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

A. Alkhodair\textsuperscript{1}, S. P. Mohanty\textsuperscript{1}, E. Kougianos\textsuperscript{2}, and D. Puthal\textsuperscript{3}

University of North Texas, Denton, TX, USA.\textsuperscript{1,2} 
Newcastle University, United Kingdom\textsuperscript{3}

Email: ahmadalkhodair@my.unt.edu\textsuperscript{1}, saraju.mohanty@unt.edu\textsuperscript{1}, elias.kougianos@unt.edu\textsuperscript{2}, Deepak.Puthal@newcastle.ac.uk\textsuperscript{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

Cyber Physical Systems
Internet of Things
Smart Things
Analysis, Decision & Feedback
Actuators

Smart Transportation
Smart Healthcare
Smart Grid
Smart Infrastructure
Smart Administration
Introduction/Challenges

- Latency
- Power Consumption
- Security
- Scalability
- Accuracy

CPS/IoT
Blockchain Technology
Introduction/Blockchain

Genesis

[Diagram of blockchain blocks connected in a network with an 'X' symbol on one of the blocks]
The Blockchain faces Many Challenges

- Fake Block Generation
- High Energy Consumption
- Lack of Scalability
- Limited One chain Storage Capability
- High Latency
- Lack of Privacy

Blockchain – Next Generation or Post-Blockchain

Hashgraph

Tangle

Current Paper (McPoRa for CPS)
Hashgraph Technology

Container/ Event/ Group of transactions. Signed by the owner broadcast it to others randomly (Gossip about Gossip Protocol)

Transactions

TimeStamp
Hash 1/ Diagonal
Hash 2/ Vertical

Round 1
A1 B1 C1 D1

Round 2
A2 B2 C2 D2

Gossip about Gossip Protocol
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
<table>
<thead>
<tr>
<th>Features/Technology</th>
<th>Blockchain (Bitcoin)</th>
<th>Proof of Authentication</th>
<th>Tangle</th>
<th>HashGraph</th>
<th>McPoRa (current Paper)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linked Lists</td>
<td>• One linked list of blocks.</td>
<td>• One linked list of blocks.</td>
<td>• DAG linked list.</td>
<td>• DAG linked List.</td>
<td>• DAG linked List.</td>
</tr>
<tr>
<td></td>
<td>• Block of transactions.</td>
<td>• Block of transactions.</td>
<td>• One transaction.</td>
<td>• Container of transactions hash</td>
<td>• Block of transactions.</td>
</tr>
<tr>
<td>Validation</td>
<td>Mining</td>
<td>Authentication</td>
<td>Mining</td>
<td>Virtual Voting (witness)</td>
<td>Authentication</td>
</tr>
<tr>
<td>Type of validation</td>
<td>Miners</td>
<td>Trusted Nodes</td>
<td>Transactions</td>
<td>Containers</td>
<td>All Nodes</td>
</tr>
<tr>
<td>Ledger Requirement</td>
<td>Full ledger required</td>
<td>Full ledger required</td>
<td>Portion based on longest and shortest paths.</td>
<td>Full ledger required</td>
<td>Portion based on authenticators’ number</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Digital Signatures</td>
<td>Digital Signatures</td>
<td>Quantum key signature</td>
<td>Digital Signatures</td>
<td>Digital Signatures</td>
</tr>
<tr>
<td>Hash function</td>
<td>SHA 256</td>
<td>SHA 256</td>
<td>KECCAK-384</td>
<td>SHA 384</td>
<td>SCRYPT</td>
</tr>
<tr>
<td>Consensus</td>
<td>Proof of Work</td>
<td>Cryptographic Authentication</td>
<td>Proof of Work</td>
<td>aBFT</td>
<td>Predefined UID</td>
</tr>
<tr>
<td>Numeric System</td>
<td>Binary</td>
<td>Binary</td>
<td>Trinity</td>
<td>Binary</td>
<td>Binary</td>
</tr>
<tr>
<td>Involved Algorithms</td>
<td>HashCash</td>
<td>No</td>
<td>• Selection Algorithm</td>
<td>No</td>
<td>BFP</td>
</tr>
<tr>
<td>Decentralization</td>
<td>Partially</td>
<td>Partially</td>
<td>Fully</td>
<td>Fully</td>
<td>Fully</td>
</tr>
<tr>
<td>Appending Requirements</td>
<td>Longest chain</td>
<td>One chain</td>
<td>Selection Algorithm</td>
<td>Full Randomness</td>
<td>Filtration Process</td>
</tr>
<tr>
<td>Energy Requirements</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Node Requirements</td>
<td>High Resources Node</td>
<td>Limited Resources Node</td>
<td>High Resources Node</td>
<td>High Resources Node</td>
<td>Limited Resources Node</td>
</tr>
<tr>
<td>Design Purpose</td>
<td>Cryptocurrency</td>
<td>IoT applications</td>
<td>IoT/Cryptocurrency</td>
<td>Cryptocurrency</td>
<td>IoT/CPS applications</td>
</tr>
</tbody>
</table>
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

Cloud of IoT/CPS

Client Nodes

Edge Nodes

McPoRa
McPoRa Components

Dynamic Blocks List (DBL)

Secure Unique Identification List (SUIL)

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

<table>
<thead>
<tr>
<th>Hashed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node A Unique Identification (UID)</td>
</tr>
<tr>
<td>Node B Unique Identification (UID)</td>
</tr>
<tr>
<td>Node C Unique Identification (UID)</td>
</tr>
<tr>
<td>Node D Unique Identification (UID)</td>
</tr>
<tr>
<td>Node E Unique Identification (UID)</td>
</tr>
<tr>
<td>Node F Unique Identification (UID)</td>
</tr>
<tr>
<td>Node G Unique Identification (UID)</td>
</tr>
<tr>
<td>Node H Unique Identification (UID)</td>
</tr>
<tr>
<td>Node I Unique Identification (UID)</td>
</tr>
</tbody>
</table>
Proposed Block Structure

(a) For Traditional Blockchain

- Block Content
  - Block Header
  - Source Public Key
  - Destination Block
  - Transactions
  - Timestamp

- Block Header
  - Header of Previous Block
  - Number Used Only Once (Nonce)
  - Timestamp
  - Merkle Tree

- Transactions
  - Trx1, Trx2, Trx3, Trx4, Trx5, Trx6, Trx7, Trx8

- Merkle Tree
  - H(1,2,3,4), H(1,2), H1, H2, Trx1, Trx2, Trx3, Trx4
  - H(3,4), H3, H4, Trx5, Trx6
  - H(5,6,7,8), H(5,6), H5, H6, Trx7
  - H(7,8), H7, H8, Trx8

(b) For Proposed Post-Blockchain

- Block Header
  - Header of previous Block1
  - Header of previous Block2
  - 1st Authenticator UID
  - Timestamp
  - Merkle Tree

- Block Content
  - Block Header
  - Source UID
  - Transactions
  - Distance (Genesis-Block)
  - Minimal Distance
  - Confirmations Number
  - Timestamp

- Merkle Tree
  - H(1,2,3,4), H(1,2), H1, H2, Trx1, Trx2, Trx3
  - H(3,4), H3, H4, Trx4, Trx5
  - H(5,6,7,8), H(5,6), H5, H6, Trx6
  - H(7,8), H7, H8, Trx7, Trx8

Location
Proposed Post-Blockchain Features

Confirmations = 7 = # of Nodes

Minimal Distance/Minimal Version

Distance

McPoRa
Proposed Algorithms & Operations

Check DBL Blocks

If confirmations number \(= 0\)

No

Yes

Pick Block 1 and 2 = 0

If confirmations number \(!= 0\)

No

Yes

Pick Block 1 = 0, and Block 2 = 1

Collecting values from actuators

Form and sign a Block

Run BFP (Find Location)

Locate randomly and Authenticate Blocks

Authenticated?

Yes

No

Broadcast new block

Append new block to location

Run reduction process

Done

Input: Data \(D_i\) collected from node \(N_i\)

Output: Authenticated Blocks \(A_b_i\) or Discarded Blocks \(D_b_i\), and Appended Block \(N_b_i\)

Terms: Confirmations = blocks’ number of authentication, \(N\) is the number of nodes
Results/ 5 Nodes Scenario

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Authentication (ms)</th>
<th>Reduction (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>2.66</td>
<td>206.52</td>
</tr>
<tr>
<td>Maximum</td>
<td>211</td>
<td>1291.6</td>
</tr>
<tr>
<td>Average</td>
<td>19.23</td>
<td>621</td>
</tr>
</tbody>
</table>

![5 Nodes Results](image1)

Block Generated by McPoRa

![5 Nodes Results](image2)

Block Reduced by McPoRa
# Results/ 10 Nodes Scenario

## Authentication Time (ms) vs. Reduction Time (ms)

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Authentication (ms)</th>
<th>Reduction (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>1.21</td>
<td>145.8</td>
</tr>
<tr>
<td>Maximum</td>
<td>494</td>
<td>1420</td>
</tr>
<tr>
<td>Average</td>
<td>5.6</td>
<td>740</td>
</tr>
</tbody>
</table>

### 10 Nodes Results

- **Blocks Generated by McPoRa**
- **Blocks Reduced By McPoRa**

**Graphs**
- Authentication Time (ms) vs. Blocks Generated by McPoRa
- Reduction Time (ms) vs. Blocks Reduced By McPoRa
### Results/ 15 Nodes Scenario

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Authentication (ms)</th>
<th>Reduction (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>1.51</td>
<td>252.6</td>
</tr>
<tr>
<td>Maximum</td>
<td>35.14</td>
<td>1354.6</td>
</tr>
<tr>
<td>Average</td>
<td>3.97</td>
<td>772.53</td>
</tr>
</tbody>
</table>

#### 15 Nodes Results

**Authentication Time (ms)**

- Blocks Generated By McPoRa

**Reduction Time (ms)**

- Blocks Reduced By McPoRa
Results/ Authentication Time

Number of Nodes versus Authentication Time

- Minimum (ms): 0
- Average (ms): 5.6
- Maximum (ms): 494

AUTHENTICATION TIME (MS)

NUMBER OF NODES:
- 5 Nodes
- 10 Nodes
- 15 Nodes

08 July 2020

McPoRa
Results/ Reduction Time

Number of Nodes Versus Reduction Time

- Minimum (ms)
- Average (ms)
- Maximum (ms)

NUMBER OF NODES

- 5 Nodes
- 10 Nodes
- 15 Nodes

08 July 2020
<table>
<thead>
<tr>
<th>Consensus Algorithms</th>
<th>Authentication Time (ms)</th>
<th>Ledger</th>
<th>Miners</th>
<th>Blockchain Type</th>
<th>Data Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of Work (PoW) [14]</td>
<td>240,000</td>
<td>Full</td>
<td>Yes</td>
<td>Public</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Proof of Importance (PoI)  [20, 21]</td>
<td>60,000</td>
<td>Full</td>
<td>Yes</td>
<td>Public</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Proof of Authority (PoA)  [22, 23]</td>
<td>5000</td>
<td>Full</td>
<td>Yes</td>
<td>Permissioned</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Proof of Authentication (PoAh) [15]</td>
<td>3000</td>
<td>Full</td>
<td>Yes</td>
<td>Private</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Proof of PUF-Enabled Authentication (PoP) [12]</td>
<td>192.3</td>
<td>Full</td>
<td>Yes</td>
<td>Private</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Proof of Block and Trade (PoBT) [24]</td>
<td>80-210</td>
<td>Full</td>
<td>Yes</td>
<td>Private</td>
<td>Blockchain</td>
</tr>
<tr>
<td>McPoRA (Current Paper)</td>
<td>3.9-19.23 (Avg.)</td>
<td>Portion</td>
<td>No</td>
<td>Private</td>
<td>Multi-Chain</td>
</tr>
</tbody>
</table>
Conclusions

- IoT/CPS
- Distributed Ledger Technology.
- Issue: Consensus Algorithm & Linked List.
- Proposed Multi-Chain Technology.
- Contributions.
- Future work.

- Blockchain.
- Post-Blockchain
  - Tangle.
  - Hedera Hashgraph.
- Consensus Algorithm Design.
- New.
References


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