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

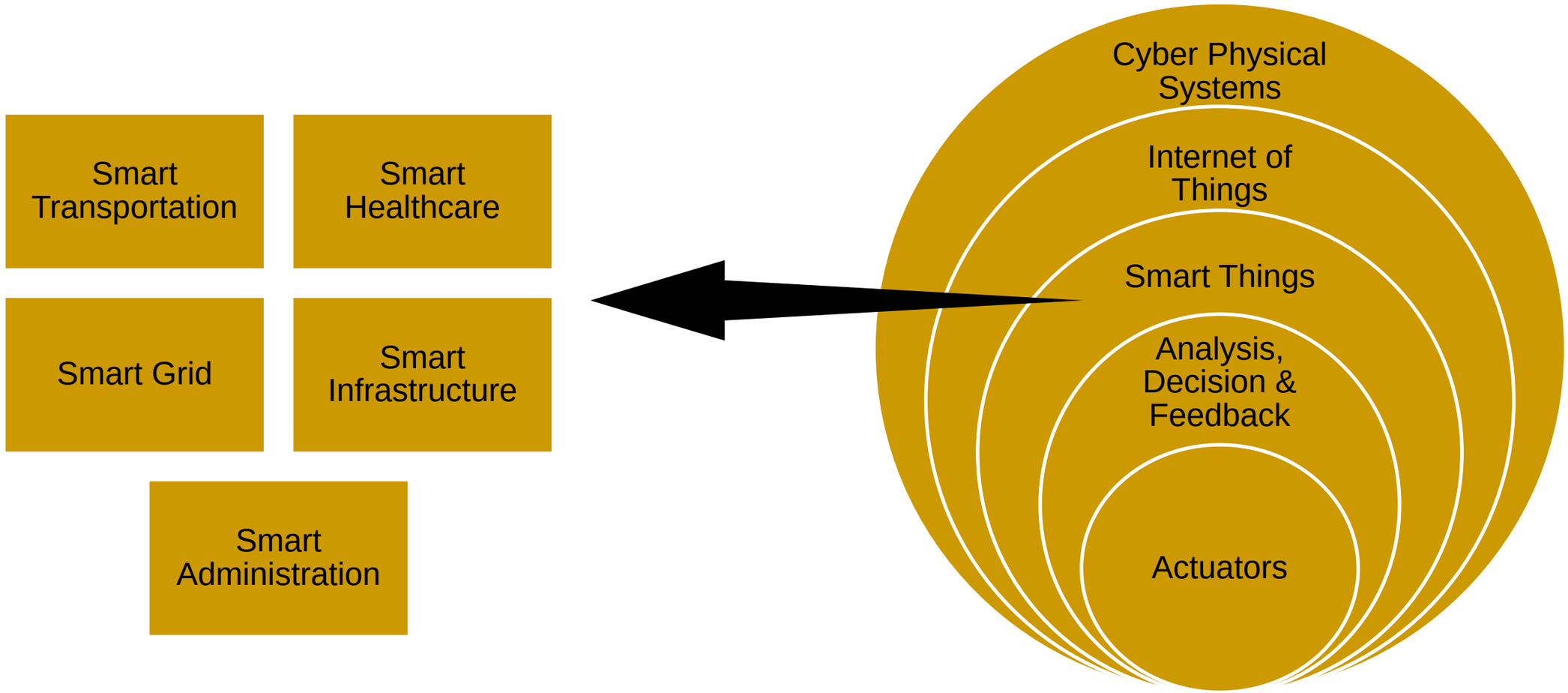
A. Alkhodair[1], S. P. Mohanty[1],
E. Kougianos[2], and D. Puthal[3]

University of North Texas, Denton, TX , USA.[1,2]
Newcastle University, United Kingdom[3]
Email: ahmadalkhodair@my.unt.edu[1], saraju.mohanty@unt.edu[1],
elias.kougianos@unt.edu[2], Deepak.Puthal@newcastle.ac.uk[3]

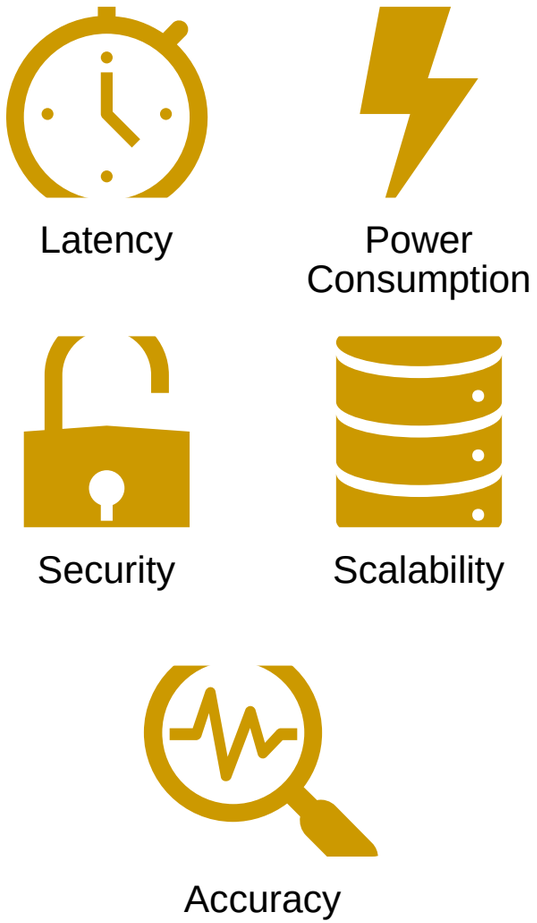
Outline

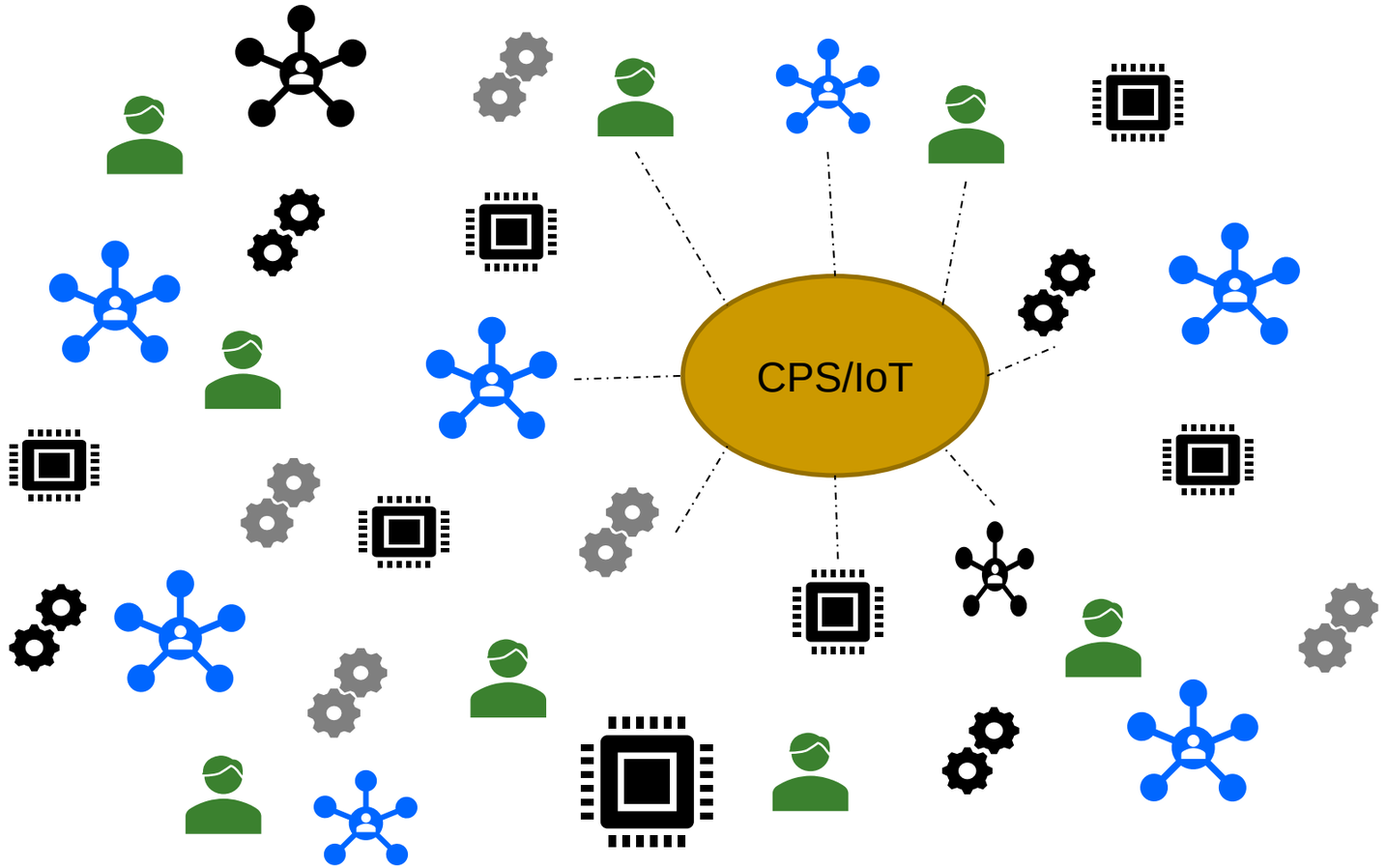
- Introduction
- Blockchain and Post-Blockchain Technologies
- The Proposed McPoRa
- Novel Contributions
- Multichain Technology Framework
- McPoRa Components
- McPoRa Algorithms and Operations
- Results
- McPoRa Versus Previous Related Work
- Conclusion
- References

Introduction

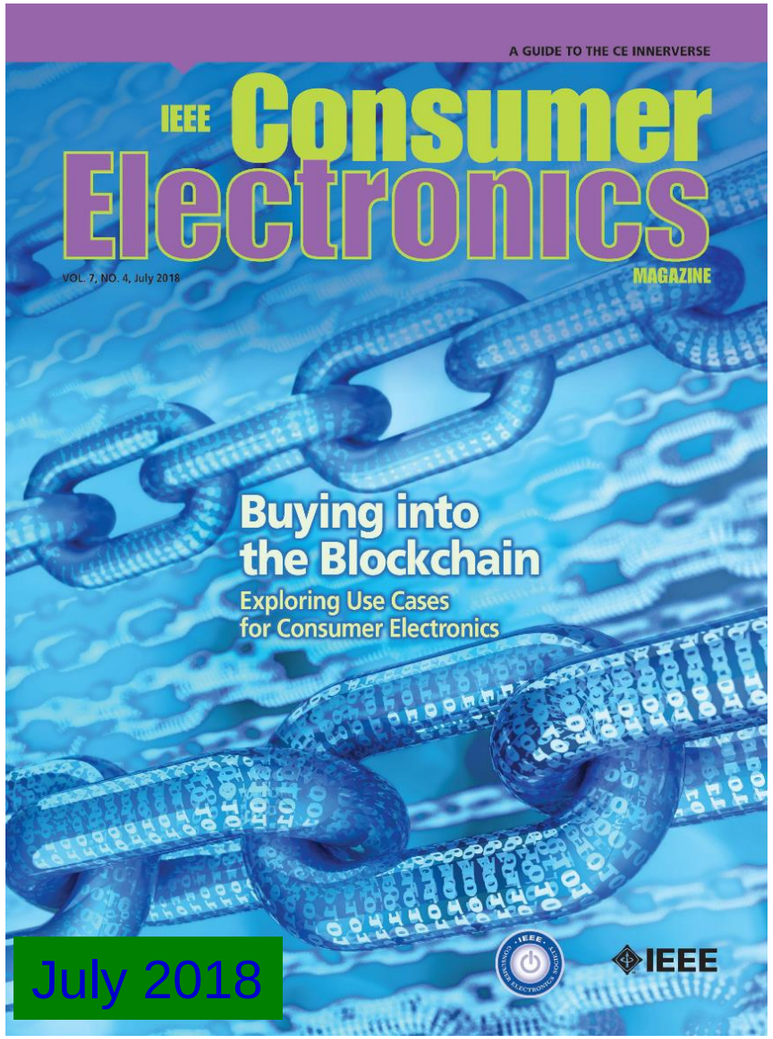


Introduction/Challenges

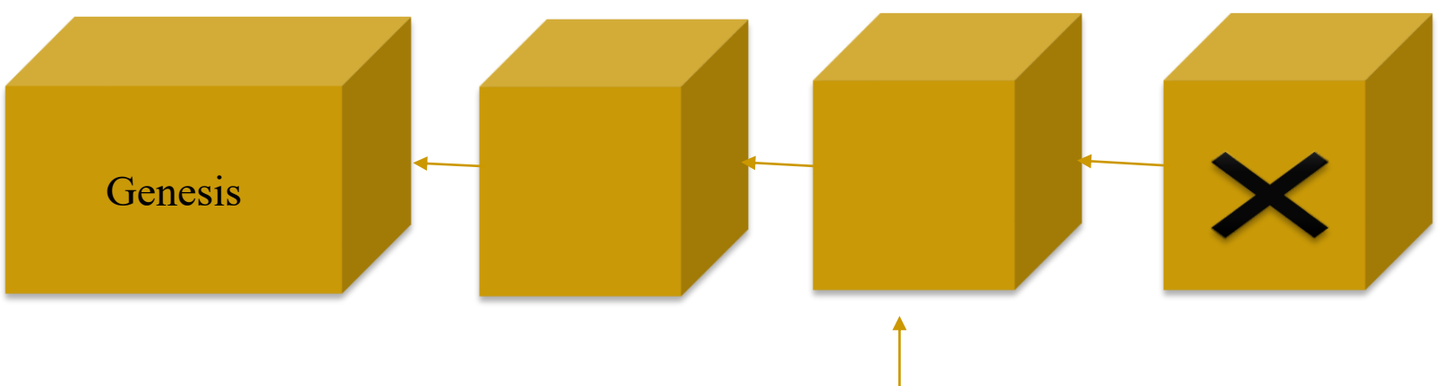


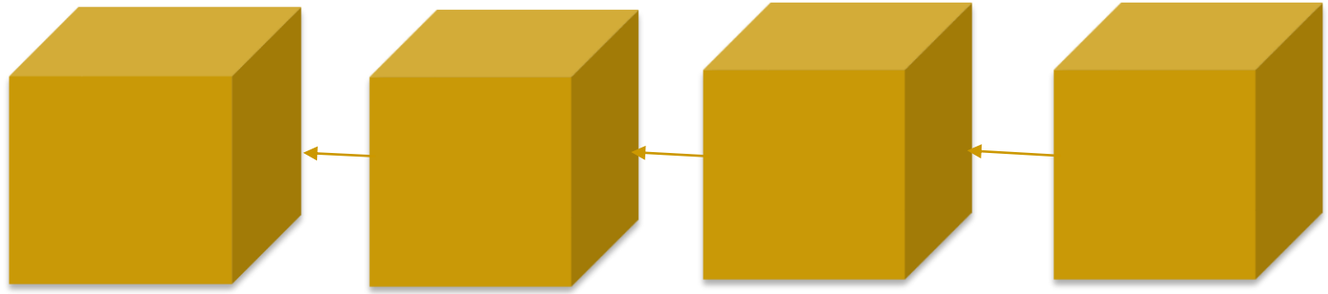


Blockchain Technology

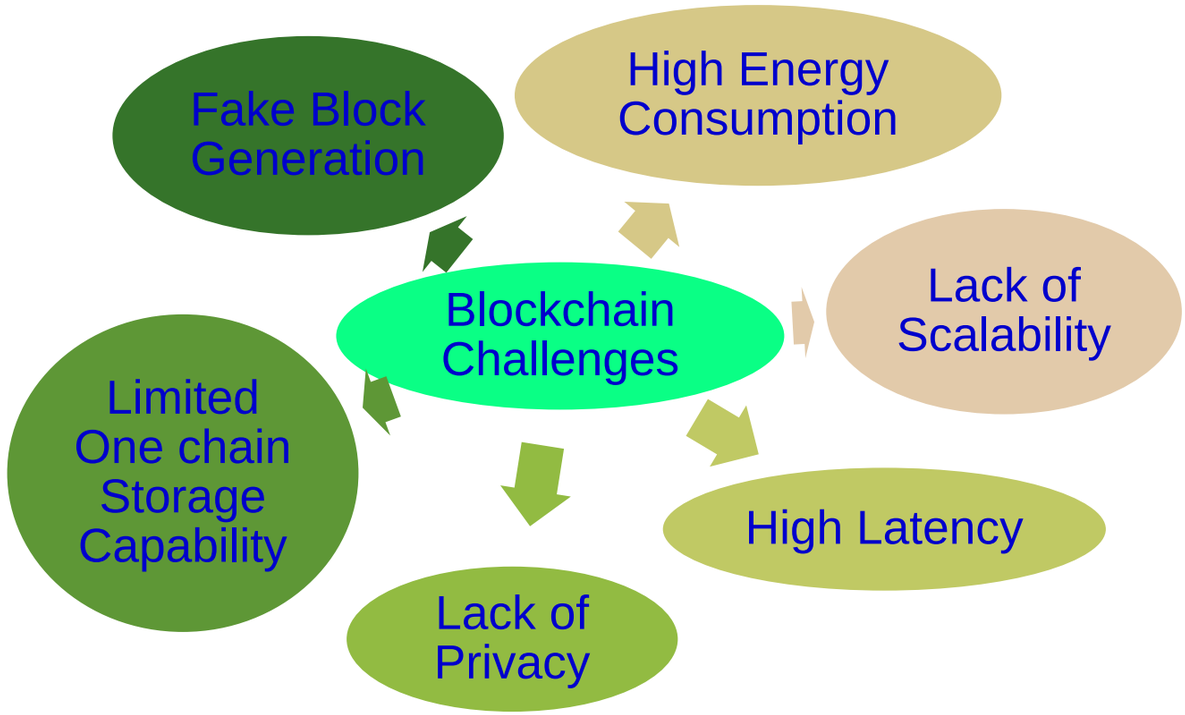


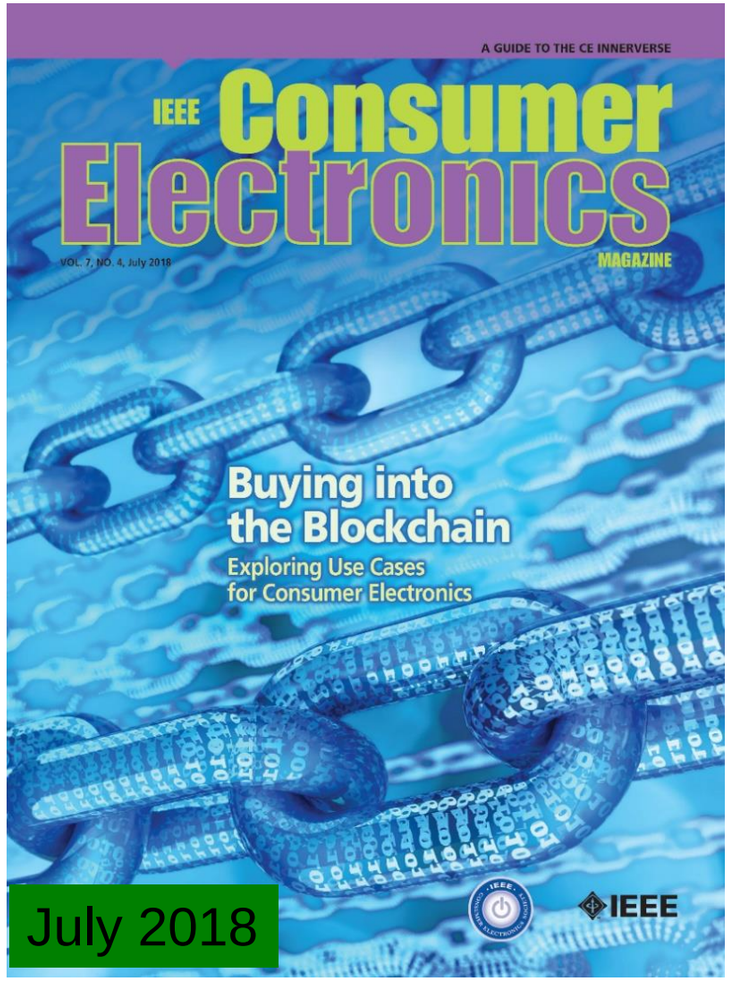
Introduction/Blockchain





The Blockchain faces Many Challenges

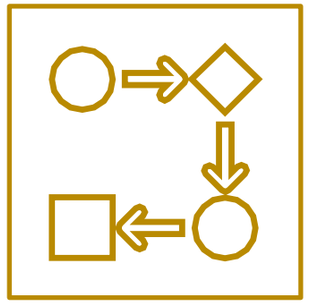




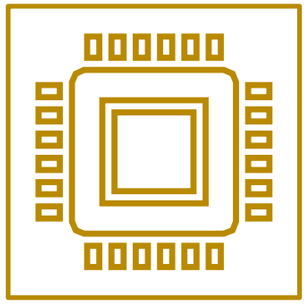
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain – Next Generation or Post-Blockchain

Hashgraph

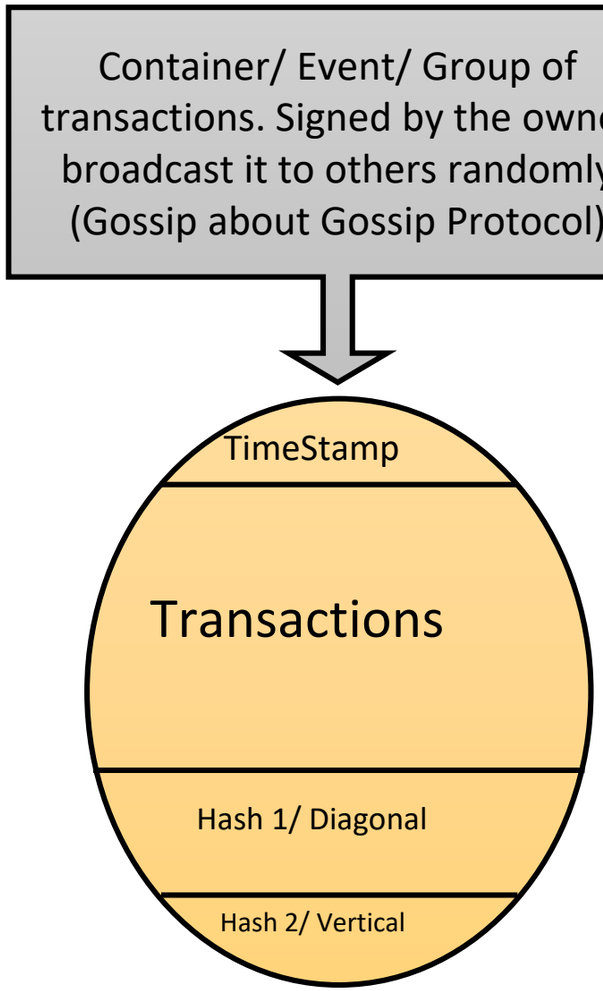


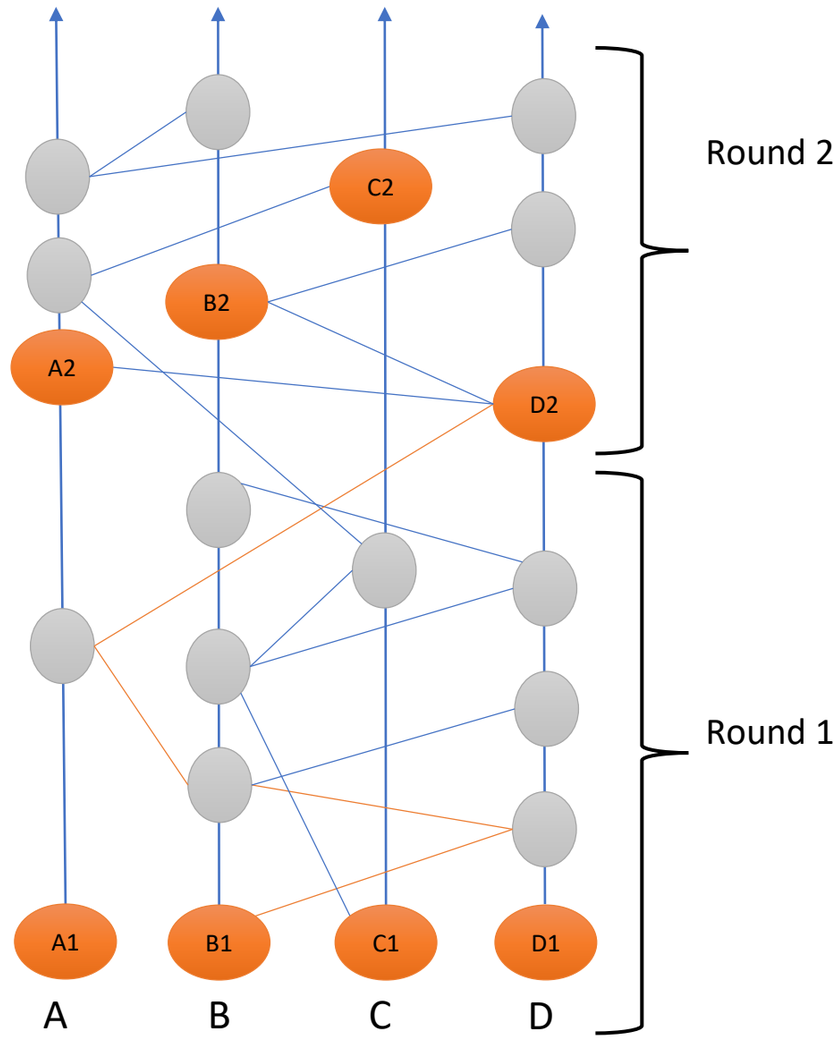
Tangle



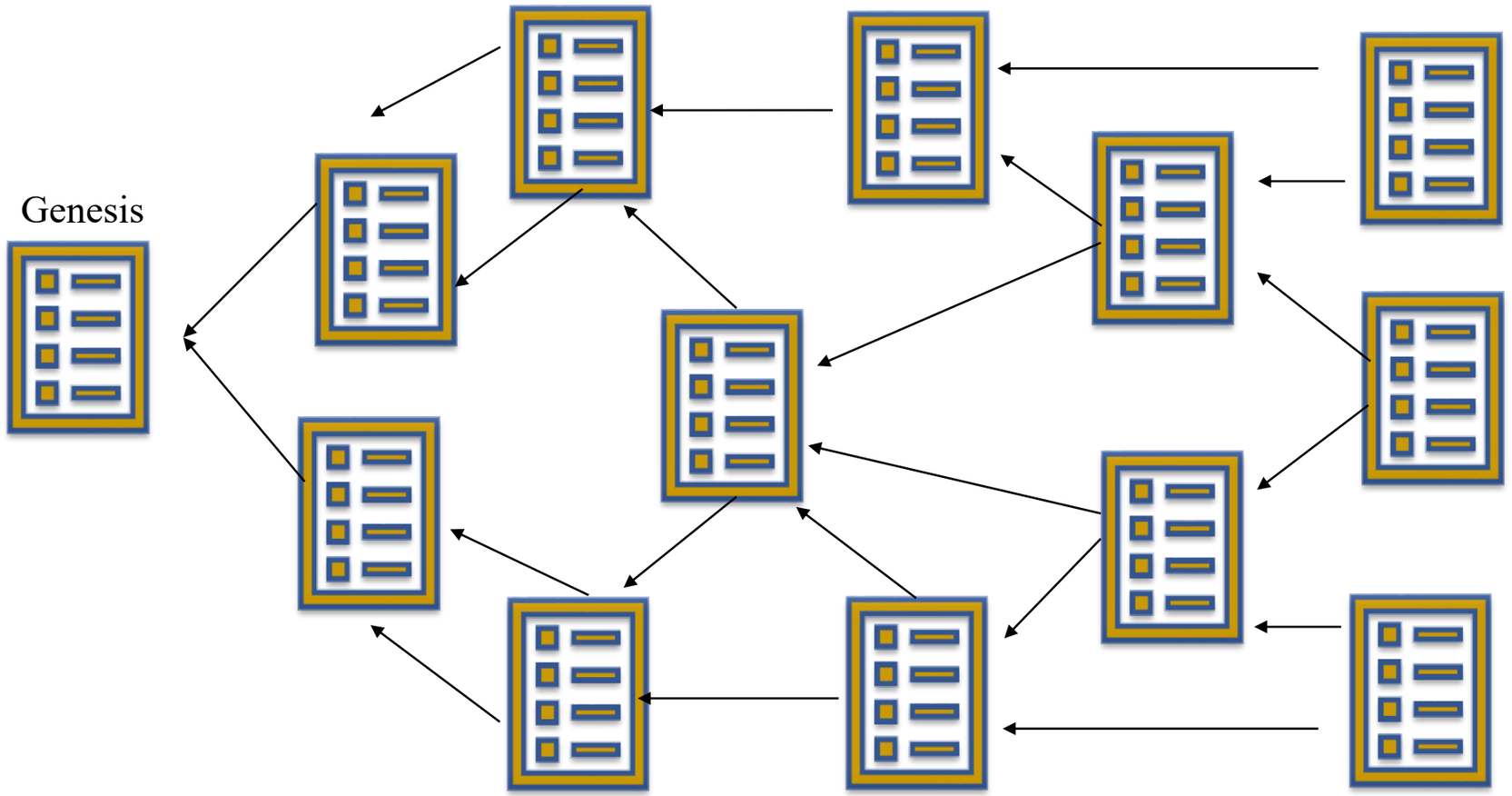
Current Paper (McPoRa for CPS)

Hashgraph Technology

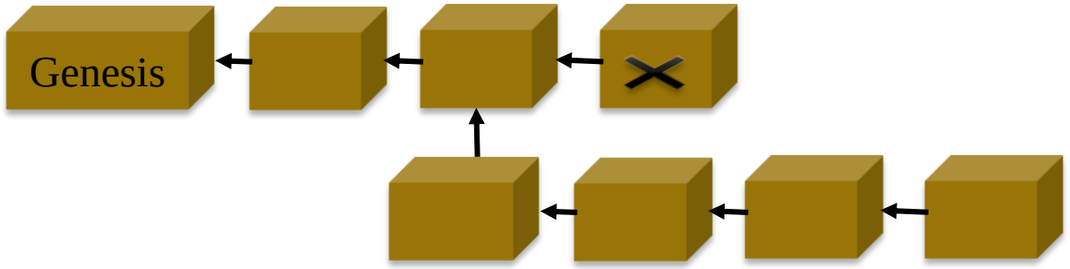




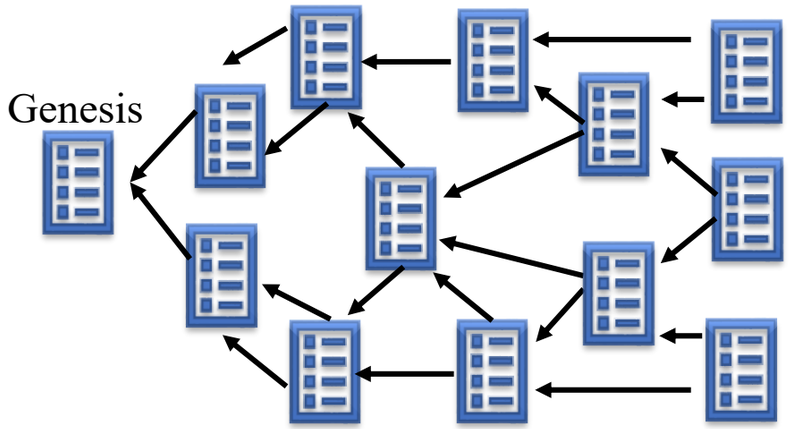
Tangle Technology



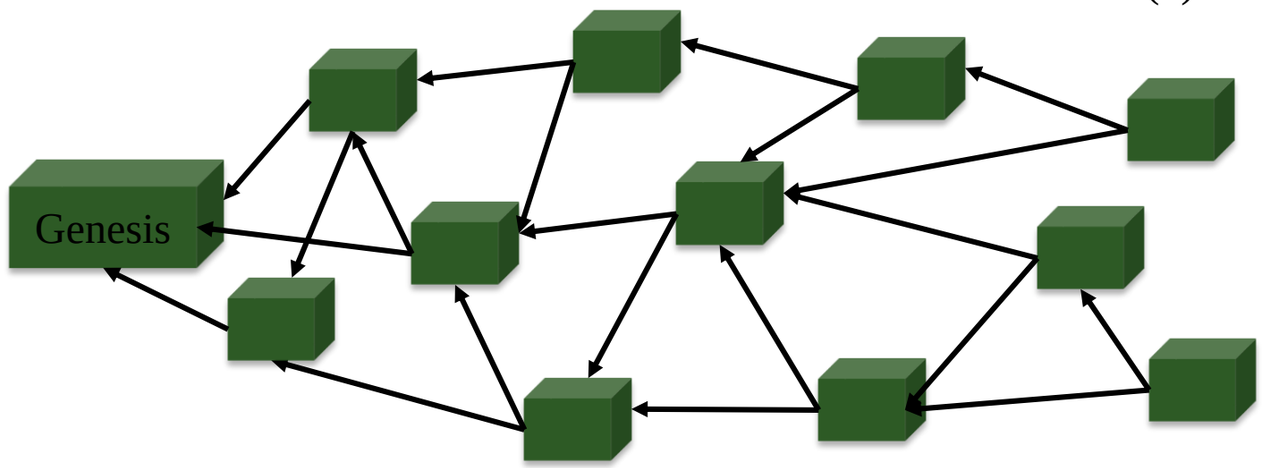
Comparative Perspective of BC, Tangle, Versus Propose MC



(a) Blockchain Technology



(b) Tangle Technology

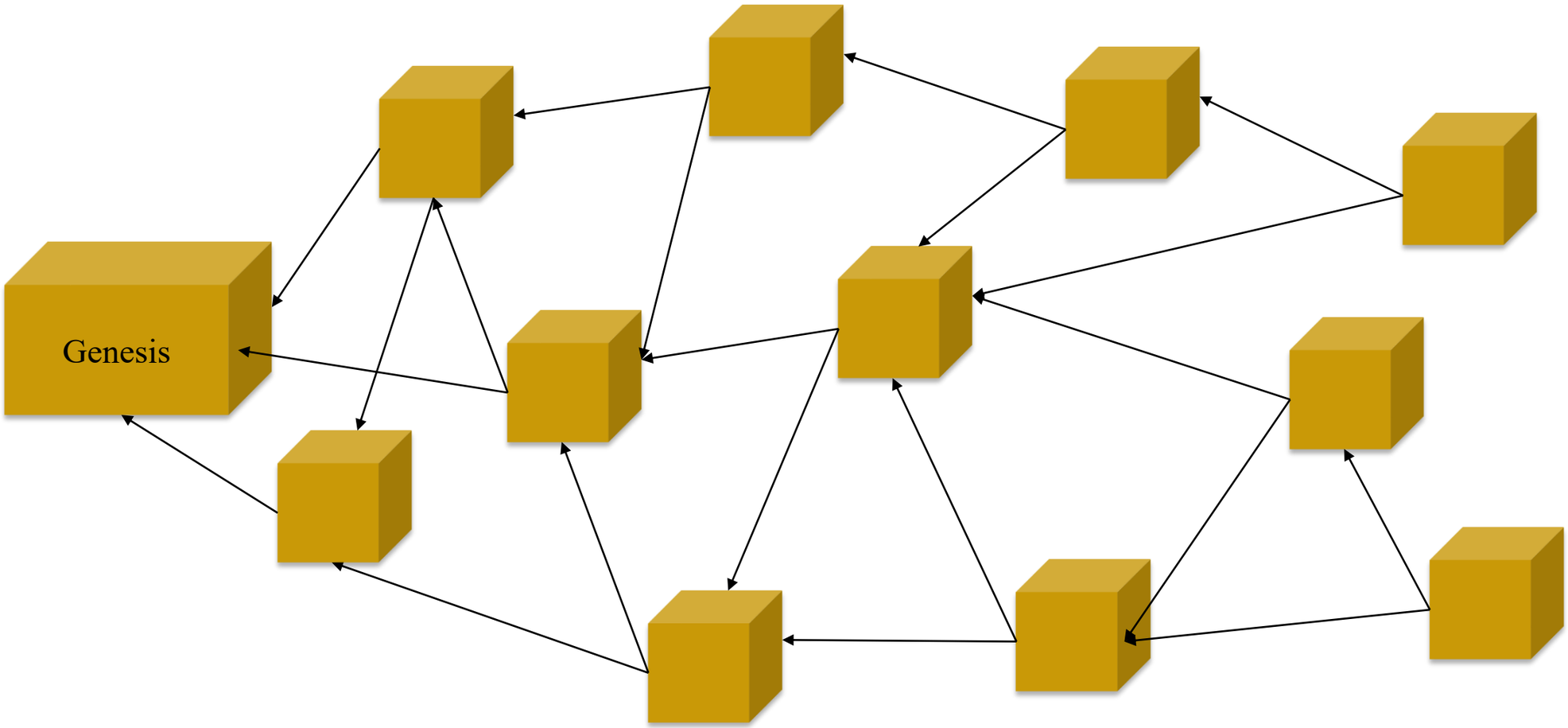


(c) Proposed Post-Blockchain Multichain as a Directed Acyclic Graph (DAG) Structure

Comparative Perspective of BC, Tangle, MC

Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRa (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions hash	• DAG linked List. • Block of transactions. • Reduced block.
Validation	Mining	Authentication	Mining	Virtual Voting (witness)	Authentication
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	aBFT	Predefined UID
Numeric System	Binary	Binary	Trinity	Binary	Binary
Involved Algorithms	HashCash	No	• Selection Algorithm • HashCash	No	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

Current Paper: Post-Blockchain (McPoRa)



Novel Contributions

SUIL

- Used in the authentication process.
- Part of each node.
- Eliminates miners.
- Low computation and calculation.

Multi-Chain

- Combination of Tangle and Blockchain.
- Data Structure.
- Speed up authentication.

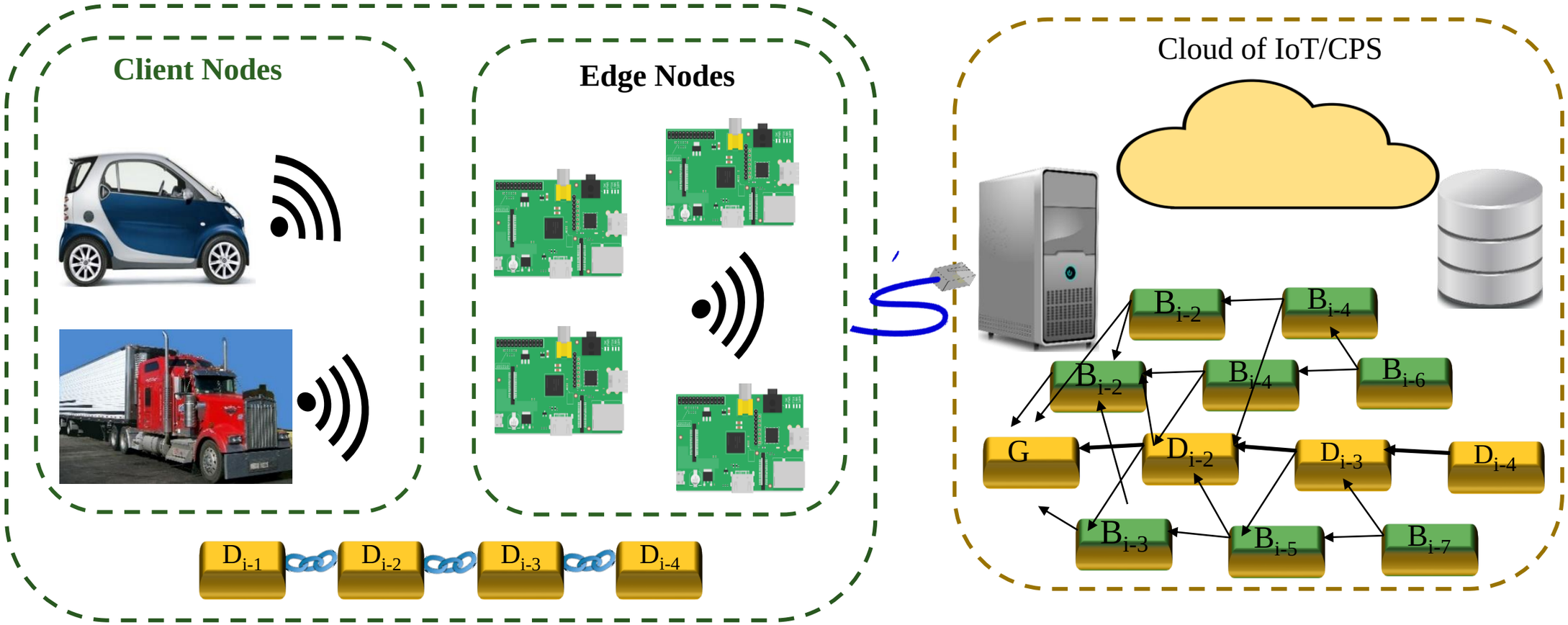
Authority Distribution

- No miners.
- Fairness.

Ledger Minimization

- Shortest Path (Local ledger)
- Reduction Process (Public ledger)

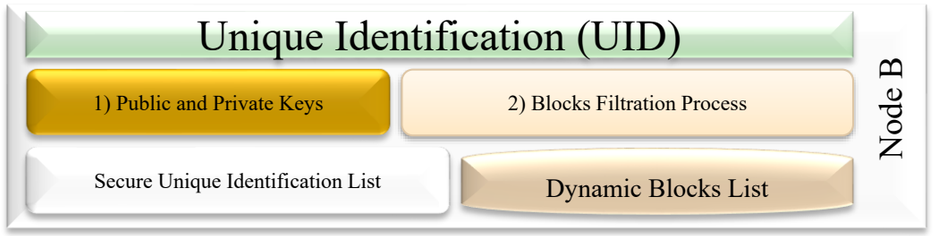
Multi-Chain Technology

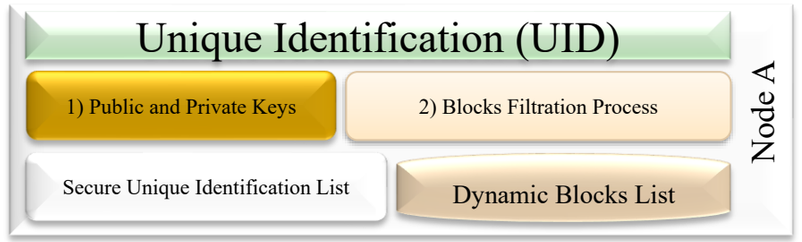


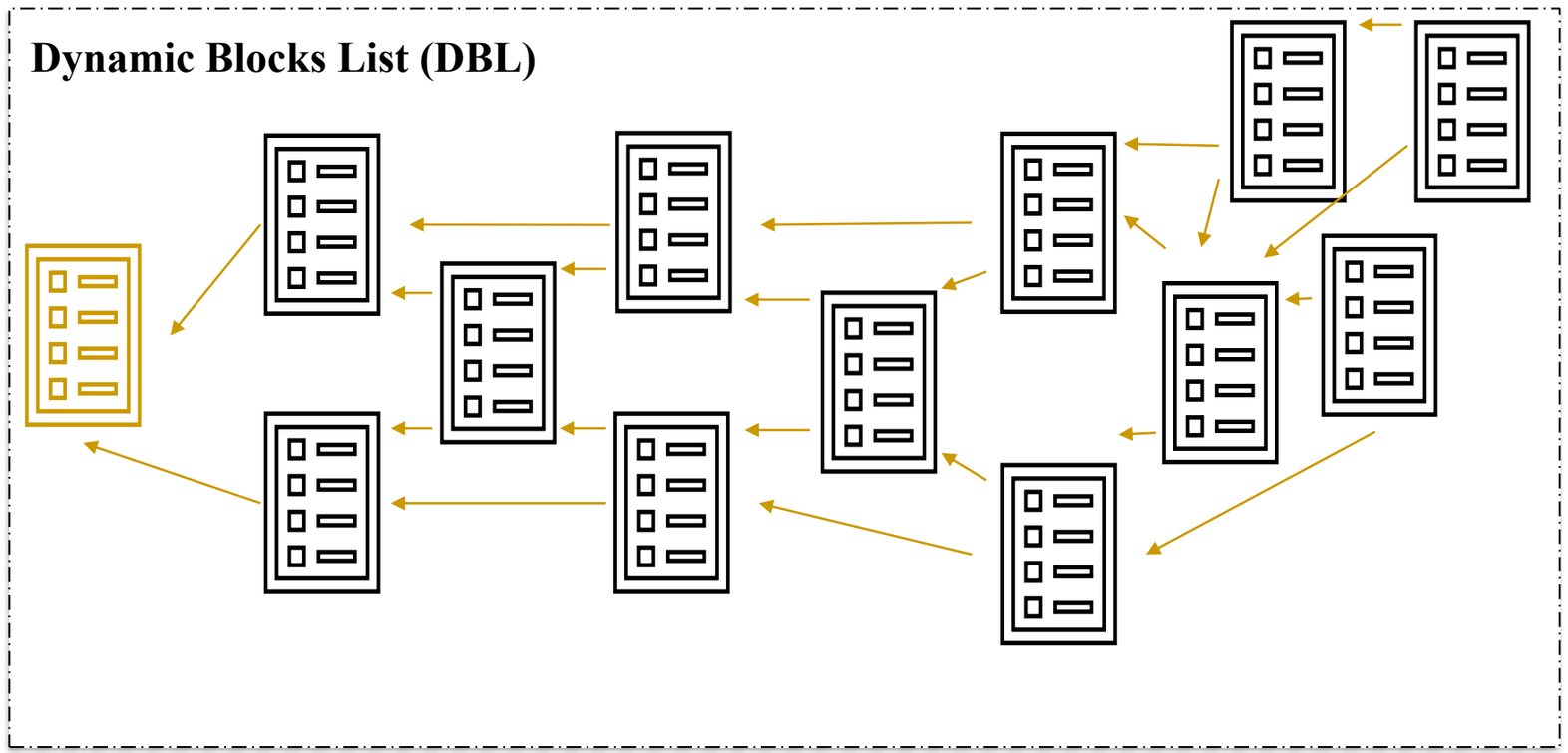
(a) Nodes-Chain

(b) Multi-Blockchains

McPoRa Components





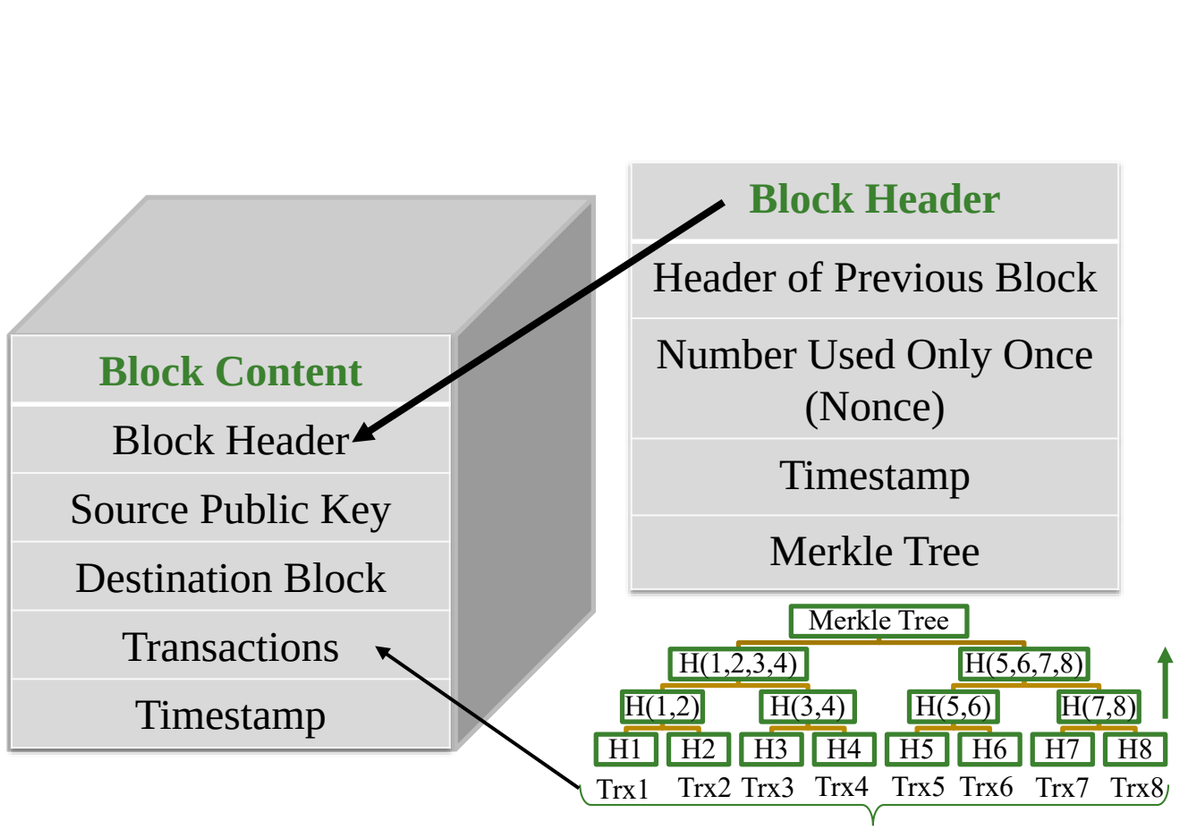


Secure Unique Identification List (SUIL)

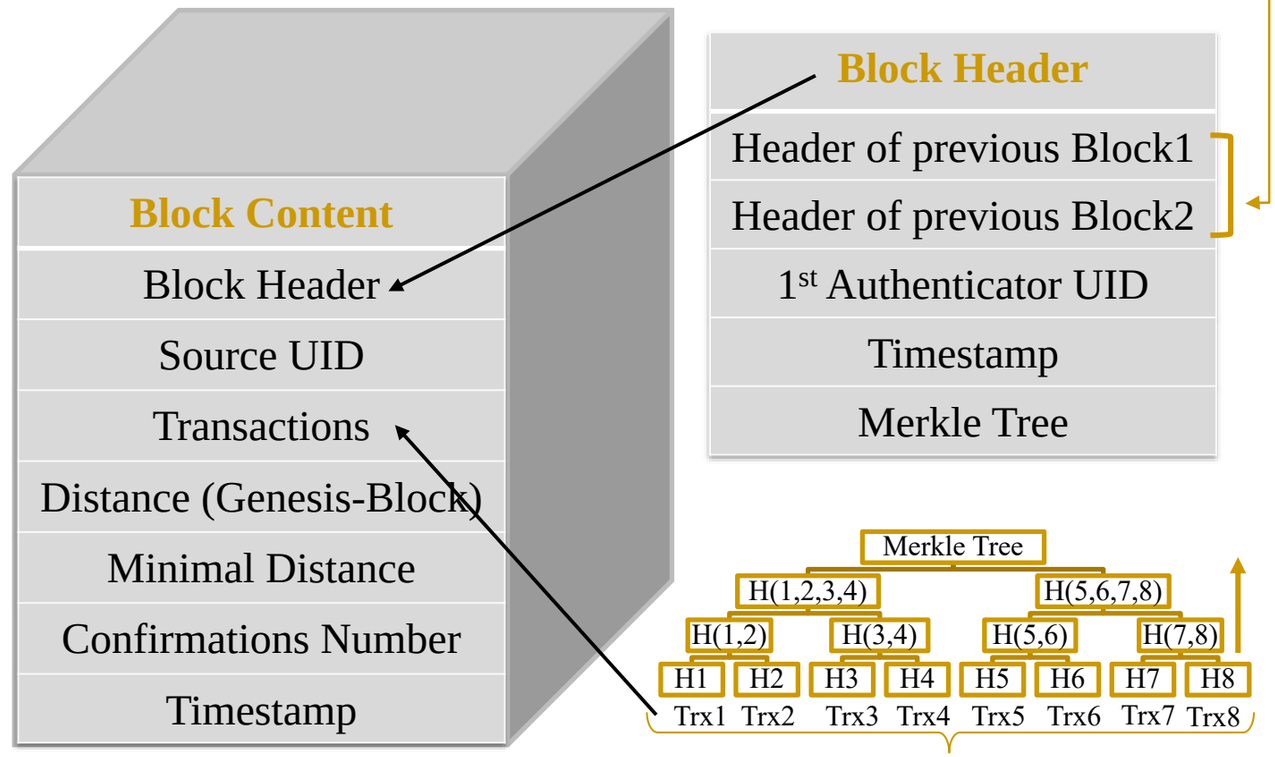
Secure IDs' file consists of all active Nodes joined the Private network.

Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique Identification (UID)

Proposed Block Structure

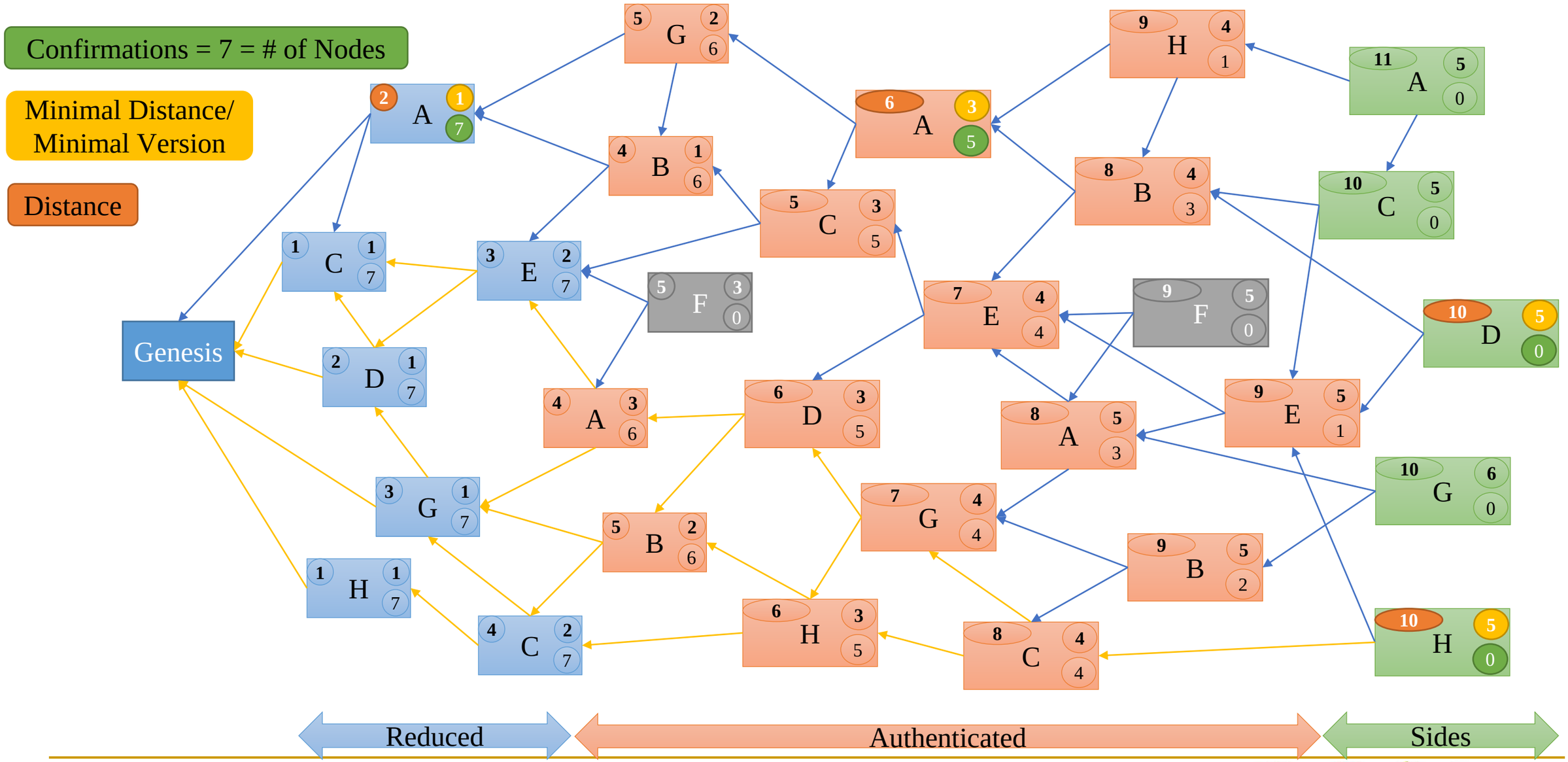


(a) For Traditional Blockchain



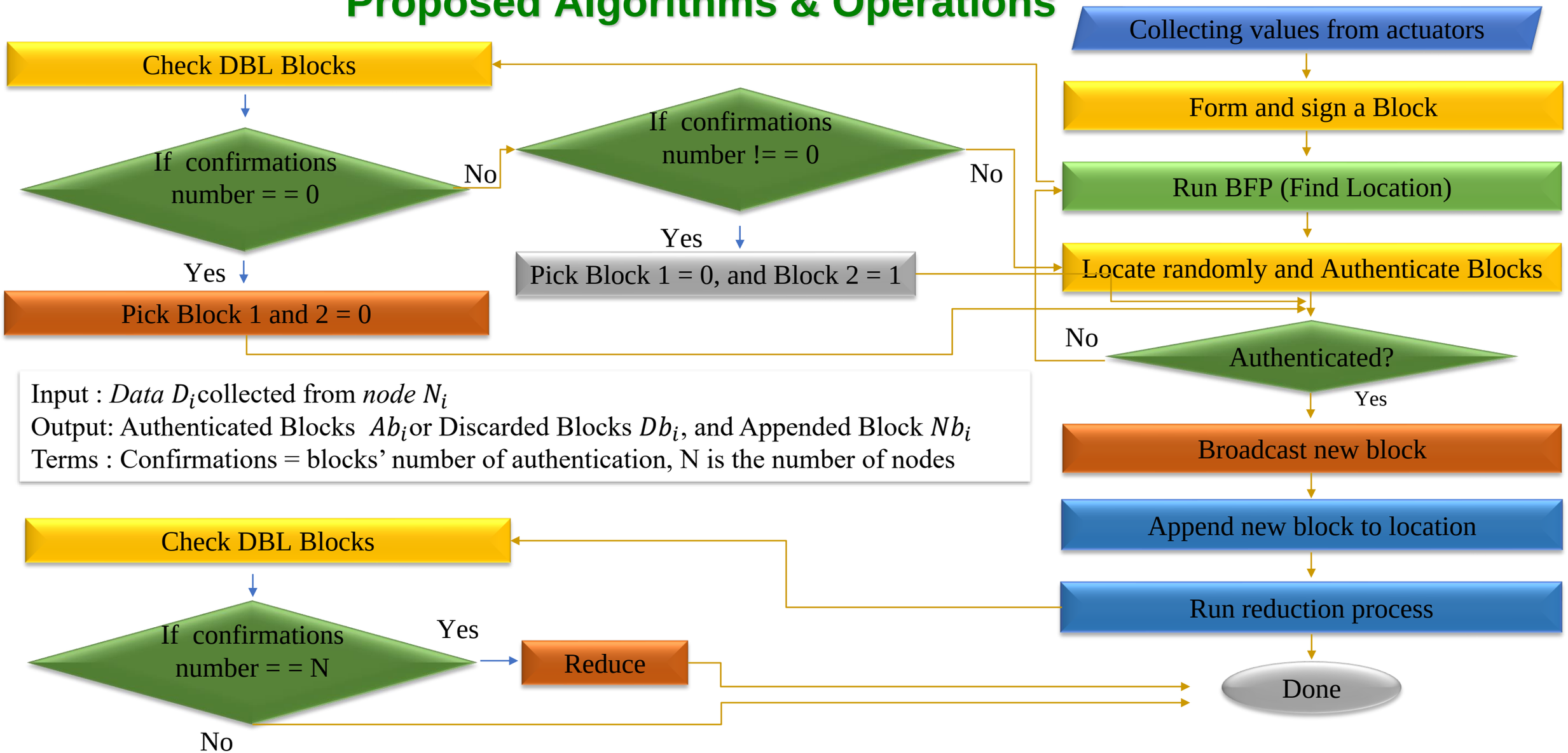
(b) For Proposed Post-Blockchain

Proposed Post-Blockchain Features



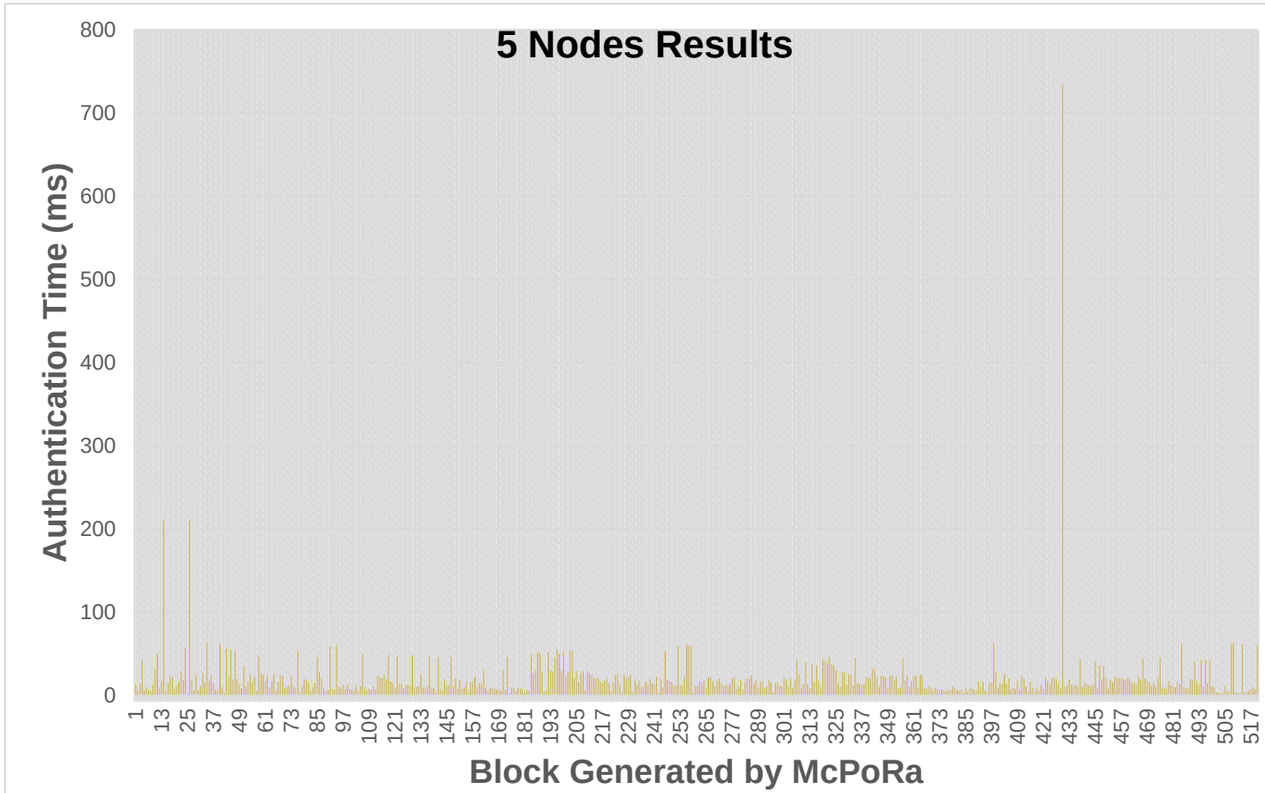
McPoRa

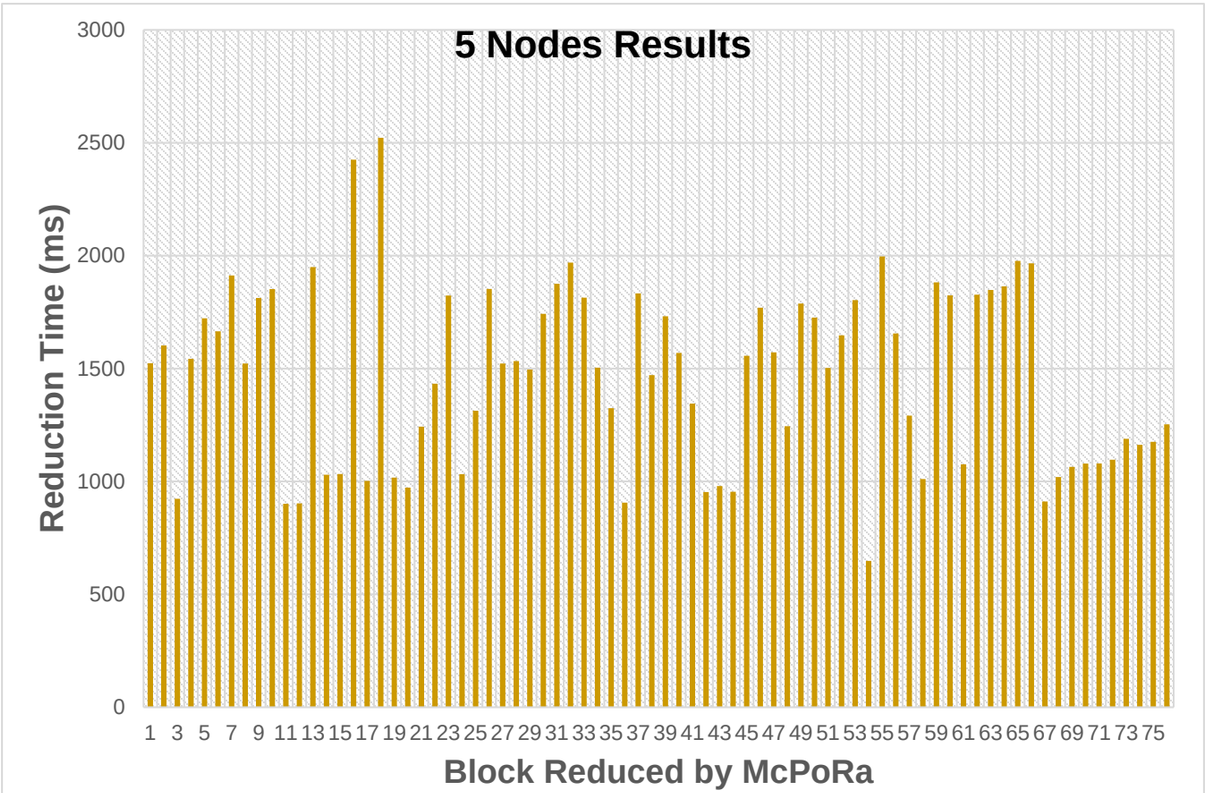
Proposed Algorithms & Operations



Results/ 5 Nodes Scenario

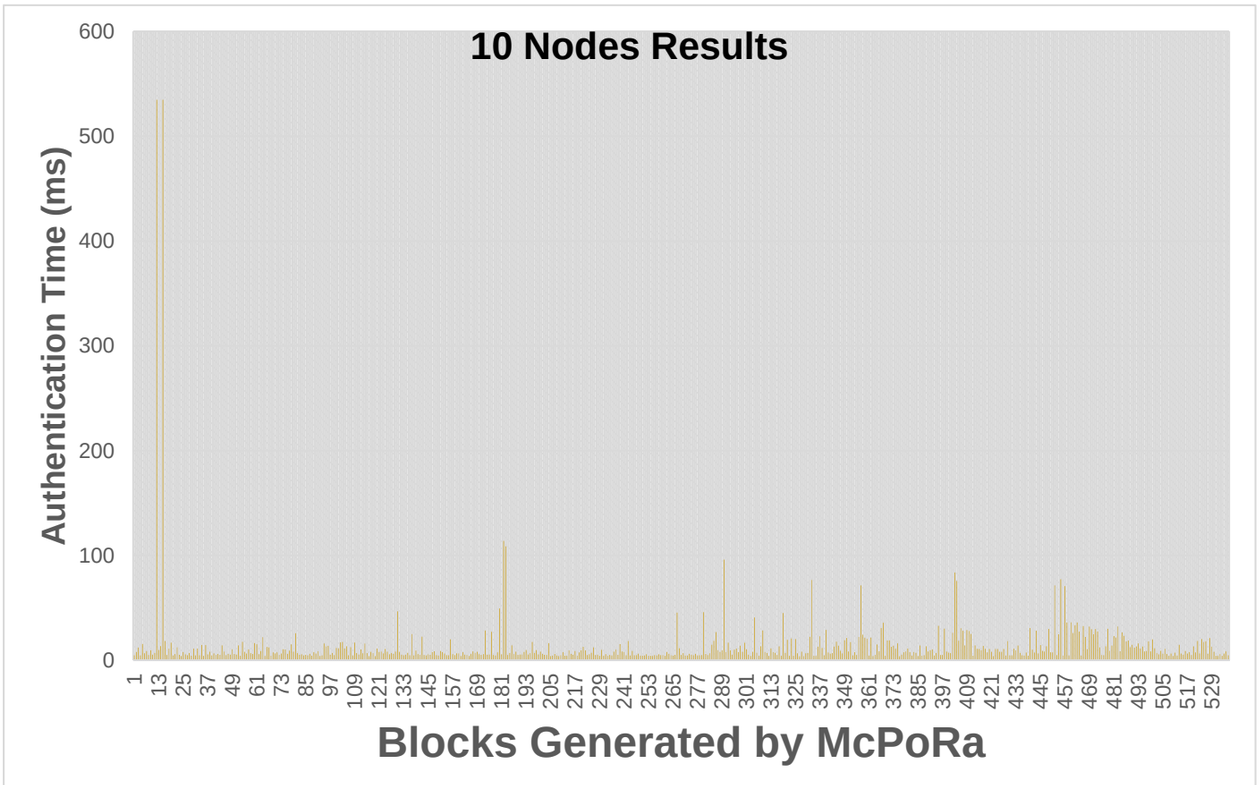
Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	2.66	206.52
Maximum	211	1291.6
Average	19.23	621

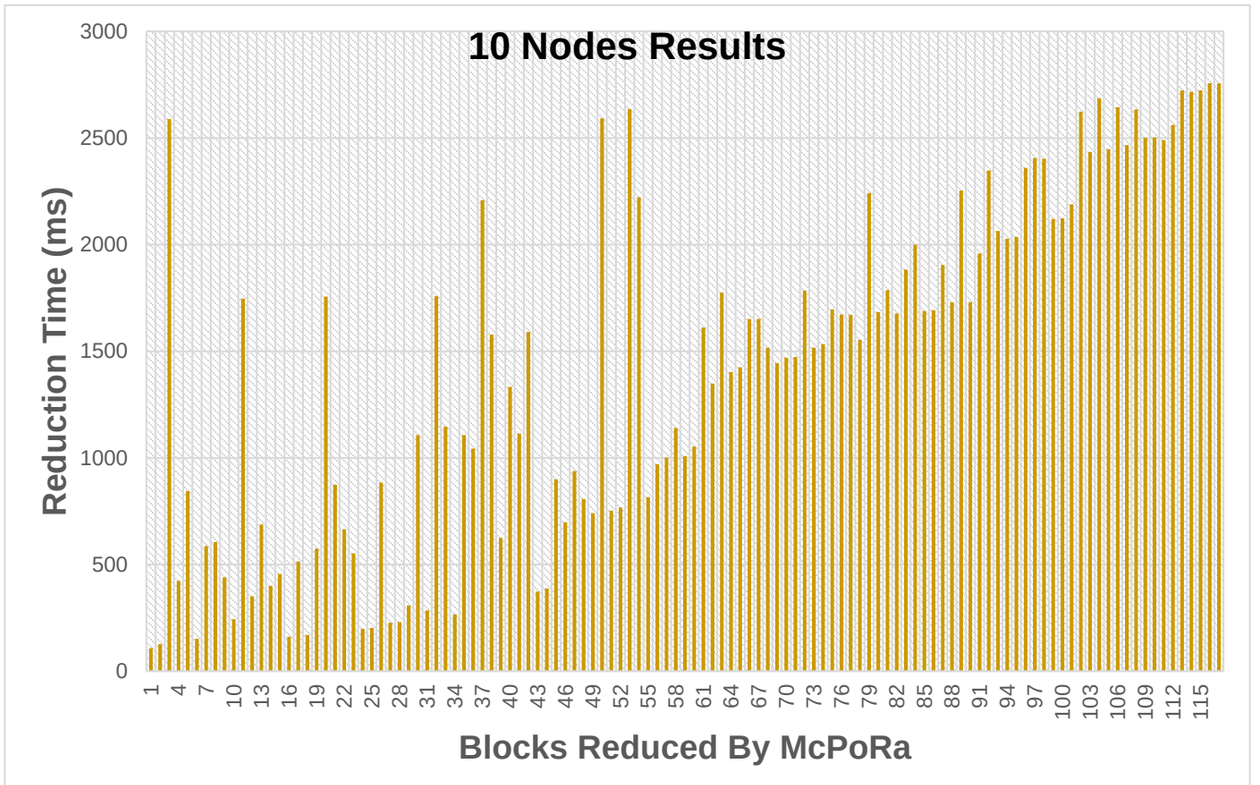




Results/ 10 Nodes Scenario

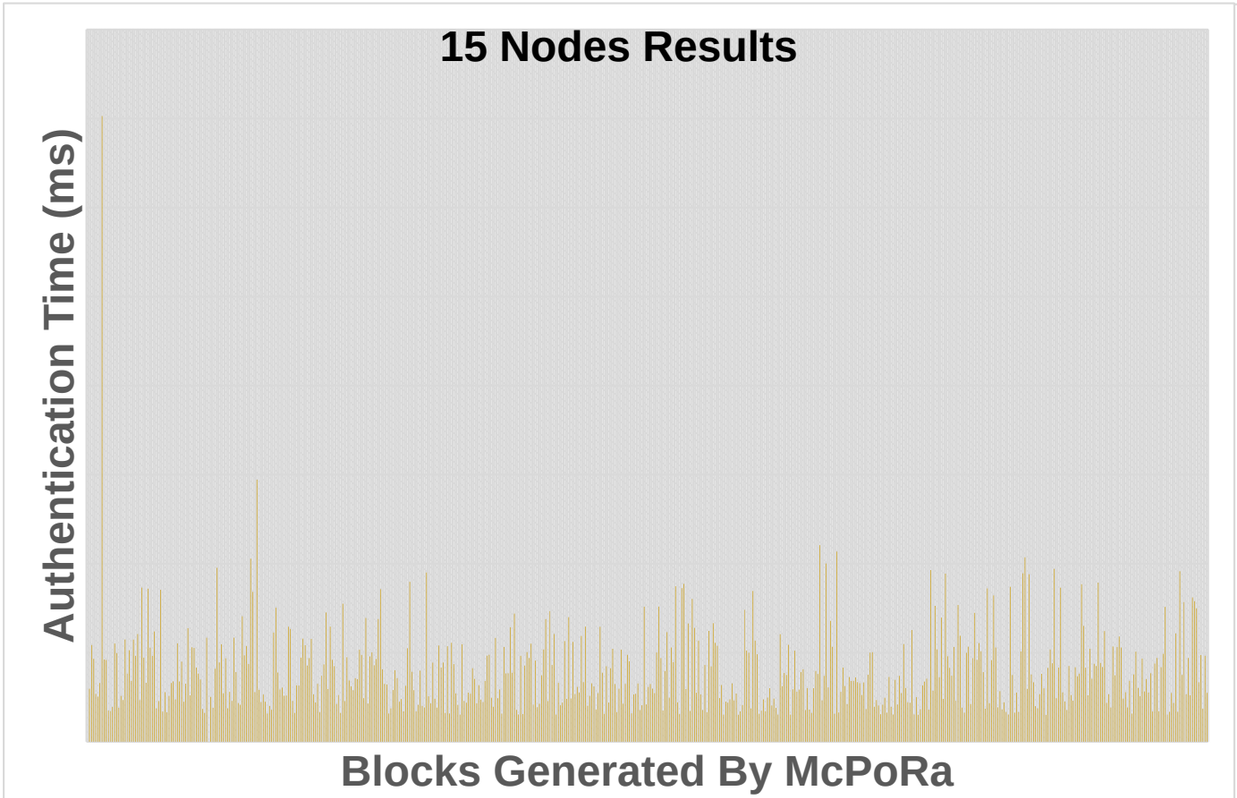
Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.21	145.8
Maximum	494	1420
Average	5.6	740

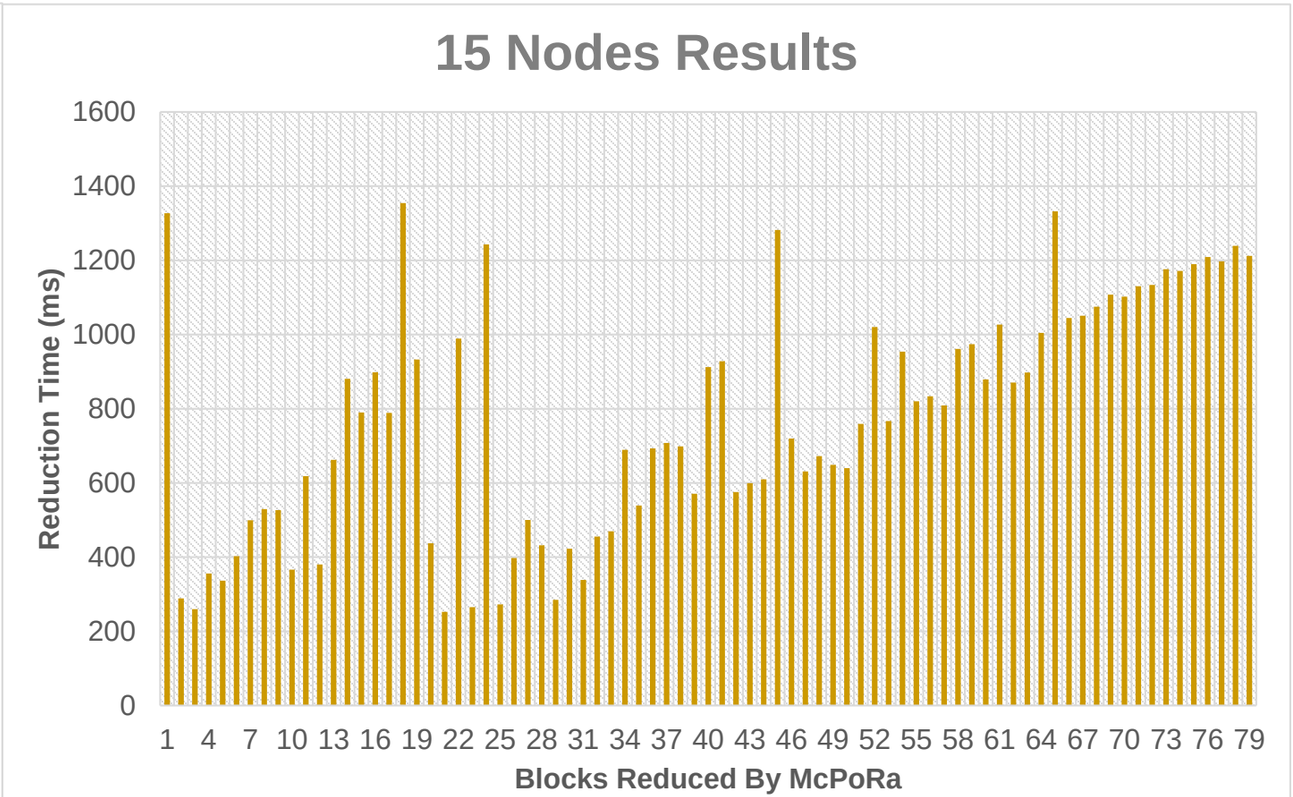




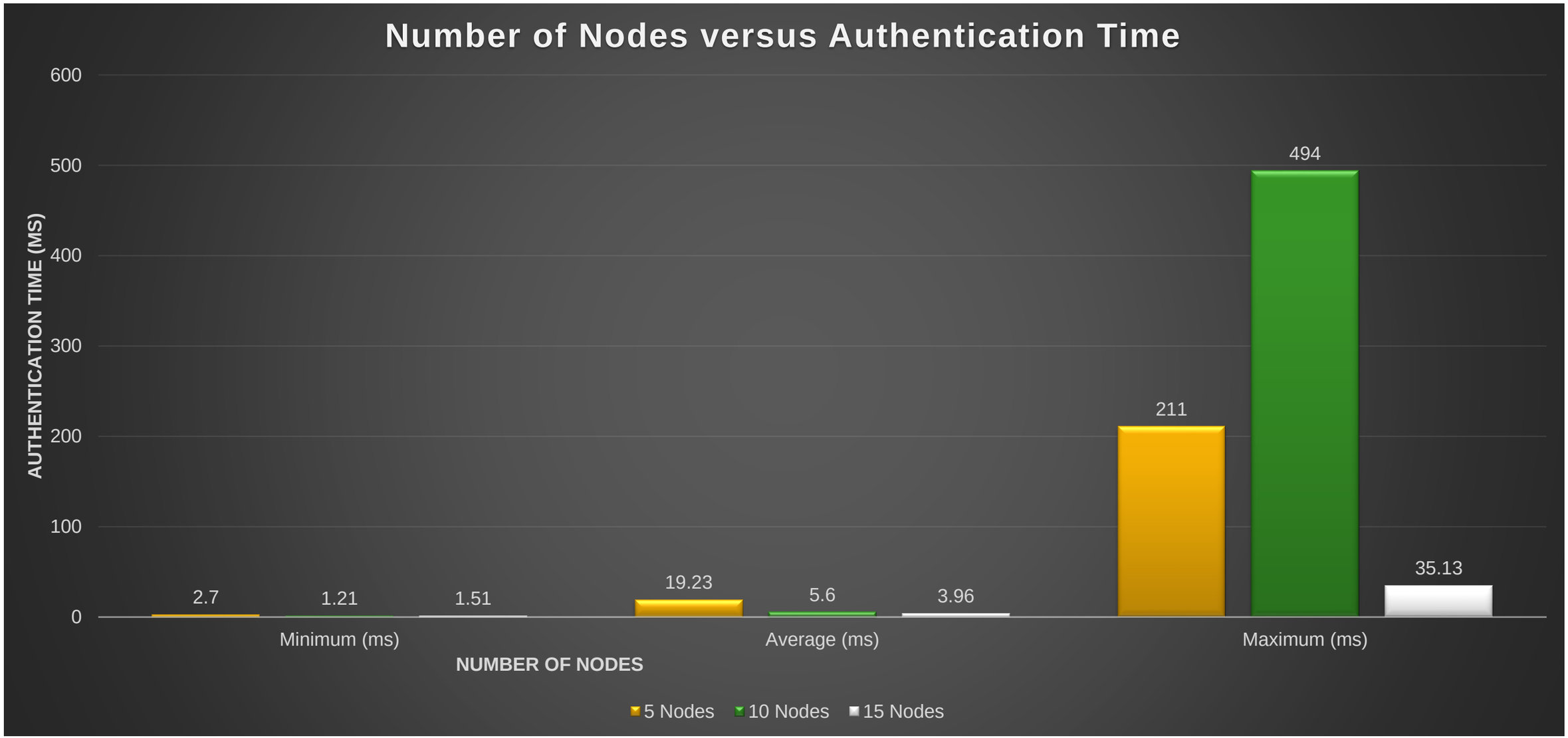
Results/ 15 Nodes Scenario

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

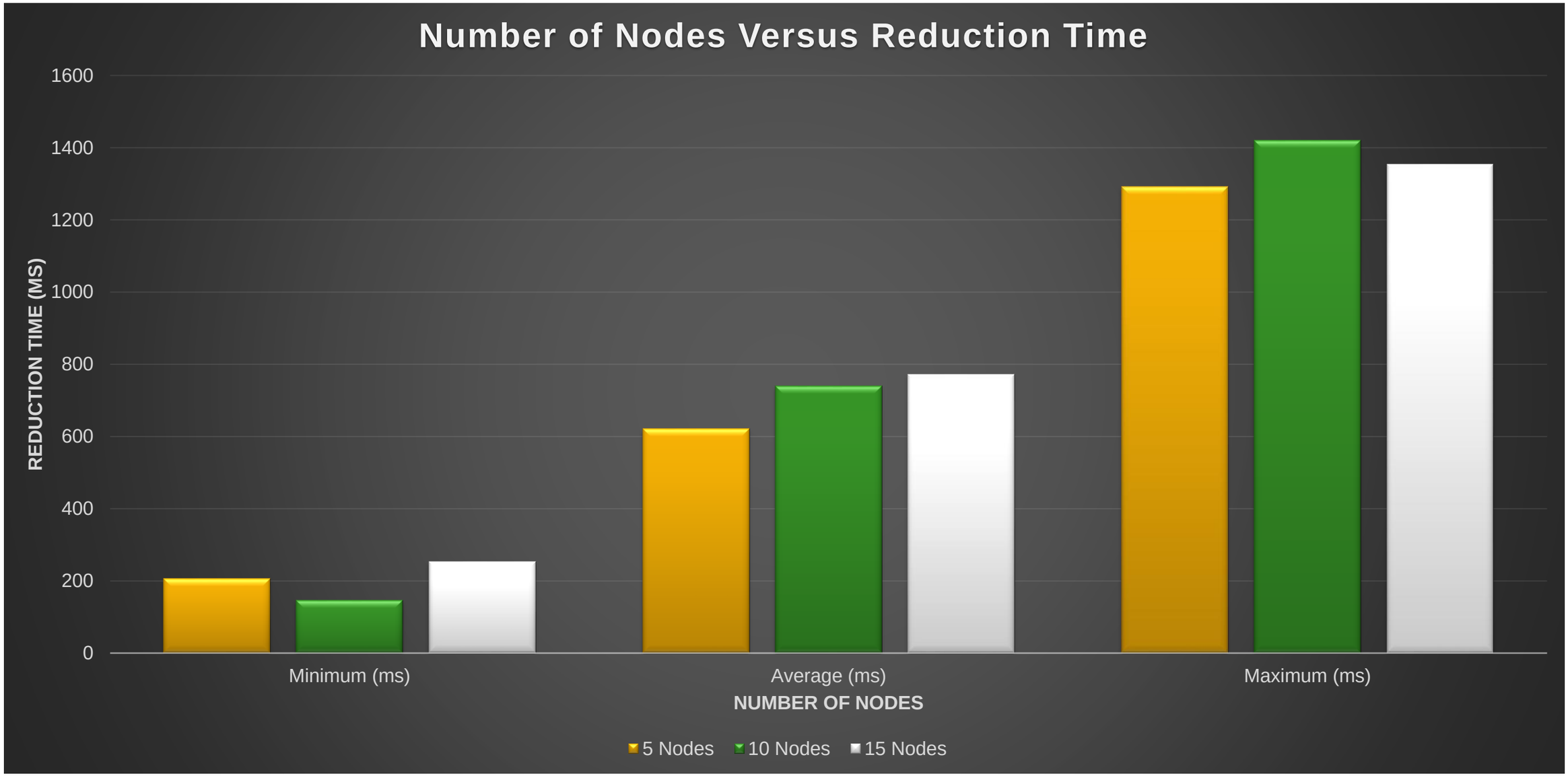




Results/ Authentication Time



Results/ Reduction Time



Comparative Perspective of McPoRA with Previous Related Work

Consensus Algorithms	Authentication Time (ms)	Ledger	Miners	Blockchain Type	Data Structure
Proof of Work (PoW) [14]	240,000	Full	Yes	Public	Blockchain
Proof of Importance (PoI) [20], [21]	60,000	Full	Yes	Public	Blockchain
Proof of Authority (PoA) [22], [23]	5000	Full	Yes	Permissioned	Blockchain
Proof of Authentication (PoAh) [15]	3000	Full	Yes	Private	Blockchain
Proof of PUF-Enabled Authentication (PoP) [12]	192.3	Full	Yes	Private	Blockchain
Proof of Block and Trade (PoBT) [24]	80-210	Full	Yes	Private	Blockchain
McPoRA (Current Paper)	3.9-19.23 (Avg.)	Portion	No	Private	Multi-Chain

Conclusions

IoT/CPS

Distributed Ledger Technology.

- Blockchain.
- Post-Blockchain
  - Tangle.
  - Hedera Hashgraph.

Issue: Consensus Algorithm & Linked List.

- Consensus Algorithm Design.
- New.

Proposed Multi-Chain Technology.

Contributions.

Future work.

References

- [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.
- [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.
- [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.
- [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.
- [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.
- [17] L. Baird, “The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance,” Swirlds, May 2016.

Acknowledgement(s)

- The authors would like to acknowledge financial support from the Saudi Arabian Cultural Mission (SACM).