PUFchain: Hardware-Assisted Scalable Blockchain

Venkata P. Yanambaka
College of Science and Engineering
Central Michigan University, USA.
Email: yanam1v@cmich.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas, USA.
Email: saraju.mohanty@unt.edu

Elias Kougianos
Dept. of Electical Engineering
University of North Texas, USA.
Email: elias.kougianos@unt.edu

Deepak Puthal
School of Computing
Newcastle University, UK.
Email: Deepak.Puthal@newcastle.ac.uk

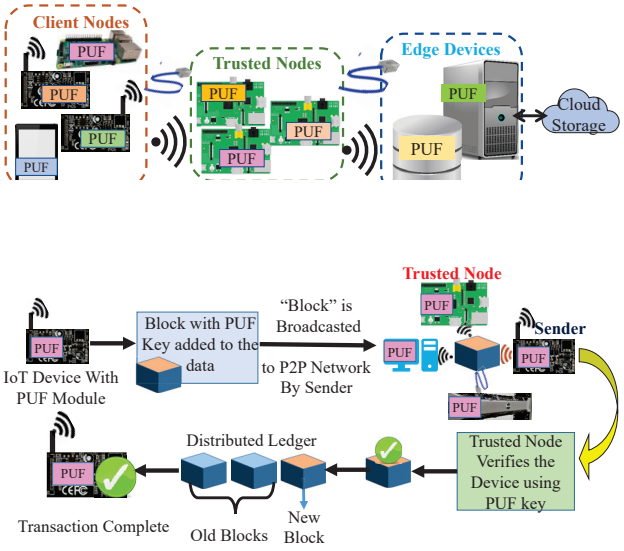
***Abstract*—This is an extended abstract for the research demo of a novel hardware-assisted scalable blockchain called PUFChain. This work presents a scalable energy-efficient private/permissioned blockchain (integrated with Physical Unclonable Functions or PUFs) which can be deployed in the IoT. PUFs have a multiple of roles in the blockchain: higher security, lower latency, and reduced energy consumption. Experimental validations of PUFChain show a transaction time of 198ms. *To the best of authors knowledge this is the first ever work that presents a comprehensive framework integrating PUFs in a blockchain*.**

I. Introduction

The blockchain uses a decentralized ledger, and in such an environment, all the nodes or participant a copy of the complete or partial ledger of transa since its beginning [1, 2]. The blockchain uses a tographic hash function for security and data int All participants agree upon a consensus algoritl validating the transactions. It was initially used fo cessing cryptocurrency transactions without the pr of a central entity [2]. Various blockchain con algorithms were proposed but require dedicated ha with high computational capabilities [3, 4]. This possible in the case of an IoT environment whicl ates on low power, resource-constrained devices. this work introduces PUFChain, a blockchain whi be deployed into an IoT environment.

II. The Proposed Hardware-Assisted Scalable Blockchain

The network of devices in PUFChain are categorized into "client nodes" and "trusted nodes". Client nodes collect the data using sensors and broadcast it to the network. Trusted nodes authenticate the devices sending the data and broadcast it back to the network. The block then gets added to the blockchain at the local storage of the nodes. PUFChain introduces a "PUF and Hashing Module" into every device in the network. Physical Unclonable Functions (PUFs) are used to generate a unique ID for each device and the hashing module performs a cryptographic hash on the data [5]. There are three phases in PUFChain: *Device Enrollment, Transaction Initiation,* and *Device Authentication.*



(b) PUFchain Working Model [7]

Fig. 1. The proposed PUF integrated blockchain - PUFchain.

A device in the PUFChain undergoes the "Device Enrollment Phase" only once until the devices' end-of-life. For every PUF module, a set of PUF challenges are selected such that they satisfy the properties of PUFs [5, 6]. These selected PUF keys are given as input to the module present in the new device and the corresponding response outputs are stored in a secure database. The devices then start collecting the environmental data, create blocks and broadcast them to the network as transactions.

A challenge input is selected and the corresponding response output is collected from the PUF. A hash of the sensor data, PUF key and the device ID is generated and broadcast into the network with the block. Once the broadcast block reaches the trusted node, the device ID, PUF challenge input and the hash are extracted from the block data. Using the device ID, the trusted node gets the response outputs from the secure database. The fetched response, device ID and the sensor data from the block are sent to the hashing module at the trusted node and a hash is computed. If the hash in the block and the generated hash match, the device is authenticated and the block gets broadcast to the network for the rest of the devices to add it to their local blockchains. If the hash does not match, the process is repeated for the rest of the keys present in the secure database with the device ID. If none of the hashes match, the block is discarded.

III. Experimental Validation

Fig. 2 shows the experimental setup for validation of PUFChain. The PUF and Hashing Module was developed on an FPGA. The Client and Trusted nodes are single board computers. The PUFChain blockchain was developed using the Node-RED development environment. The Client nodes and the Trusted node are connected to the General Purpose IO pins of the FPGA.

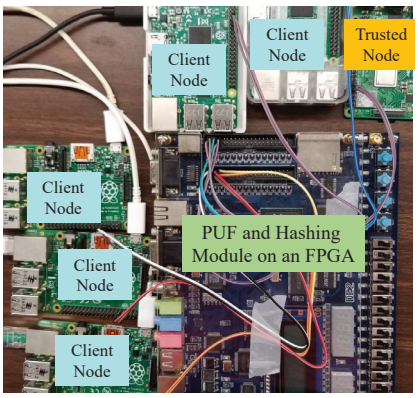


Fig. 2. Experimental Setup of PUFchain [7].

Table I shows the experimental results of PUFChain. ClearPi is the client node and BlackPi is considered a trusted node. With 500 unique keys generated from the PUF module, the uniqueness property of the PUF is 47% and the reliability of the keys is 1.25%. The uniqueness and reliability properties of PUF keys estimate the robustness of the keys generated. The time taken to complete a transaction with 5 client nodes and one trusted node is 198 ms.

TABLE I
Characteristics of PUFchain

Parameter	**PUFchain Value**
Blockchain Type	Permission Based
Mining	Authentication Based
Security primitive	Hashing and added PUF Key
Overhead	Device ID
Time taken to add the received block	
BlackPi	120.03ms
ClearPi (Raspberry Pi 3)	46.5ms
Time taken for a transaction	198ms
BlackPi Power Consumption	4.3W – 6.6W

IV. Conclusions

This work presents a blockchain called PUFChain which can be deployed in IoT environments. PUFChain uses PUFs and a hashing module for increased scalability and low power operations. Experimental evaluation shows the time taken for transactions is 198ms.

Acknowledgment

This is an extended abstract for a demo at the Research Demo Session of iSES 2019 based on our article [7].

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] 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.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Cryptography Mailing list*, 03 2009.

[3] H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks," *IEEE Access*, vol. 7, pp. 41 426–41 444, 2019.

[4] R. Henry, A. Herzberg, and A. Kate, "Blockchain Access Privacy: Challenges and Directions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 38–45, July 2018.

[5] V. P. Yanambaka and S. P. Mohanty and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security," *IEEE Trans. Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285–294, 2018.

[6] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," *IEEE Trans. Consumer Electronics*, 65(3), pp. 388–397, 2019.

[7] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)," *IEEE Consumer Electronics Mag.*, 2020, p. Accepted.