ASID: Accessible Secure Unique Identification File Based Device Security in Next Generation Blockchains

Ahmad J. Alkhodair*, Saraju P. Mohanty*, Elias Kougianos†,
* Department of Computer Science and Engineering, University of North Texas, USA
† Department of Electrical Engineering, University of North Texas, USA
Email: AhmadAlkhodair@my.unt.edu, saraju.mohanty@unt.edu, elias.kougianos@unt.edu

***Abstract*—In this paper, a new hardware security method is proposed to secure resource-constrained devices using blockchain technology. The new method is utilizing manufacturer parameters of a device, such as PUF, memory, firmware parameters, etc. to create a linked list of unique identification (UID) data, or an identity that could secure, monitor, and act accordingly to ensure device integrity and honesty.**

***Index terms*—** Cyber Physical Systems (CPS), Internet-of-Things (IoT), Device Authentication, Unique Identification (UID), Unique Node Identification Generator (UDIG), Virtual Node (VN), Genesis Blockchain, Multi-Chain (MC).

I. Introduction

Device authentication using devices' digital identity and signatures is a common solution [1]. In this paper, hardware security and integrity, digital identity, and authentication are targeted using blockchain technology to increase device security and ensure integrity. The proposed method is to create an independent ledger that stores extrinsic parameters such as memory characteristics, firmware parameters, PUF parameters, etc. based each device's manufacturer specifications, hashed and processed to generate a UID and store it in the ledger for data authentication purposes. The blocks of a chain represent the virtual existence of the device in the independent ledger. The whole method represents a registration process through a private type of blockchain to create an independent ledger to authenticate, monitor, discard, and add new devices to the network. The whole linked list represents the connection between the nodes' UIDs and the blocks. Figure 1 is a high level depiction of the NodeChain proposed in this paper.

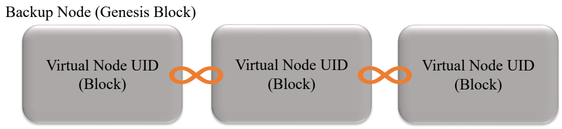
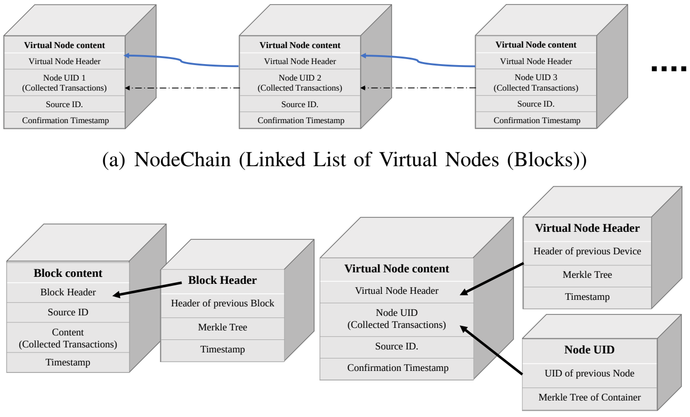


Fig. 1: High-Level Representation of The Proposed Method

II. The Proposed Next Generation BLOCKCHAIN TECHNOLOGY: The NodeChain

The NodeChain is a new method proposed in this paper to resolve the security and integrity issues at the devices level. NodeChain is a linked list of virtual existence of the real participants within the network to monitor their behavior and ensure security. NodeChain is built on the current structure of the traditional blockchain to create a chain of nodes. However, the purpose and the consensus algorithm differs from the traditional one. The purpose of this chain is to link device digital IDs and make tit very expensive to impersonate or attack them. NodeChain is proposed as a supportive technology to be integrated in any platform such as Multi-Chain (MC) technology to replace the registration process of assigning digital signatures and digital identities using the traditional form of blockchain and integrate it with the next generation of blockchain [2].

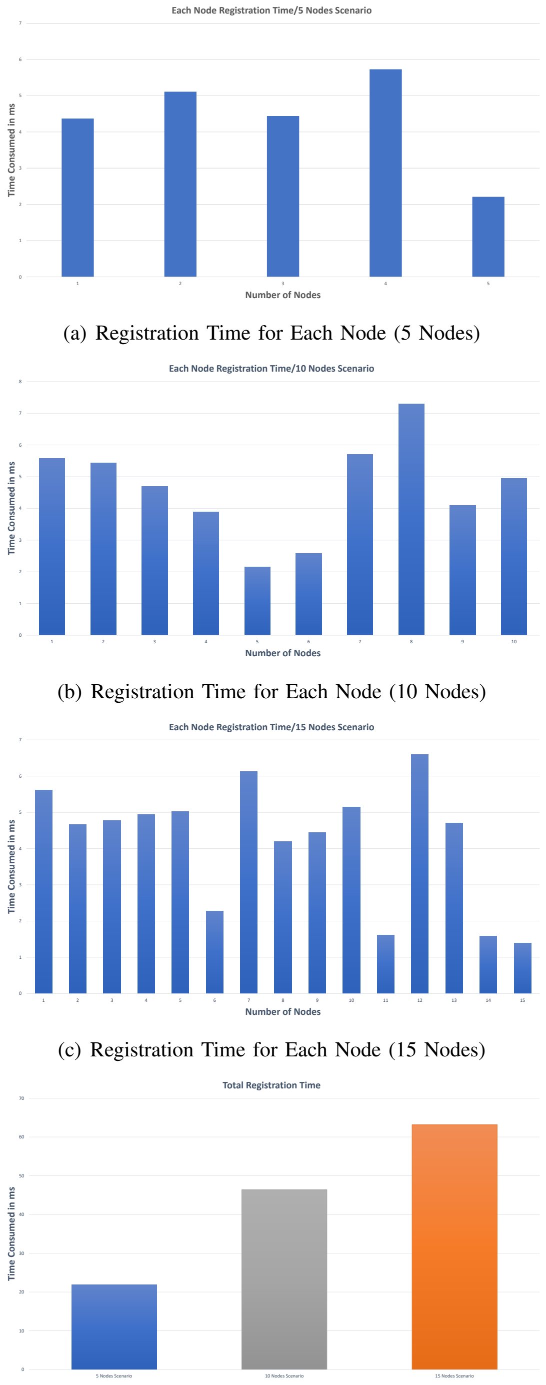


(a) NodeChain (Linked List of Virtual Nodes (Blocks))

(b) Traditional Blockchain's Block Versus NodeChain's Virtual Node (Block)

Fig. 2: NodeChain Linked List and Virtual Node Content Compared to Traditional Block

The structure used to create the UIDs for nodes is called NodeChain. NodeChain is a series of linked UIDs that have been generated using the target hash of extrinsic parameters and rehashed with the previous UID. With each update, and



(a) Registration Time for Each Node (5 Nodes)

(b) Registration Time for Each Node (10 Nodes)

(c) Registration Time for Each Node (15 Nodes)

(d) Total Registration Time for All Scenarios

Fig. 3: Registration Time

using this method, any changes happening to any node will be perceived by all nodes in the network and the BN can acts accordingly. Figure 2(a) presents the NodeChain linked list. Observing this structure, the similarity of the approach used to monitor the changes in UIDs to the blockchain is clear and has the same objective. NodeChain aims to secure hardware by monitoring the changes in UID using parameters extracted.

Requests are transactions broadcast by devices to the network and received by the BN to append the node to the NodeChain. Two transactions are generated. First, include the hash of extrinsic parameters. Second, the constructed public ID. The response is the block broadcast to the whole network as the virtual existence of the same node that includes the UID and the constructed public key. The response is only generated by BNs. Figure 2(a) illustrates the NodeChain, and the NodeChain block content compared to the traditional blockchain in Figure 2(b).

The UIDG function exists only in BNs. This function isused to generate the UID for each node. The UIDG includes two modules: the first one is the SCRYPT function [3], and the second is the SHA256 function. The extrinsic parameters and previous UID will be fed to the SHA256 module and the result will be fed to the SCRYPT function.

III. Experimental Results

The NodeChain has been built using Python and PostgreSQL. A P2P connection has been created between 5, 10, and 15 nodes, each of which has a Back up node (BN) initialized with the system.

The maximum time consumed to register each node in NodeChain takes approximately 5.7, 7.3, and 6.6 ms, respectively for 5, 10, and 15 nodes (Figure 3(a-c)). Although, each node's registration time was highest for 10 nodes, the total registration time for each scenario is 21.9, 46.4, and 63.1 ms. Observing the results, the number of nodes has a direct relationship with the time, (Figure 3(d)). The timing results are summarized in Table I.

TABLE I: Timing Analysis for NodeChain for All Scenarios.

Nodes—Time	Total Registration	Min	Max
5 Nodes	21.9	2.2	5.7
10 Nodes	46.4	2.2	7.3
15 Nodes	63.1	1.4	6.6

IV. Conclusions

Accessible Secure Identification is proposed to resolve the embedded-sensor devices security issues in CPS and IoT environment by generating a linked list of UIDs called NodeChain stored in a genesis blockchain in the post-blockchain structure Multi-Chain. The method experiments illustrated a fast registration time and high resistance against several attacks.

References

[1] 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.

[2] A. Alkhodair, S. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems," in *Proc. IEEE Computer Society Annual Sympo. on VLSI (ISVLSI)*, 2020, pp. 446–451.

[3] C. Percival, "Stronger key derivation via sequential memory-hard functions," Online, Tarsnap, 2012. [Online]. Available: https://www.tarsnap.com/scrypt.html, Last Accessed on 26 Feb 2021.