PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)

Saraju P. Mohanty
University of North Texas

Elias Kougianos
University of North Texas

Venkata P. Yanambaka
Central Michigan University

Deepak Puthal
Newcastle University

***Abstract*—This article presents the first-ever blockchain that can simultaneously handle device and data security, which is important for the emerging Internet-of-Everything (IoE). It presents a unique concept of blockchain that integrates hardware security primitives called physical unclonable functions (PUFs) to solve scalability, latency, and energy requirement challenges and is called PUFchain. This article also introduces a new consensus algorithm called "Proof of PUF-Enabled Authentication" (PoP) for deployment in PUFchain. PoP is 1000 times faster than the well-established proof-of-work (PoW) and 5 times faster than proof-of-authentication (PoAh).**

Electronic financial transactions helped grow E-commerce in leaps and bounds.[1] But in all E-commerce, a central entity was responsible for the financial transactions between the entities. This increased the chance of single point failure and the question of integrity always persisted. There is also the delay that is added to the transactions with the central entity

Digital Object Identifier 10.1109/MCE.2019.2953758
Date of current version 7 February 2020.

Published by the IEEE Consumer Electronics Society

presence.[1] Blockchain provides an answer to many issues. Every participant having a copy of the entire or partial ledger of transactions, makes the entire process transparent. Since its introduction in 2008, it has been explored for a variety of applications (See Figure 1 [1–4]).

The Internet of Things (IoT), a possible application of blockchain, is part of a bigger environment, the Internet-of-Everything (IoE). With the increased number of devices in IoE environments, the number of vulnerabilities increase at the same rate.[5–7] Every new device can potentially act as a different entry point for attackers. The blockchain uses cryptographic hash functions for maintaining consistency and security in the ledgers.[8] Various IoT devices are prone to attacks and data safeguarding has become a major issue. The blockchain can be a potential solution with an integration into IoT architectures.[8]

INTERNET OF EVERYTHING (IOE)—THE NEED FOR BOTH DEVICE AND DATA SECURITY

The IoT is the backbone for a variety of smart application domains, including smart cities, smart healthcare, and smart transportation. In essence "Instrumentation," "Interconnections," and "Intelligence," which are referred to as the 3Is of a smart city, are due to the IoT.[9] The IoE is a concept that has the IoT integrated as one of its components.[6] An edge layer is present as part of the IoT network helping in data processing before sending it to the cloud. With such environments appearing in most of the application domains, the use of devices with communication capabilities has seen new use cases. A new idea for the network of connected devices is making its way, the IoE.[6,7] There are four main components to an IoE environment (See Figure 2): (1) People; (2) Data; (3) Process; and (4) Things.

People, in an IoE environment, are part of the network of nodes. Traditionally, electronic devices, hand held or desktop helped the people connect to the Internet and have access to the world. But with the introduction of the IoE, innumerable new ways of communication are at the disposal of people. As an example, implantable medical devices (IMDs) that are inside a human

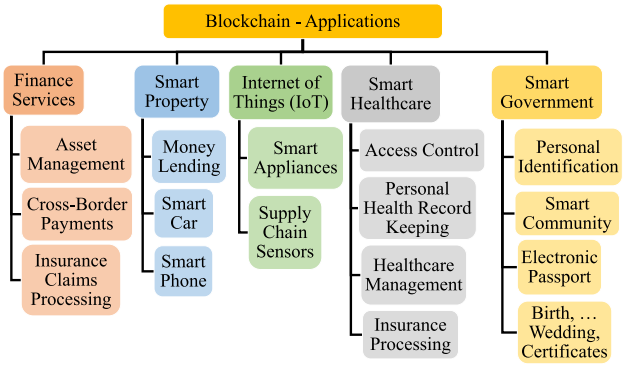


Figure 1. Possible applications of blockchain technology.[1]

body, such as a pacemaker, transmit the data to the server for doctors to diagnose. Similar are wearable medical devices (WMDs), which a person can wear on their body for various applications such as heart rate monitoring.[2] These are collectively called implantable and wearable medical devices (IWMDs).[10]

Data, in the case of the traditional IoT network, are transferred as is. With the introduction of an Edge layer added to the network, not all the data are transmitted to the destination. Data collection could be performed using various methods, such as crowd sourcing, involving people. Only the information that can be used for further analysis is sent to the cloud. The raw data are converted into useful information by the devices themselves or the edge layer. This processing of data into information in an IoE environment helps in making decisions more accurately at a faster rate. The data that are collected are leveraged for making intelligent decisions in various aspects of our day-to-day-life.[7,11]

Process helps in delivering the right data to the right place at the right time. This process is responsible for the flow of data through the network. An IoE network contains many entities, from people, to devices and cloud. The data that are collected by the devices from the environment or the people, has to be processed and information has to be extracted. This information from the raw data is transmitted to the cloud or for further processing or decision making.

Things are responsible for the data collection. Things have evolved in many categories. The devices have communication capabilities, wireless or wired and are capable of transmitting data collected from the environment.

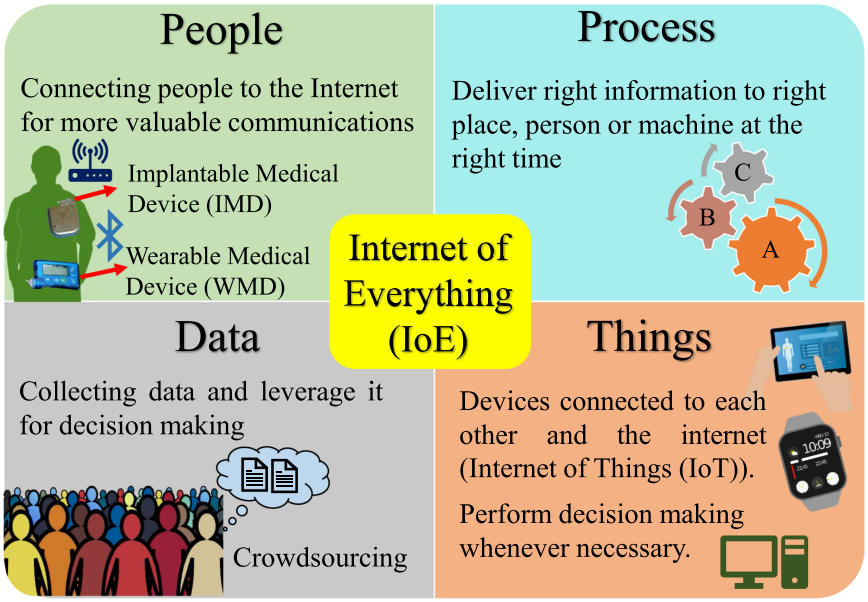


Figure 2. Vision of IoE with human-in-the-loop driving the need for security and privacy for device, person, location, and data.

CONTRIBUTIONS OF THIS ARTICLE

Problem Definition—Blockchain Bottlenecks

In an IoE environment, most of the "things" are low power and low performance devices. Various other characteristics of the devices, such as security and privacy, power consumption, and computational ability become bottlenecks when integrating a blockchain environment into the IoE. The blockchain has been computationally intensive since its introduction. So, there are some challenges that need to be dealt with before integrating it into IoE environments.

A Novel Solution: PUFChain

As a solution to these issues, a novel blockchain, called "PUFChain," which can be integrated into a resource constrained IoT environment is presented in this article. It uses physical unclonable functions (PUFs) for its enhanced security and scalability.[12] A PUF and Hashing module reduces the computational strain on the main processor, thus, making it ideal to be integrated into most scenarios. With ultralow power designs of the PUF, the power overhead can also be significantly reduced.

A Novel Consensus Algorithm: POP

For the integration of the blockchain into IoT architectures, a new consensus algorithm is proposed in this article, Proof of PUF-Enabled Authentication (PoP). A PUF and hashing module is used in the blockchain, and the unique keys generated by a PUF module present in the devices are used in the cryptographic hashing function. The keys generated by the PUF module act as a unique identifier for the respective device and raw keys are not transmitted over the network, which makes the algorithm more robust. the use of the PUF and hashing module also reduces the load on the main processor and reduces transaction times.

Modes of Operation of PUFchain

PUFChain can be operated in two configurations: (1) PUF mode and (2) PUFchain mode. As the name suggests, PUF mode utilizes only the PUF module present in the system for cryptographic purposes. The PUF keys can be utilized for various applications including the assignment of device IDs and for encryption of data stored locally or communication. The other configuration is the PUFChain mode, which uses the entire module, PUF, and hashing module and implements the blockchain in the network.

TYPES OF BLOCKCHAIN

Blockchain technology can be of various types (see Figure 3).[1] The blockchain uses the

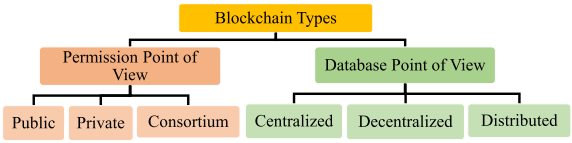


Figure 3. Different types of Blockchain.[1]

concept of a distributed ledger where the copy of the entire ledger, or a part of it, will be stored at the local storage of every node in the network. There is no central entity in the case of a blockchain network. The lack of central entity in the blockchain is replaced by a consensus algorithm.[1] All the participants in the network agree upon a consensus algorithm, a set of rules, required to validate the transactions. For a block of transactions to be validated and added to the blockchain, the "miners" in the network should run the consensus algorithm and validate the transactions.

Consensus algorithms follow different processes to generate and validate blocks. There are several important consensus algorithms (See Figure 4). We classify them into three groups: (1) validation based; (2) voting based; and (3) authentication based. Bitcoin uses proof-of-work (PoW), Etherium uses proof-of-stake and Link uses delegated proof-of-stake.[13–15] In the blockchain, multiple transactions form blocks, which are then validated and accepted according to the consensus algorithm. Once the blocks are validated, they are cryptographically connected to the blockchain. The consensus algorithm is the computationally intensive part of the blockchain.[13] Proof of authentication (PoAh) is a lightweight consensus algorithm developed for IoT architectures.[16] PoAh follows the cryptographic authentication mechanism for the mining process.

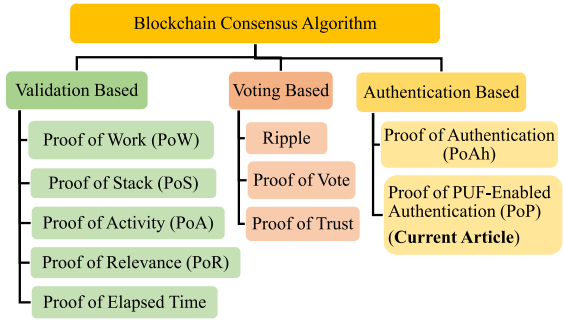


Figure 4. Various consensus algorithms used in the blockchain.

CHALLENGES OF BLOCKCHAIN

The blockchain faces many challenges (see Figure 5) despite of its many applications.[1, 17, 18] Once a block has been added to the blockchain, it can neither be edited nor deleted. If any data modification is performed on the blocks added to the blockchain, the entire ledger/chain is broken indicating a discrepancy.

The transactions in the blockchain are combined to form the blocks. Once the nodes in the network form blocks with the transactions, the process of mining starts, which validates the blocks and the transactions in it. The mining process requires high computational resources and dedicated hardware, which consume a high amount of power. The dedicated hardware requirements also make scalability difficult.[8,16,17] With an increased amount of data and nodes in the P2P network, latency also increases. As the number of transactions increases, the time taken to validate the transactions also increases and this gives rise to more issues. It also becomes more difficult to conceal the identity of the user in the case of a distributed ledger.[17] Observing the transactions, a user can be backtracked to their real-world identity. There are also the issues of attacks on the blockchain where fake blocks can be generated.

Overview of the Proposed PUFchain

This section presents the proposed architecture for PUFchain that we envision as a PUF-integrated secure blockchain, which can solve energy requirements, scalability, and latency requirements of the existing blockchain. A node in the PUFchain network consists of the IoT device and a

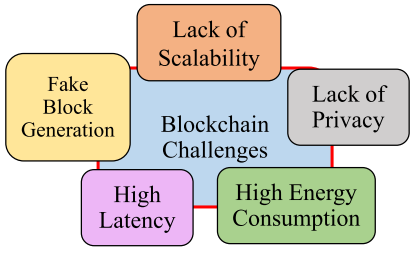


Figure 5. Challenges or issues of blockchain technology.

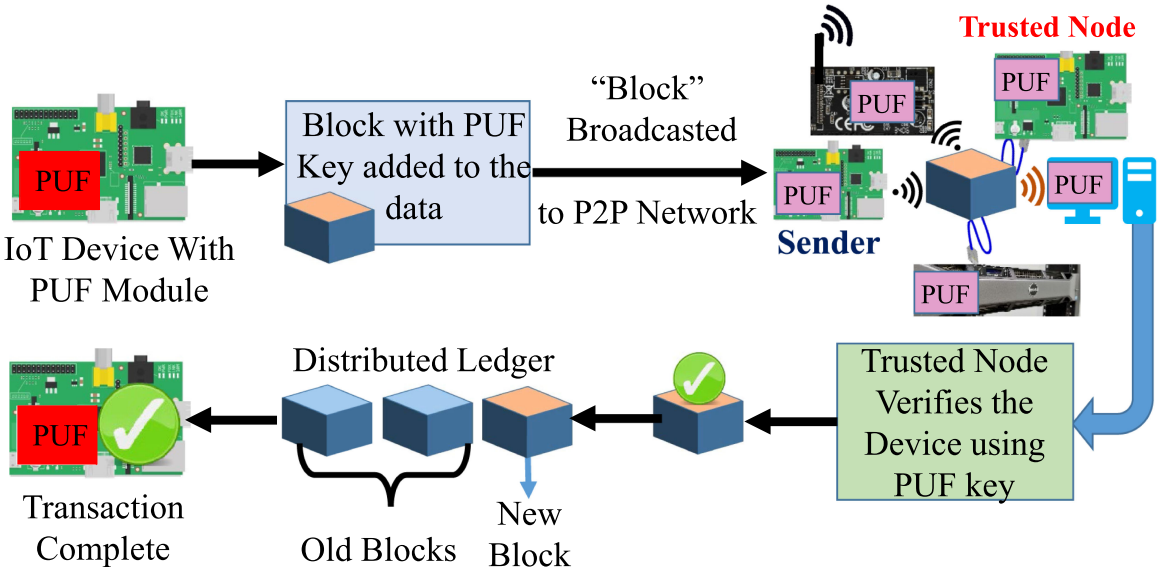


Figure 6. PUFchain working model.

hardware module, which has the PUF generating the key, and also the hashing capabilities (see Figure 6). The IoT device is responsible for gathering the environmental data. The PUF and hashing module is added to the IoT device. This reduces the computing burden on the IoT device itself. The specifications of the IoT device do not affect the security aspects or the performance of the PUFchain. The PUF and hashing module consists of a cryptographic processor and the PUF module. The cryptographic processor gets the data from the IoT device and the PUF module, which supplies the unique key. The cryptographic hashing function is performed in the cryptographic processor. Once the hash is computed, the IoT device transmits the data to the network.

Why and How PUF Integration in Blockchain?

The main intention of PUF chain is integration of the blockchain consensus algorithm in an IoT network, which has low power and low form factor presence. The PUFchain network consists of trusted nodes and the client nodes. Client nodes will collect the environmental data and broadcast it to the network. The trusted nodes are responsible for mining and validating the devices that collect the data. A PUF is responsible for generating a unique identity for the IoT device. A PUF can generate a series of unique keys that can only be generated from that PUF module. The output of the PUF key depends on the input and as the challenge input changes, the response from the PUF module also differs. The set of keys generated from a PUF module cannot be cloned or generated form any other module. Hence, the name physical unclonable function. The PUF keys are not stored in the memory of the IoT devices. When the keys are required, they will be generated from the module and the hashing is performed using the module. This makes the IoT device more secure as, depending on the PUF architecture, more than one key can be generated by changing the input. The output of the PUF key can be changed on-the-fly and various security threats can be avoided.

PROPOSED NOVEL POP

This section presents the novel PoP, a PUF-based blockchain consensus algorithm. The consensus algorithm is proposed to be implemented on an IoT network, which has energy and processing power constraints. In the case of PoP, the PUF module is responsible for generating the device's unique identification. The hash that is in the block is the cryptographic hash of all the previously considered data and also the PUF key that is uniquely generated at the PUF module of the device. The same key cannot be generated at any other device. The properties and working of the PUF module are

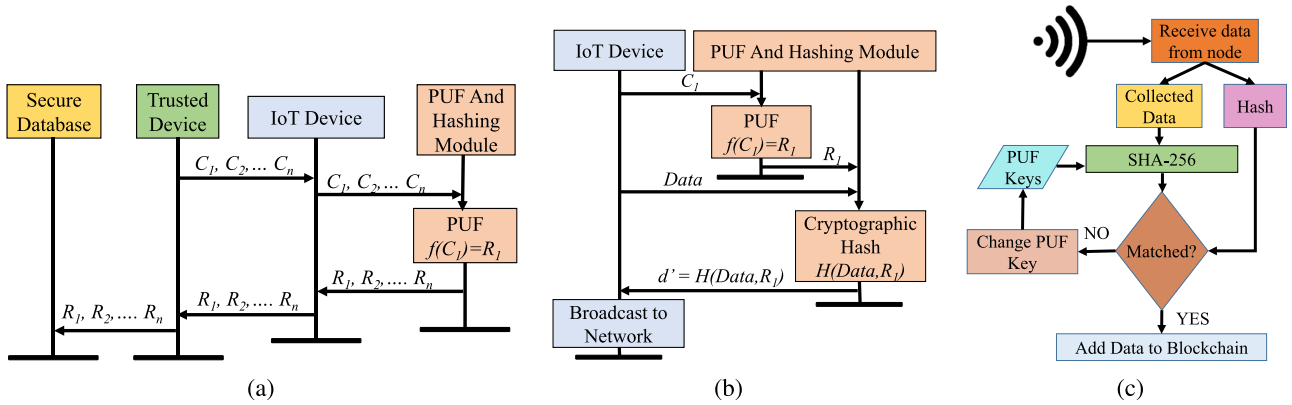


Figure 7. Enrollment and authentication steps in the proposed PoP consensus algorithm. (a) Device enrollment steps. (b) Transaction initiation steps. (c) Device authentication steps.

discussed in detail in the "Physical Unclonable Functions (PUF) as Hardware Security Primitive" section. The different steps involved in various phases of the proposed PoP consensus algorithm are shown in Figure 7.

Device Enrollment Phase

The network of devices using the PUF chain consensus algorithm is closed to any new devices that have not gone through the enrollment phase. Initially, a set of challenge inputs are selected for the PUF module in the new device and the corresponding responses are generated. The challenges should satisfy a set of requirements to be considered as inputs to the PUF. This set of requirements is discussed in the "Physical Unclonable Functions (PUF) as Hardware Security Primitive" section. The challenge-response pairs (CRPs) are stored in a secure database, access to which is granted only to the trusted nodes in the network.

Initiating a Transaction

Once the device is introduced into the network, data collection starts. The device collects the data and sends it to the PUF and hashing module present on the respective device. A challenge input, which is stored in the secure database, is given to the PUF and the response is generated. This response is added to the block of data and a hash is generated for the block. This block then gets broadcast to the network of devices in PUFchain.

Device Authentication Phase

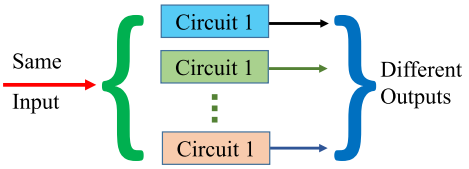
The trusted node listens to the message sent by the client and extracts the data and the hash from the block. The PUF keys for the corresponding device that broadcast the block are retrieved from the secure database. Each key is fed to the PUF and hashing module at the trusted node and a hash is computed for the data and added the PUF key. If the hash present in the block and the generated hash match, the device gets validated and the block is ready to be added to the blockchain. If the hashes do not match, the procedure is repeated for all the keys stored for the corresponding device. If none of the hashes match, the block gets discarded.

PUF AS A HARDWARE SECURITY PRIMITIVE

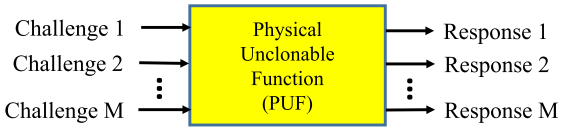
PUF is one of the key components in the PUFChain and PoP. A PUF brings out the nanoelectronic manufacturing variations from the devices on a silicon wafer. The outputs generated by PUF modules act as a fingerprint to the devices they are deployed.[19]

PUF Working Principle

Nanoelectronic manufacturing variations are introduced into the IC during fabrication process. Due to these, no two devices on an IC are identical geometrically. Hence, they are used as PUF modules. Figure 8 elaborates the working principle of PUF.[12,20] Input to a PUF module is called "challenge" and the output is called "response." The outputs generated by various



(a) Same Input Generates Different Outputs for Different PUFs



(b) Different Inputs Generate Different Outputs for a Specific PUF

Figure 8. Working principle of the PUF.[12]

circuits are compared with each other to generate cryptographic keys.

Figures-of-Merit (FOMS) of PUF

A set of properties including uniqueness, reliability, and randomness, has to be satisfied by the CRPs before they can be used for applications.[12] Uniqueness is the property to evaluate the uniqueness of the keys generated by the PUF design. A key once generated by a PUF design has to be unique to the respective module. Once the key is generated, the PUF module has to be reliable and should have the capability of generating the same key under various conditions such as power supply variations or aging effects. Both uniqueness and reliability are evaluated by checking the Hamming distance between the keys generated. Randomness is another key FoM. Once the key is generated, there has to be an equal number of 0s and 1s in it.

SPECIFIC CASE STUDY OF PUFCHAIN

Pufchain Security Verification

The PUFChain methodology is written in the Scyther simulation environment using the Security Protocol Description Language (.spdl).[21] The simulation is conducted in Scyther v1.1.3 in the Ubuntu 18.04.3 OS. According to the features of Scyther, we define the role of D and S, where S is the source of the block and D is the miner or authenticator node in the network. In the simulation, we have initialized all the features, as described in the model description. PUF random numbers are chosen randomly in this simulation. In our simulation, we have evaluated the scenario at the authenticated node (D) to find whether it authenticated the blocks thoroughly without any compromise.

Table 1. PUFchain case study platform.

PUFchain parameters	Specific values	
IoT Devices	Trusted node	Client node
	Raspberry Pi 3	Raspberry Pi 3
	Model B+	Model B,
		Raspberry Pi 1
Operating system	Raspbian 4.14	
Communication	Wireless	Wired and wireless
PUF and hashing module	Altera® DE-2	
Transaction completion time	192.3 ms	

Real-Life Testbed of PUFchain

The Node-RED development tool was used for designing the trusted node and the client nodes. The environment is more suited for development of IoT applications on multiple platforms, and hence, there is also a possibility of portability. The experimental setup consists of the Raspberry Pi single board computers and an Altera® DE2 FPGA module on which the PUF and the hashing module were developed. The characterization of the PUFchain is listed in Table 1. For evaluation of PoP and PUFChain, they were implemented on a testbed containing six Raspberry Pi single board computers of which one was a trusted node. For evaluating the performance across high performance and low performance devices, the nodes in the network are a combination of Raspberry Pi 1, Raspberry Pi 3 Model B, and Raspberry Pi 3 Model B+ boards. The prototype of PUFchain is shown in Figure 9.

Transaction Time Analysis of PUFchain

As listed in Table 1, the total time taken to complete a transaction is 192.3 ms. Table 2 presents the time taken by various devices to add the block that the device has received.

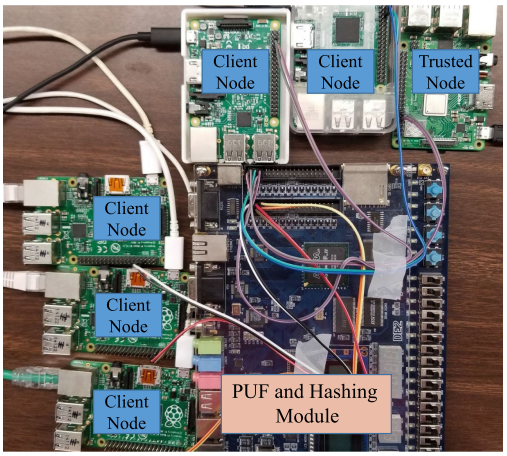


Figure 9. Prototype of the PUFchain.

Most of the processing has been offloaded to the PUF and Hashing module, which reduces the load on the IoT devices themselves. Hence, as shown in the table, the block can be added to the blockchain in 120.03 ms on a trusted node. The additional overhead added to the transaction completion time has been added by the communication between the devices in the network.

Comparative Perspectives of PUFchain

The well-established PoW, while running in high-performance computing resources has a latency in the order of 10 mins. PoAh, while running in limited computer resources has a latency in the order of 3 s. Thus, PoAh is at least 200 times faster than PoW, which is used in the traditional blockchain.[16] The proposed PoP algorithm is 5 times faster than PoAh. Thus, PoP is approximately 1000 times faster than the well-established PoW. Overall, it can be concluded that PoP is highly scalable for large datasets, which will run significantly faster, uses minimal resources, and has a minimal energy consumption footprint.

CONCLUSION

The blockchain has the potential to secure IoE environments and protect data privacy and security. But the integration of blockchain into IoE presents a challenge. The consensus algorithms used for achieving distributed device authentication or data validation traditionally were computationally intensive tasks. This article presents a new consensus algorithm, PoP and a novel blockchain architecture, PUFchain. As a future direction, an ultralow power design of PUF integration can be pursued as well as other consensus algorithms can be explored.

Table 2. Time taken to add a block to the blockchain once it is received.

Node	Mean (ms)	Standard Deviation (ms)
Raspberry Pi 1	72.27	18.07
Raspberry Pi 2	46.5	2.66
Raspberry Pi 3 (Trusted Node)	120.03	3.44

ACKNOWLEDGMENTS

The idea of this article is being demonstrated as a conference demo.[22] A significantly extended version[5] of this article has been archived.

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 Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.
2. H. Wu and C. Tsai, "Toward blockchains for healthcare systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consum. Electron. Mag*, vol. 7, no. 4, pp. 65–71, Jul. 2018.
3. F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gomez, and V. Santamaria, "Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 72–81, Jul. 2018.
4. N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by blockchain: Safeguarding internet of things devices," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 28–34, May 2019.
5. S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," Sep. 2019. [Online]. Available: https://arxiv.org/abs/1909.06496

6. A. Weissberger, "Qualcomm Keynote & IoT Track Overview," 2014. [Online]. Available: https://techblog.comsoc.org/2014/05/23/tiecon-2014-summary-part-1-qualc omm-keynote-iot-track-overview/
7. D. Evans, "The internet of everything: How more relevant and valuable connections will change the world," Cisco Internet Business Solutions Group, Cisco Systems Inc., San Jose, CA, USA, 2012.
8. 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.
9. S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, Jul. 2016.
10. M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.
11. R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things," IEEE Internet Initiative Online Document, 2015. [Online]. Available: https://iot.ieee.org/images/ files/pdf/IEEE_IoT_ Towards_ Definition_Internet_of_Things_Revision1_ 27MAY15.pdf
12. V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making use of manufacturing process variations: A dopingless transistor based-PUF for hardware-assisted security," *IEEE Trans. Semicond. Manuf.*, vol. 31, no. 2, pp. 285–294, May 2018.
13. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing List*, Mar. 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf
14. S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," 2019. [Online]. Available: https://decred.org/research/king2012.pdf. Accessed: Jun. 4, 2019.
15. K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with ethereum, swarm, and LoRa: The software solution to create high availability with minimal security risks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019.
16. 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 Int. Conf. Consum. Electron.*, Jan. 2019, pp. 1–5.
17. R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 38–45, Jul. 2018.
18. I. Paliokas, N. Tsoniotis, K. Votis, and D. Tzovaras, "A blockchain platform in connected medical-device environments: Trustworthy technology to guard against cyberthreats," *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 50–55, Jul. 2019.
19. 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. Consum. Electron.*, vol. 65, no. 3, pp. 388–397, Aug. 2019.
20. J. R. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud*, 2016, pp. 99–106.
21. "Scyther," 2019. [Online]. Availavble: https://people.cispa.io/cas.cremers/scyther/. Accessed: 2019.
22. V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PUFchain: Hardware-integrated scalable blockchain," in *Proc. IEEE Int. Symp. Smart Electron. Syst.*, 2019, pp. in Press.

Saraju P. Mohanty is currently a Professor with the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. Contact him at Saraju.Mohanty@unt.edu.

Venkata P. Yanambaka is currently an Assistant Professor with the College of Science and Engineering, Central Michigan University, Mount Pleasant, MI, USA. Contact him at yanam1v@cmich.edu.

Elias Kougianos is currently a Professor of electrical engineering with the University of North Texas, Denton, TX, USA. He is the corresponding author of this article. Contact him at elias.kougianos@unt.edu.

Deepak Puthal is currently a Lecturer with the School of Computing, Newcastle University, Newcastle upon Tyne, U.K. Contact him at deepak.puthal@newcastle.ac.uk.