A FPGA-Based PUF Integrated Blockchain to Overcome the Challenges of Internet of Everything (IoE)

Lukram Dhanachandra Singh and Preetisudha Meher

Abstract Today almost everything is upgrading into a smarter one, connecting them to the internet, which makes their data accessible to the network. Securing these data is the most important thing in the present day situation. Many researches have been proposing various solutions, PUF is one of them which is considered as hardware security primitives and on another side, blockchain technology is an advancing technology which is vigorously taken up by many applications such as financial applications for secure transactions, smart applications to secure the data by decentralizing them using some cryptography algorithm. But it is a bitter truth that the security issues do not end with them. It is high time for us to search for an alternate solution and to design a new better system that can bring these security issues to an end. So we proposed an FPGA based PUF to be implemented with Blockchain technology which can provide a better secure and reliable platform, which will be a decentralized platform consuming ultra-low-power and having efficient computational resources.

Keywords Blockchain technology · FPGA · Programmable unclonable function · Internet of things · Internet of everything

1 Introduction

The introduction of the Internet in commercial applications helps in the development of electronic commerce which encourages the financial trades among various entities [1]. A central entity takes all the responsibility to provide security both in communication and financial transaction among the different entities. And if any fraud or failure occurs, the central entity will be questioned and will remain responsible. In such centralized systems, at a single point of failure, it has a chance to cause

L. D. Singh (✉)
Electrical Engineering Department, National Institute of Technology, Manipur, India
e-mail: dhana.lukram0@gmail.com

P. Meher
Department of Electronics and Communication Engineering, National Institute of Technology, Tadepalligudem, Arunachal Pradesh, India

P. K. Mallick et al. (eds.), *Electronic Systems and Intelligent Computing*, Lecture Notes in Electrical Engineering 686, https://doi.org/10.1007/978-981-15-7031-5_6

a terrible system failure. Thus, a central entity has challenges of being trusted and issues of security and privacy. The central entity also has slow processing during the transaction process [2].

To solve the issues of the central entity discussed above, it needs to be decentralized and for the same, blockchain technology was introduced which practices a decentralized ledger, in which all the members in the network uphold a synchronized copy of the whole or partial ledger. A cryptocurrency called Bitcoin was introduced in 2008 which was a blockchain-based cryptocurrency [3]. Since then numerous researches have been taken on to practice blockchain technologies in various applications of finance services, Internet of Things (IoT), Smart Healthcare, Smart Governmental schemes, etc. Every transaction achieved among multiple entities are deposited in the distributed ledger and after all positive transaction, the ledger is synchronized among all the nodes in the network. Now not only the industry is using cryptocurrency, but also the healthcare, military, and many more are implementing this blockchain technology, as it excludes the need of a central entity, and also the problems discussed above.

The Internet-of-Things (IoT) is known to be the pillar for various smart application areas, comprising smart healthcare, smart cities and smart transport. The IoT is a network formed with the interconnection of devices, which communicate and exchange data among each other through the internet for smart resolution. But lately, a new concept of interconnecting such various IoTs as one component of its architecture and environment has been presented [4], called the Internet of Everything (IoE).

The IoE is consists of four components People, Data, Things and Processes. The Things in the IoE represent the devices that are associated with each other and the Internet exchanging data and decision making. People in the IoE come to be nodes inside the network. Countless devices belonging to the People are endlessly linked to the Internet and partake in performing communications among devices and other People. The remaining component is the Data which takes the role of information. The collected data is used for making intellectual choices in various phases of our daily life. Once the data is collected, transferring the correct data to the correct place at the accurate time is the Process in this IoE case. With every component of IoE, data collection, processing and security can aspect numerous potential threats. As an answer to all such problems, a FPGA based PUF integrated with Blockchain is considered and proposed.

2 Problem Definition

There is a common smash at the moment about the Internet of things (IoT) and its impact on almost everything we face in our day to day life from travelling to shopping and health. The IoT is a huge network that connects people and the things, all of which collect and share data about the way they are used. The collected data amount on the Internet of Everything rises every day.

The performance of devices used for these types of applications are low, which consumes less power, unable to deliver sufficient computational power for the architecture. To come up with all these concerns, researches are going on around the world which works on the development of solutions in which the computational requirements are unloaded to the edge of the network [5]. In such situations, the integration of edge datacenters assisted to remove the restrictions of resource-limited and low-performance devices [6].

2.1 Why Blockchain?

Privacy and security are two additional features of IoT architecture that require the highest consideration through the design level. Numbers of crypto graphical algorithms were suggested which can be used to reinforce the IoT security. But, IoT needs a central entity where all the data are stored and various devices or people communicated through; which is crucial if a cryptographic algorithm is used to secure the IoT architecture. Blockchain technology can be used to eliminate the necessity of a central entity from IoT architectures as the blockchain uses a decentralized public ledger for arranging the data and completing the transactions. As a copy of the ledger is shared with every node connected to the network, it helps to maintain consistency and security [1].

Blockchain technology is one among the emerging technologies worldwide which has the prospective to present it as a solution to several issues in multiple situations and everyday uses, such as the IoT.

In the blockchain, blocks are formed combining several transactions and nodes residing in the network produce blocks. All the blocks and their transactions should be authenticated by the identified node of the network as a portion of the consensus algorithm. Next to block confirmation, they are cryptographically linked with other blocks in the chain.

2.2 Why PUF Need to be Integrated into Blockchain?

Along with the advantages of blockchain, it also has some challenges which are essential to be solved prior to integration with any environment. More or less challenges require high computational resources, scalability, consumes more power, privacy and security. As an example, if we consider an IoT atmosphere, almost all these challenges are at the point of congestion for the integration of blockchain which comes up so fast and together at a time, which makes it hard to handle them quickly.

A Physically Unclonable Functions (PUF) is random functions which cause intrinsic properties of hardware to give unique response for a set of inputs (or challenges). A PUF is in charge of creating a unique key as an identity for the IoT device. A PUF can produce a sequence of unique keys that can only be generated from the same PUF module. The set of keys produced by a PUF module can neither be duplicated nor produced form any other module. The PUF keys are not to be store in the IoT devices memory. When it required the keys, the PUF module will generate it and is forwarded to the module used for hash, which increases the security of the IoT device based on the architecture of PUF, an additional key can be created by varying the input. The output of the PUF key can be altered during the progress and several security threats can be dodged.

3 Type of Blockchain and Its Challenges

Blockchain technology is of several types. It is elaborated in Fig. 1 [2]. Blockchain technology uses the idea of a distributed ledger in which the replica of the whole ledger or a portion of it were shared with every node in the network. Central entity is substituted by a consensus algorithm in case of a blockchain network [2]. Every member in the network approve on the consensus algorithm which is like rules essential to authenticate the transactions. For a block of transactions to be authorized and added to the blockchain, the miner in the network runs the consensus algorithm and confirm the transactions.

3.1 *Blockchain Technology Challenges*

The blockchain practices cryptographic hashes to uphold consistency and security. When a block is added to the blockchain, it cannot be changed or removed. If anyone tries to modify the data in the blocks linked with the blockchain, the entire ledger will be destroyed signifying an inconsistency. There are several challenges for blockchain [7]. Several challenges of blockchain technology that demands energy or computation power or prevent its application have found, such as, shortage of scalability, consumption of high energy, high latency, lack of privacy and fake block generation.

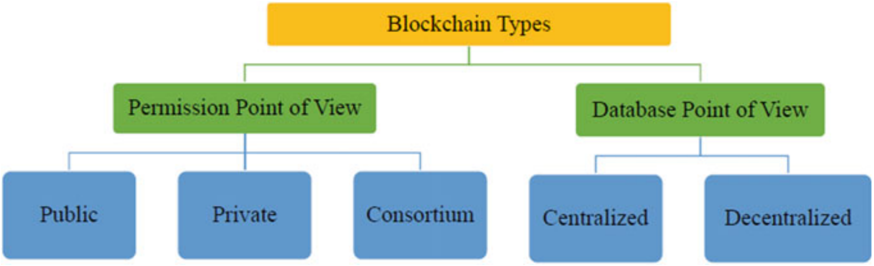


Fig. 1 Different types of blockchain [2]

Different transactions in the blockchain collectively form the blocks and when the block is formed at the nodes in the network, the process of mining begins which check and confirm the transactions in blocks and the blocks it selves. The process of mining needs higher computational power and dedicated hardware, consuming an enormous power. The scalability is also poor due to the needs of dedicated hardware. The latency also surges due to the rise in amount of data and nodes in the network. The time taken to authorize the transactions also surges with increases in the number of transactions which increases the issues too. There are also some issues where fake blocks can be made to attack the blockchain.

4 Review on Existing Consensus Algorithm

Consensus algorithms comprises various processes to create, check and confirm blocks. There are lots of key consensus algorithms, as shown in Fig. 2. We categorize them into three groups: (1) Validation based, (2) Voting based and (3) Authentication based.

Bitcoin practices Proof-of-Work (PoW) in which for consistent and secure transaction, it maintain miners inside the blockchain network and archive the same distributed ledger. In PoW algorithm, the participating nodes contest compared with each other to encrypt the new block into the prevailing chain [3]. New blocks are mandatory to be under a target value. It consumes a lot of resources; though provide security by determining the malicious nodes from inserting blocks into the blockchain. It verifies the new blocks depending on total computing power.

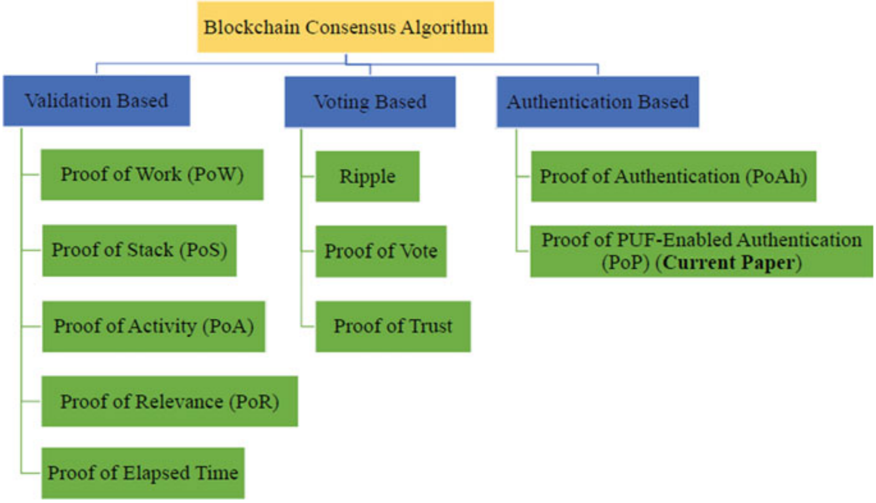


Fig. 2 Various consensus algorithms used in the blockchain

Etherium and Peercoin use Proof-of-Stake (PoS) which utilizes coinage (time for which the user held a particular currency) concept to determine the target value [8]. As in PoW, new blocks are mandatory to be under a target value but here it is determined individually. Higher the coinage is, it is easy for miner to find the solution. For every new solution provide by miner, a coinstake block that comprises a coin is referred back to the miner itself, which gives chance to miners [9].

The concept of PoW focused on rewarding the miners for validating the block, but it also increases the chances for them to win for on-line peers, but off-line peers cannot claim their reward as they are unable to sign their signature onto the blocks to claim the reward. Proof of Activity (PoA) was established to reduce the effect of these matters, whereby refining the security of the network [9].

Voting-based consensus algorithms consist of Ripple [10], Proof-of-Vote [11] and Proof-of-Trust [12].

Proof of Authentication (PoAh) implements an old-fashioned PoW consensus method for simple block confirmation [13]. The trusted nodes in the network act as miners which validate the blocks, trailed by authenticated nodes which drive the network peers to add block into the chain. This algorithm comprises two steps:

1. Validate the transactions in a block and respective sources, and
2. After positive validation, the corresponding trusted node's trust value is increased by one unit (Table 1).

Based on blocks from miners, the distributed ledger is shared to the network peers. Individual transactions in a block are confirmed by the trusted nodes in the networks. If it happens to be false identifications, after a certain number a trusted node will turn into normal node. The trust value of a respective trusted node is reduced by a unit for each false transaction.

However, for resource-limited IoT applications, any such consensus algorithm is not yet developed or tested. PoW and PoS are strong consensus algorithms and will not run in simple, battery-powered IoT devices.

Table 1 Comparison of different existing consensus algorithm

Consensus algorithm	Year	Types of blockchain used	Mining based on	Prone to attack
PoW [3]	2008	Permission less	Computation power	Bribe attack, Sibil attack
PoS [8]	2012	Permission less	Validation	DoS, Sibil
Ripple [10]	2014	Permissioned	Voting	DoS, Sibil
Proof of vote [11]	2017	Consortium	Voting	–
Proof of trust [12]	2018	Permission based	Probability and voting	DDoS
PoAh [13]	2019	Permission based	Authentication	–
PoP [14]	2019	Permission based	Authentication	–

Another consensus algorithm that is integrated with PUF termed as Proof of PUF enabled Authentication was proposed recently, which was permission-based blockchain and its mining was based on Authentication [14].

5 Physical Unclonable Functions (PUF) as Hardware Security Primitive

PUF was specially introduced for hardware security [15] as a random function which led to manufacturing variations in chip levels from the devices on the Integrated Circuit (IC). It introduces variations during the IC fabrication process which are random, inescapable, and uncontrollable and automatic. Due to these Nano-electronic manufacturing dissimilarities, none of the devices on a wafer are the same. The input challenge and its resultant response obtained from PUF circuit are termed as Challenge Response Pair (CRP). For evaluation of PUFs, three main figures of merit are measured as Uniqueness, Reliability, and Randomness, due to which PUF is considered as a hardware security primitives.

PUF can be categorized as Silicon PUFs and Non-Silicon PUFs based on fabrication and it is also classified as Strong, Controlled and Weak PUFs based on security-based. Many researches have been going on for efficient PUF designs according to their targets. Some of them are for Intellectual Property protection, anti-counterfeiting, test and debug security, device authentication, and key generation. And some are for implementing machine learning algorithm in it to provide more security and some researchers also seek to merge it in FPGA for low power consumption, to improve processing speed and also for size reduction [1]. Many review papers are also published on different architectures of PUF, like MUX based PUF, SRAM PUF, Butterfly PUF, Arbiter PUF, Ring Oscillator PUF and hybrid PUF which is a combination of two or more PUFs.

6 Contribution of the Paper

6.1 PUF Integrated Blockchain–PUFchain

The main target is to integrate the consensus algorithm for blockchain in IoE network which has a short form factor and less power for better security and data management. Figure 3 displays the structure of nodes in PUFchain. The network consist is client nodes that gather environmental data from devices and upload them to the network and trusted nodes that are accountable for mining and validation of devices collecting the data.

A high level of security can be attained with the integration of blockchain to the network. A hybrid oscillator arbiter PUF was used to implement a PUFchain [14]. A

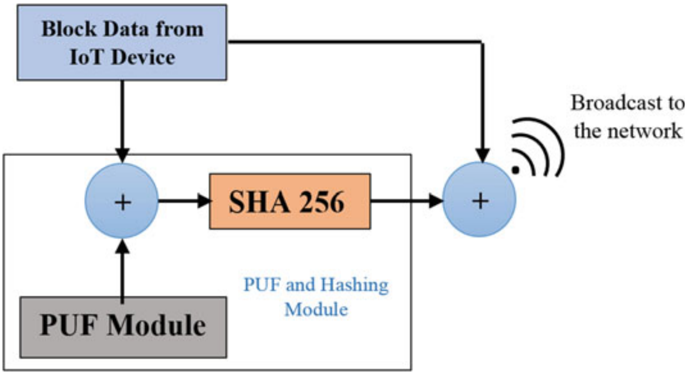


Fig. 3 Structure of nodes in PUFchain

Hashing module and PUF module is employed above the IoT device that improves the computation of cryptographic hashes. Addition of PUF module for unique key generation and cryptographic hash computation lessens the computational needs of the IoT devices. By selecting FPGA based PUF designs, FPGA based hashing module and optimization, we can significantly reduce the power consumption; improve security, scalability and latency of the blockchain. Figure 4 presents the architecture of the PUF-integrated blockchain.

The PUF and module used for hash consist of a cryptographic processor build up on FPGA and the FPGA based PUF module. The cryptographic processor collects the data from the IoT device and the PUF module supply the unique identification key. A sequence of transactions was commenced, authenticated and inserted to the blockchain which authorizes the consensus algorithm. Figure 5 shows the block structure of PUF integrated blockchain.

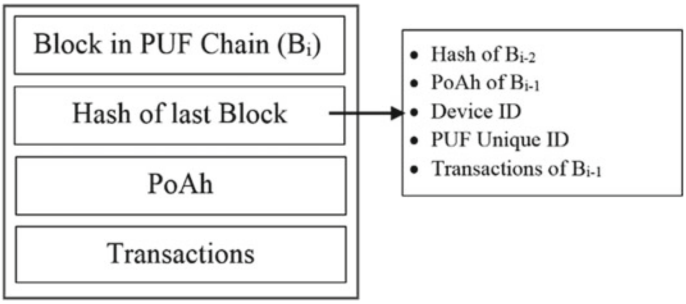


Fig. 4 Block structure of PUF integrated blockchain

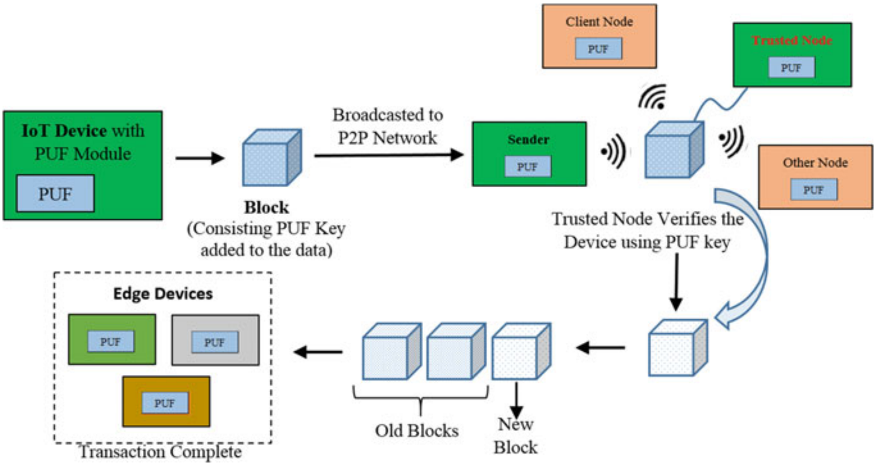

Client Node
PUF
Trusted Node
PUF
IoT Device with PUF Module
PUF
Broadcasted to P2P Network
Sender
PUF
Other Node
PUF
Block
(Consisting PUF Key added to the data)
Trusted Node Verifies the Device using PUF key
Edge Devices
PUF
PUF
PUF
Transaction Complete
Old Blocks
New Block

Fig. 5 Architecture of PUF-chain

6.2 Consensus Algorithm for PUF Integrated Blockchain

There are three phases in designing a consensus algorithm. First one is the device enrollment phase (E phase) in which it checks the IoT Device at the node if it can be selected or enrolled for PUF chain consensus algorithm. This can be achieved with PUF module. All the IoT devices in the PUF chain network should comprises PUF module to produce a unique identification key which is used later for authentication. So, in this E phase, a set of challenge inputs will be selected for PUF module and these challenges should satisfy a set of requirements to be considered as inputs to PUF [14]. And thus the corresponding CRPs are stored in a secured database which can be accessed later by trusted nodes. As soon as the IoT device is positively registered into the network, it is qualified for the initiation of transactions which will be authenticated by trusted nodes.

Second phase is the initiation of transaction (T phase) which will be generated after collection of data from the sensor device. The transaction data will consist of the collected sensor data and the device's MAC address. The MAC address works as identification for the remaining nodes in the network including trusted nodes. Just after the transaction is processed, hardware accelerator will receive it. It consists of the PUF which is proficient to compute the cryptographic hash. A challenge input (Ci) is chosen for the PUF which is one among the challenges saved in the secure database which can be accessed by the trusted nodes. The challenge is passed to the PUF module and it will collect the response. Then the data linked with the generated response are computed for hashing by the hardware accelerator. And it is directed reverse to the IoT device which further broadcast it to the network.

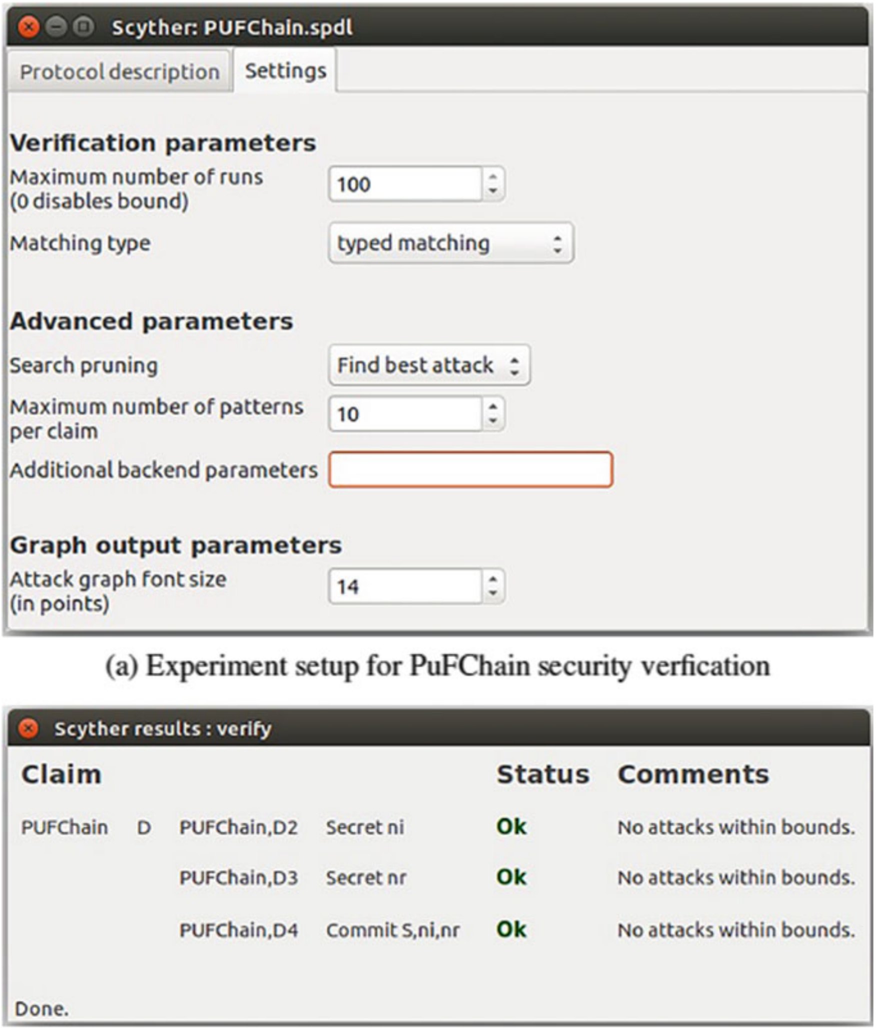
And the last phase is Authentication phase (A phase), which authenticates the block which is not broadcast to the network before adding to the blockchain. Just after trusted nodes received the block, the data (D_n which consists of the data collected by the node along with its MAC address) and the hash (H_n) are recovered which help of identification of the device. The trusted node obtained the PUF keys from the secure database with the help of the MAC address and it is sent along with the data to the hardware accelerator to perform the hashing part. The function used for hashing by the devices throughout the network should be the same. The resultant hash is checked for matching with the Hn received from the node. If both the hashes found to be a match, the device is authenticated and the block is added to the blockchain and it is broadcasted to the network. If they are found not to be matched with each other, the process carries on with all the PUF keys that are saved in the E phase. And if it cannot authenticate the device, the block will be released and not broadcast.

6.3 Evaluation and Analysis of Result

We can evaluate/analyses the result for the proposed PUF-chain using both software and hardware platform. We can develop a hardware accelerator containing PUF module and hashing module on an FPGA and we can use Raspberry Pi module as nodes as done in [14]. The consensus algorithm can be written in the Scyther simulator which is an automatic verification tool of security protocols. In this, we need to write the code in Security Protocol Description Language (.spdl), simulation can be done in Scyther v1.1.3 with a system running with Ubuntu 18.04.3 or higher version OS. The result can be checked as shown in Fig. 6 [14]. We can also perform analysis the transaction time and power consumption for the PUFChain. Table 2 gives the comparison of two existing consensus algorithms, i.e. PoAh [13] and PUFchain [14].

7 Conclusion and Future Directions

In this paper, we elaborate the steps in various phases of consensus algorithm which are required to authenticate the nodes in an FPGA-based PUF integrated blockchain network, providing better security, scalability, and reliability to and enhancing computational power of IoTs/IoE. We also promoted the ways to analyses the proposed PUF integrated Blockchain module. Some results of the existing consensus algorithm are also shown. We can implement SHA-256 on FPGA using blockchain concept as mentioned in [1] for hashing module we can provide far better security. And if we can implement the proposed consensus algorithm with machine learning then its security will be very strong that it takes years to have a breakdown of the barrier in the system.



Verification parameters

Maximum number of runs (0 disables bound): 100

Matching type: typed matching

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 14

(a) Experiment setup for PuFChain security verfication

Claim				Status	Comments
PUFChain	D	PUFChain,D2	Secret ni	Ok	No attacks within bounds.
		PUFChain,D3	Secret nr	Ok	No attacks within bounds.
		PUFChain,D4	Commit S,ni,nr	Ok	No attacks within bounds.

Done.

(b) Seecurity verfication results

Fig. 6 PUFchain security verification using Scyther

Table 2 Comparison of PoAh based blockchain and PUFchain

Parameter	PoAh based blockchain	PUFchain
Blockchain type	Permission based	Permission based
Mining	Authentication based	Authentication based
Security primitive	Hashing	Hashing and added PUF key
Over head	Device ID	Device ID
Hardware needed	IoT device capable of performing hashing	IoT device
Time taken to add received the block (ms)		
BlockPi	843	120.3
Clear Pi (Raspberry Pi 3)	85	46.5
Clear Pi (Raspberry Pi 1)	162.4	120.3
Time taken for a complete transaction	950	198
Power consumption range		
BlockPi	3.1 W|3.6 W	4.3 W|6.6 W
Clear Pi (Raspberry Pi 3)	2.1 W|2.5 W	3.3 W|5.6 W
Clear Pi (Raspberry Pi 1)	1.5 W|1.8 W	2.7 W|5 W

References

1. Singh LD, Meher P (2019) Advancement of blockchain security solution with FPGA. Int J Adv Sci Technol 28(3):276–283 (Elsevier)
2. Puthal D, Malik N, Mohanty SP, Kougianos E, Das G (2018) Everything you wanted to know about the blockchain: its promise, components, processes, and problems. IEEE Consum Electron Mag 7(4):6–14
3. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. Cryptography Mailing List 03
4. Miraz MH, Ali M, Excell PS, Picking R (2015) A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In: Proceedings of internet technologies and applications (ITA), Sept 2015, pp 219–224
5. Stanciu A (2017) Blockchain based distributed control system for edge computing. In: Proceedings of 21st international conference on control systems and computer science (CSCS), May 2017, pp 667–671
6. Wright K, Martinez M, Chadha U, Krishnamachari B (2018) SmartEdge: a smart contract for edge computing. In: Proceedings of IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber,

physical and social computing (CPSCom) and IEEE smart data (SmartData), July 2018, pp 1685–1690

7. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of IEEE international congress on big data (BigData Congress), June 2017, pp 557–564
8. King S, Nadal S (2012) PPCoin: peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf. Last accessed on 17 May 2019
9. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun Surv Tutor 18(3):2084–2123
10. Schwartz D, Youngs N, Britto A (2014) The ripple protocol consensus algorithm. In: Ripple Labs Inc white paper, vol 5
11. Li K, Li H, Hou H, Li K, Chen Y (2017) Proof of vote: a high-performance consensus protocol based on vote mechanism & consortium blockchain. In: Proceedings of the IEEE 19th international conference on high performance computing and communications; IEEE 15th international conference on smart city; IEEE 3rd international conference on data science and systems (HPCC/SmartCity/DSS), pp 466–473
12. Zou J, Ye B, Qu L, Wang Y, Orgun MA, Li L (2018) A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. IEEE Trans Serv Comput 1–14
13. Puthal D, Mohanty SP, Nanda P, Kougianos E, Das G (2019) Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In: Proceedings of IEEE international conference on consumer electronics (ICCE), Jan 2019, pp 1–5
14. Mohanty SP, Yanambaka VP, Kougianos E, Puthal D (2019) PUFchain: Hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of Everything (IoE), Sept 2019. https://arxiv.org/1909.06496.pdf
15. Pappu R, Recht B, Taylor J, Gershenfeld N (2002) Physical one-way functions. Sci J 297(5589):2026–2030