-Blockchain Technology.

A. Blockchain Technology and Limitations

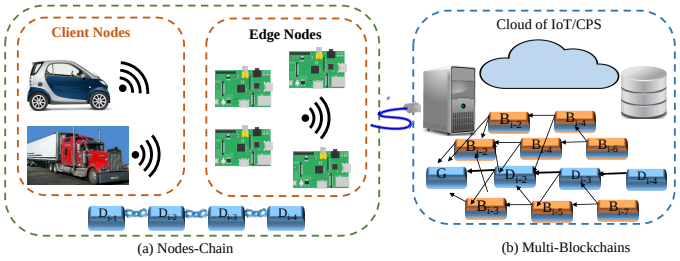
Blockchain technology deploys Proof of Work as a heavy-duty consensus algorithm to validate a group of transactions [6], [14]. Blockchain technology is a distributed database that uses a linked list graph for a group of digital assets and each group is represented as a block. The linked lists of transactions are organized in a public ledger published by regular users (traders) and validated by miners. The order of the new transactions joining the ledger should be preserved. A block should be placed in the public ledger under two conditions: honest publisher and consistent order. The operations suffer from scalability problems in the current applications such as the first cryptocurrency, Bitcoin. Storage, process, power and time consumption have direct relationship with the ledger expansion. Thus, the fees and operational costs increase significantly. These limitations are preventing many companies from placing the blockchain technology in their business solutions. PoW has been designed to be placed as the technology behind a cryptocurrency and will not be suitable for CPS/IoT due to the requirements of high resources.

B. Tangle Technology

Tangle is a recent technology introduced to reduce the high cost of operation of the blockchain [8], [16]. It uses a better scalable structure DAG and deals with independent transactions that are referenced by two previous transactions by performing Proof of Work with no mining process or miners. Multiple factors are involved in this process such as a selection algorithm for location selection, and longest and shortest path for ledger minimal version. Tangle has attracted attention due to the unique mathematical structure of the DAG. It could also remove the miner role toward a full decentralization and lower cost. However, the entire process requires resources to be performed as proposed.

C. Proposed Novel Post-Blockchain Multi-Chain Technology

Multichain technology is the proposed structure in this paper as shown in Fig. 1. This structure could resolve many issues in the traditional Blockchain such as forks, miners, scalability, and latency. It combines the traditional blockchain with DAG using a secure unique identification file in a private framework to authenticate blocks instead of power and process consuming protocols that are used in the PoW based Blockchain and Tangle. Using Multi-Chain will resolve the issue of high fees and will eliminate the role of miners thus avoiding the 51% attack in PoW, and selection priority PoS as shown in Table I.



(a) Nodes-Chain (b) Multi-Blockchains

Fig. 2: Illustration of Post-Blockchain Multi-Chain Technology in a Transportation CPS Infrastructure.

The blocks are strongly connected by referencing two previous blocks instead of one in the traditional structure. The blocks are consistent and will grow even with the existence of a malicious blocks as shown in Fig. 5. The malicious unauthenticated block will be orphaned and discarded once all the participants de-authenticate it. Therefore, the orphaned blocks will not affect the grow of the ledger. The topological order in Multi-Chain avoids any time conflicts between blocks because time consensus is applied for agreeing over a sequence of side blocks. The side blocks will prioritize based on the time consensus which will always use the median time of the chosen blocks. Prior to broadcasting, blocks are located in the ledger. Once the nodes receive the block, they will recognize the location of the new block which incurs very low traffic as detailed in Fig. 1. The nodes unable to broadcast

TABLE I: 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]	**McPoRA based Multi-Chain (current paper)**
Linked Lists	• Linked list of blocks • Each block contains multiple transactions	• One linked list of blocks • Each block contains multiple transactions	• DAG linked list • One transaction	• DAG linked List • Container of transaction hash	• DAG linked List • Each block contains multiple transactions
Validation	Mining	Authentication	Mining	Virtual voting (witness)	Authentication (No miner)
Type of Validation	Miners	Trusted Nodes	Transactions	Containers	All Nodes
Ledger Requirement	Full ledger required	Full ledger required	Portion based on longest and shortest paths.	Full ledger required	Portion based on authenticators' number
Cryptography	Digital Signatures	Digital Signatures	Quantum key signature	Digital Signatures	Digital Signatures
Hash Function	SHA 256	SHA 256	KECCAK-384	SHA 384	SCRYPT
Consensus	Proof of Work	Cryptographic Authentication	Proof of Work	Asynchronous Byzantine Fault Tolerance (ABFT)	Predefined unique identifications (UID)
Numeric System	Binary	Binary	Trinity	Binary	Binary
Involved Algorithms	HashCash	No	• Selection Algorithm • HashCash	No	Block Filtration Process (BFP)
Decentralization	Partially	Partially	Fully	Fully	Fully
Appending Requirements	Longest chain	One chain	Selection Algorithm	Full Randomness	Filtration Process
Energy Requirements	High	Low	High	Medium	Low
Node Requirements	High Resources Node	Limited Resources Node	High Resources Node	High Resources Node	Limited Resources Node
Design Purpose	Cryptocurrency	IoT Applications	IoT Cryptocurrency	Cryptocurrency	IoT/CPS Applications

before ensuring the authenticity of the location are handled as discussed in Section IV-D. The block type will be recognized for the appending process by identifying the authenticator. The whole structure will represent a fully connected graph from the single transaction and single device block to the whole ledger showing a stronger, simpler, and organized graph that includes devices and transactions to ensure privacy, integrity, confidentiality, availability, and security, as shown in Fig. 2. The Multi-Chain has the feature of providing certain paths for certain type of blocks by identifying the source UID. Scalability is resolved in this structure by using minimization techniques such as short distance minimization and reduction process. Reduction process influence will be over the whole ledger. Shortest path minimization influence will be over the nodes' local ledger, as shown in Fig. 5.

Post-Blockchain Multi-chain Technology is designed and built for CPS/IoT applications and suits the limited resources' ends. It could also be used for multiple purposes. Multi-chain has the feature of providing certain paths for certain types of block by identifying the SUIL which ensures that only authentic nodes could participate in the network by reaching a consensus over the existence of UID. Using Multi-chain associated with PoRa makes it easy to detect any malicious behavior inside the network, as demonstrated in Fig. 5.

The uniqueness of this structure comes from the flexibility this network offers to the users, such as flexibility in operating in one sub-blockchain, minimization over the entire ledger or the nodes' local ledger, flexibility in ensuring the integrity of the nodes within the same network and finally operating with different types of blocks. Post-Blockchain Multi-chain Technology is presented in Fig. 2. NodeChain is an independent blockchain and it represents the registration steps of the devices. Each block is the virtual existence of each device in the network. By the completion of the registration step, there exists a linked list of virtual devices. This linked list is the genesis blockchain, and the rest of the joining blocks generated by the original devices will be built over this genesis blockchain to form the DAG. The expansion of the DAG and the number of chains won't be defined and will be based on the growth of the DAG. For adding devices during the growth of the DAG, the type of the block will be recognized and the block (virtual device) and one of its arcs will be linked to the genesis blockchain.

IV. Proposed Novel Post-Blockchain - Multi-Chain

The proposed consensus algorithm comprises of four essential parts: Dynamic Blocks List (DBL), Secure Unique Identification List (SUIL), Transaction, and Block content.

A. Dynamic Blocks List (DBL)

Dynamic Blocks List (DBL) is the structure used to store the data in a topological order. The list has two stages: first, the stage of the unauthenticated blocks, and second, the stage of the authenticated blocks. The vertices are organized in order and that indicates fairness in the order of blocks [19]. Reachability: there is always a way from one vertex to another within the same graph which indicates that all the blocks are reached by the genesis block (strongly connected). The path from/to the genesis block is used to identify the volume of the storage for each node. Rapid-Authentication: in DBL, there are two arcs attached to each block, which allows authenticating two blocks using only one block. This process improves speed.

Finally, the more blocks are added to the multi-chain, the more blocks will be authenticated, which will speed up the process of authentication.

B. Secure Unique Identification List (SUIL)

SUIL is the file used to store the unique identifications (UIDs) associated with the nodes in the private multi-chain. Fig. 3 illustrates the assumed SUIL that includes the nodes' UIDs. The UID is also part of each transaction joining the DBL. The purpose of having this unique UID is that the nodes will be able to authenticate blocks by just matching the source UID of the block with the predefined one that exists in the SUIL.

C. Block content

Each block content is presented in Fig. 4 along with details of the Merkle tree. The block comprises of four different parts: the block header, source UID, the content or data, and the timestamp. Moreover, the block header of each block consists of the block header 1 of a previous block and the block header 2 of a different previous block. In addition, the block header contains the Merkle tree and timestamp.

D. Proposed Algorithm and It Operations

Each node in this protocol is assumed to be predefined and granted a UID from the network. Once a node collects the data and creates the block, it will filter the DBL to choose a location for the new generated block by specifying two side blocks and authenticate them. Once the block is part of the unauthenticated stage of DBL, the block might be chosen by other nodes to authenticate and append their own blocks.

Algorithm 1 describes the process of collecting the data from a certain node, authenticating previous blocks, and finally appending the new generated block to the unauthenticated stage of DBL. If another node generated a new block, it will follow the same process. Fig. 5 illustrates the proposed algorithm.

Algorithm 1 The Steps of the Proposed McPoRA.

Input : *Data D_i collected from node N_i*
Output: *Authenticated Blocks b_i or Discarded Blocks d_i*
Terms : *bc_n is blocks' number of authentication, n is the number of nodes*

```
/* Node collects data                                   */
```
$N_i \hookrightarrow b_i$ Node N_i creates block b_i
Node runs Blocks Filtration Algorithm (BFA)
if $bc_i \equiv 0$ *in DBL,* **then**
  Pick b_{i_1} and b_{i_2} with $bc_i = 0$,
else
  Pick b_{i_1} and b_{i_2} with $bc_i = 0$ and $bc_i = 1$,
end
Pick b_{i_1} and b_{i_2} randomly
Node identifies two previous blocks as a location (l_i) $l_i \hookrightarrow b_i$
```
/* Node checks the authenticity of the
   previous two blocks by comparing the
   predefined UID stored in the SUIL with the
   UID associated with the blocks                       */
```
if *UID in* $\overline{b_{i_2}}$ *and* $\overline{b_{i_1}} \neq$ *UIDs in SUIL* **then**
  Discard
else
  Authenticate
end
```
/* Node broadcasts the new block to the
   network                                              */
```
N_i broadcasts block b_i `/* New block appended to DBL as a side block */`
$b_i \hookrightarrow DBL$
if bc_i *for each* b_i *in* $DBL \equiv n$ **then**
  Reduce
else
  Leave
end

V. Experimental Results

In this section the results of the proposed protocol McPoRA are demonstrated and analyzed. McPoRA has been implemented using Python. P2P connections have been created between 15 nodes. Each node is sending a block of 1024 bytes every few seconds. All the nodes within the private network share the same authority over the whole system. Postgres SQL is used in this implementation to store the block headers and the data collected from the nodes. It is also used to create the SUIL that contains the UIDs in the network and is stored in each node.

We present experiments for 5, 10, and 15 nodes in the network and the results are shown in Tables II, III, and IV. Fig. 6(a) shows the authentication time for the ledger and Fig. 6(b) presents the time reduction for the 15 node case.

Comparing the three scenarios, the authentication time decreases with the increase of participants and block flow which indicates that the network becomes fast and stable with more participants joining the multi-chain. However, the reduction time increases with the number of participants. For each block to reach the reduction level, the block must receive authentication equal to the number of participants excluding the source. In Fig. 7, authentication and reduction times are illustrated against the number of nodes. Moreover, for each scenario, the lowest, average and highest time are shown for comparison. Table V presents the results that are

TABLE II: Nodes Timing Analysis for McPoRA for 5 Nodes.

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	2.66	206.52
Maximum	211	1291.6
Average	19.23	621

TABLE III: Timing Analysis for McPoRA for 10 Nodes.

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.21	145.8
Maximum	494	1420
Average	5.6	740

TABLE IV: Timing Analysis for McPoRA for 15 Nodes.

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.51	252.6
Maximum	35.14	1354.6
Average	3.97	772.53

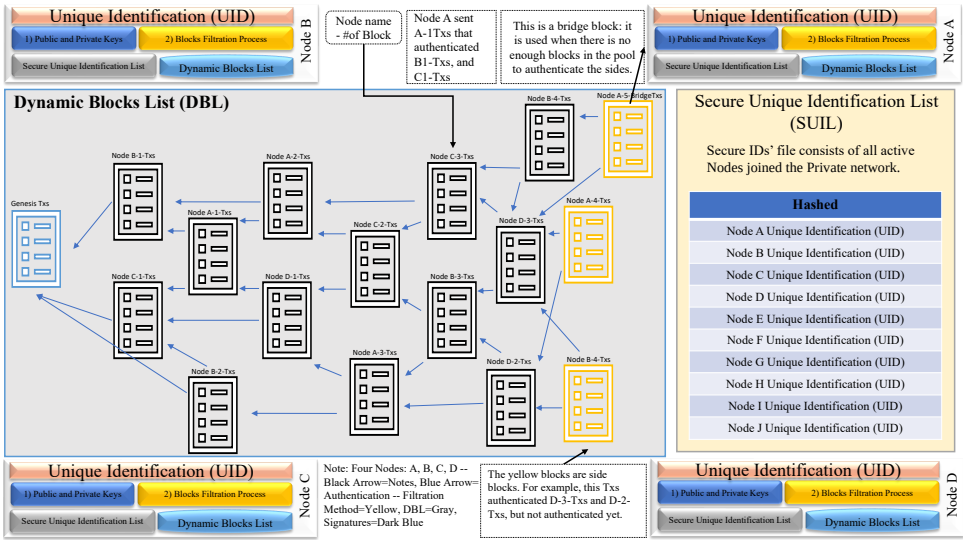


Fig. 3: A Detailed Depiction of The Proposed Consensus Algorithm Operation in the Multi-Chain Framework.

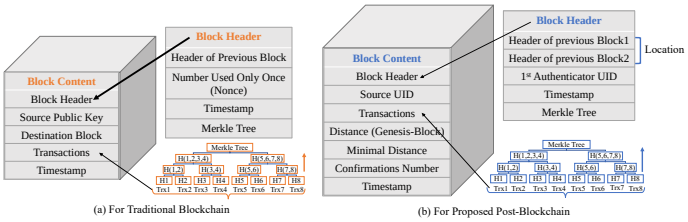


Fig. 4: The structure of block in the proposed post-blockchain.

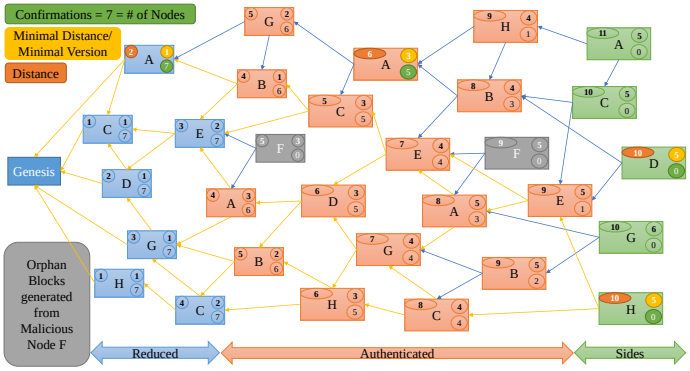
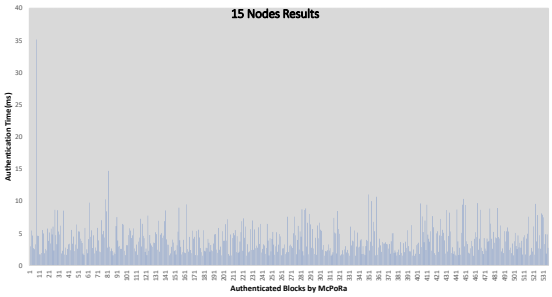
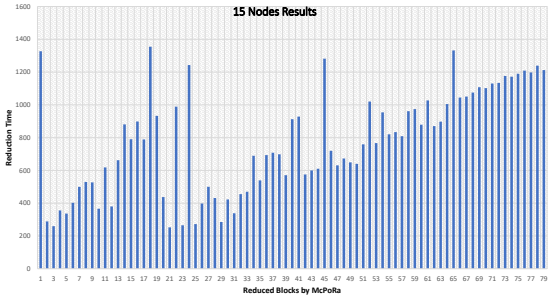


Fig. 5: Illustration of actions of the proposed McPoRA Algorithm in post-blockchain.



(a) for Block Authentication



(b) for Block Reduction

Fig. 6: Time Consumed by McPoRA for 15 Nodes.

obtained in McPoRA versus previous proposed protocols. It is seen that the proposed protocol preforms better in terms of latency. McPoRA also avoids miners and full ledger to address scalability.

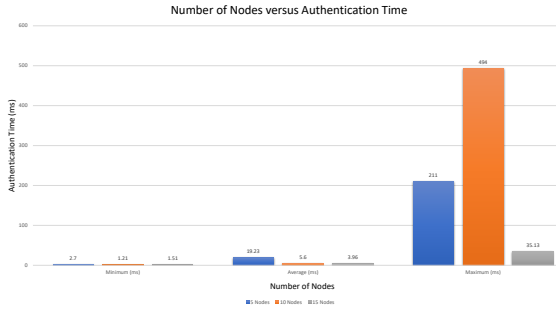
VI. Conclusions and Future Directions

The integration of IoT and the blockchain are active research areas. For effective integration, the consensus algorithms should be suitable for IoT resource-constrained nodes. Traditional consensus algorithms such as PoW are not suitable because of the high power and time requirements. In this article we presented the multi-chain to replace the traditional blockchain structure to avoid the need of having a full ledger to authenticate blocks. Also, we propose a new private consensus algorithm to authenticate blocks that resolves the latency issue in the traditional blockchain.

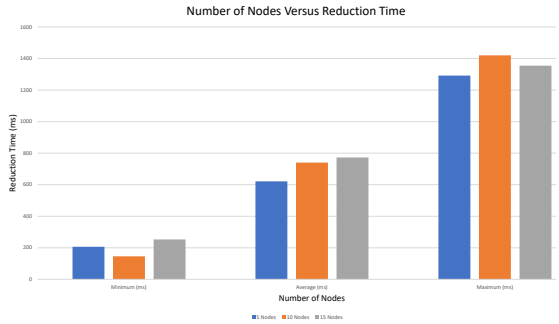
Our research on post-blockchain ledger as Multi-Chain is ongoing. We plan to present a method to use this Multi-Chain for security of resource constrained devices in CPS. We also plan to validate with further real-time data of CPS like smart transportation, and smart energy.

TABLE V: A Comparative Perspective of McPoRA with Previous Related Work.

Consensus Algorithms	Authentication Time (ms)	Ledger	Miners	Validation	Blockchain Type	Data Structure
Proof of Work (PoW) [14]	240,000	Full	Yes	HashCash (Huge calculations)	Public	Blockchain
Proof of Importance (PoI) [20], [21]	60,000	Full	Yes	Accounts Importance	Public	Blockchain
Proof of Authority (PoA) [22], [23]	5000	Full	Yes	PoS	Permissioned	Blockchain
Proof of Authentication (PoAh) [15]	3000	Full	Yes	Mac address verification	Private	Blockchain
Proof of PUF-Enabled Authentication (PoP) [12]	192.3	Full	Yes	Predefined PUF keys verification	Private	Blockchain
Proof of Block and Trade (PoBT) [24]	80-210	Full	Yes	Smart Contract and BFT	Private	Blockchain
McPoRA (Current Paper)	3.9-19.23 (Avg.)	Portion	No	UID verification	Private	Multi-chain



(a) Block Authentication Time.



(b) Block Reduction Time.

Fig. 7: Scalability study in terms of Number of Nodes.

REFERENCES

[1] T. M. Fernández-Caramés 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, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," in *Proc. IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–5.

[16] N. Živi, E. Kadušić, and K. Kadušić, "Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains," in *Proc. 27th Telecommunications Forum (TELFOR)*, 2019, pp. 1–3.

[17] L. Baird, "The Swirlds Hashgraph 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.