International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Lightweight Blockchain to Improve Security and Privacy in Smarthome

D.M Sheeba, S. Jayalakshmi

Abstract - Internet of Things (IoT) growing at a rate of exponential numbers in recent years has received extensive attention with BlockChain (BC) technology which provide trust to IoT with its immutable nature, decentralization in computing, resource constraints, security and privacy. The distributed ledger of transactions in BC is path leading technology for addressing Cyber Threats in the form of data theft; it provides secure application architecture which has proven track of record for securing data. IoT devices using BC enabled to communicate between objects, share data, decide based on business criteria and act as a medium to securely transmit information. This work provides lightweight BlockChain with two prominent consensus mechanism PoW – Proof of Work and PoS – Proof of Stake for smart IoT devices. Next, Smart Home Device (SMD) is ensures providing best-in-class Security and Privacy for smart home Appliances. Further provides future advances in the Approach.

Keywords – Blockchain, Decentralization, Consensus Mechanism, Smart Home Device, Security and Privacy.

I. INTRODUCTION

Blockchain (BC) mechanisms are proven in financial area and crypto currency in recent years; it has been recognized by leading Companies, Governments and end-users for its security and privacy. IoT on other hand needs a proven mechanism for ensuring privacy and security in data transmission, storage and presentation; this makes BC as a natural partner for utilizing the power of BC in recent IoT solutions.

Decentralized nature of BC helps IoT devices to have multiple copies of same data in digital ledgers as same versions; any alteration to original content cannot be done without permission of all other blocks/nodes. This makes IoT data immutable and secure since without permission of all blocks content cannot be changed.

Hence adoption of BC in IoT Architectures is inevitable wherever Security and Privacy are essential; the real-time examples of BitCoins, Crypto-Currency and Governments transaction ledger maintenance are evident. While arguing for BC in IoT Architectures

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
D.M. Sheeba*, Dept of Computer Science, New Prince Shri Bhavani Arts & Science College, Chennai, India.
S. Jayalakshmi, Dept of Computer Applications, VISTAS, Chennai, India.

, it has few pitfalls in terms of high computational cost, bandwidth usage, energy requirements and block minting delays. So BC cannot be accommodated in all IoT devices and necessitates need of a lightweight BC [1].

Lightweight BC provides mechanisms to retain security and privacy by providing low cost computation, less bandwidth usage in IoT devices and providing additional Block Manager to handle the minting delays. Also centralized digital transactions ledger enables IoT devices to share payload with high computation devices in SmartHome. SmartHome manager enables IoT devices to share data publically in secure environment.

This work demonstrates effective use of lightweight BC in SmartHome and how it is going to improve security, privacy in IoT devices. Also utilizes widely used cryptographic puzzles PoW – Proof of Work, PoS – Proof of Stake to mine new blocks of IoT data.

A. Decentralization

Decentralized way of record keeping in Digital Ledger used in BC in order to ensure data privacy, this ensures no record is altered without knowledge of another nodes / blocks in the chain. Fig 1 shows decentralization of blocks in BC.

To maintain consistency and timestamps of blocks, BC utilizes consensus methods like PoS, POW mechanisms [2]. Recent IoT devices are broadly categorized as centralized nodes and each device authenticated and enabled in IoT network. So decentralization of devices enhances the end-to-end communication via peers and ensures security.

- **Efficiency**

The efficiency of the system can be improved by its participating nodes in the blocks, resources, decentralized architecture of Blockchain and the Distributed Timestamp Ledger. The efficiency can also be improved by the reduction of resources in various aspects [3].

- **Deployment and Maintenance**

In a centralized IoT environment, infrastructure, server storage and network maintenance cost will be high and it makes IoT solutions expensive, it is going to impact the IoT solutions negatively. BC helps in decentralized most of the operations and storage facilities which helps in reduction of cost and also improving security [4]. Huge data transmission using encryption and transformation costs reduced by the way of decentralization and overall deployment cost reduces. This improves high utilization of IoT solutions.

- **Reliability**

Reliability of IoT devices always important aspect since it replaces manual effort of monitoring;

deciding based on critical data elements, the sole purpose of bringing in IoT is compromised if reliability is not ensured [5]. To bring more reliability on the IoT solutions, decentralized BC can bridge the gap of failure in centralized networks.

Data is available at multiple points and easily accessible though few nodes unavailable due to interruption in network. Also authentication is always ensured minted blocks and hash keys, so physical availability of nodes are not 100% required [6].

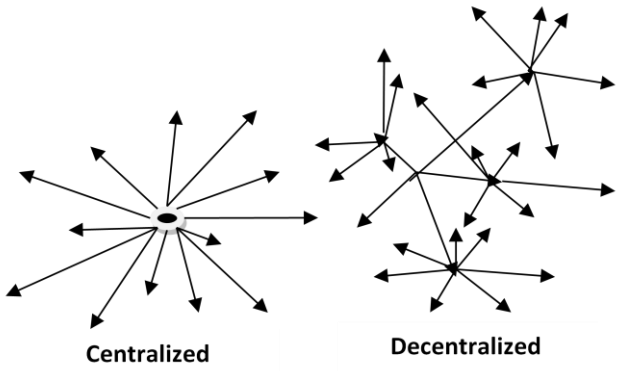

Fig 1. Centralized and decentralized BC

- **Security and privacy**

IoT security is complex since its resource constraints and multiple device connectivity. Large scale network and less standardization cause the security issues [7]. BC can provide the standard way of authentication, data storage, retrieval and authentication. Conventional methods always utilize the audit trails in the form of user data, authentication and actual business values. This again increases the network bandwidth and possible causes privacy issues.

Privacy issues in IoT eliminated through peer to peer authentication of each node and also data validated against the hashes stored in previous minted data. This provides double authentication of user security and privacy [8].

- **Scalability**

IoT networks contain very large number of devices in BC, Enabling the scalability of devices without compromising performance, Security and data privacy is a challenging task [9]. The BlockChain scalability issue related to many aspects, such as Data Control, Automated bootstrap, micro services architecture for faster connectivity [10]. BC provides ability to scale up the system with privacy and security in the form of peer to peer authentication and data storage.

B. Transaction Throughput

Blockchain Bitcoin can process 7 transactions per second (tps) since there is a restriction of block size, time interval, whereas Ethereum can process at the rate of 25 tps [11]. Similarly VISA at the rate of 2000 and Twitter at 5000 tps respectively [12]. Millions of devices connected through IoT and requires a better throughput to communicate with high throughput.

C. Transaction Latency

In Bitcoin mechanism, to mine a block it takes 10 minutes in order to ensure security of whole network; this is to eliminate attacks like double spending. To confirm and add a transaction to a block in BC, it takes 6 blocks mining time, only after this block is recommended to be added [13]. Few high critical transactions require more than 6 blocks like 10 or 15 based on nature of transaction.

D. Network Bandwidth

In Blockchain, All transactions, confirmed blocks to be broadcasted across whole network, this confirmation mechanism will occupy huge network bandwidth and undesirable for IoT devices where network bandwidth usually limited [14].

E. Storage

Blockchain Architecture is a distributed storage databases; each node will have a separate storage to validate data integrity and ensure the transaction shared by other nodes. Whereas IoT devices are not always equipped with high storage, when transactions per day or week increase, need for huge storage is essential and it's certainly not in capability of IoT [15].

II. BUILDING TRUST WITH BLOCKCHAIN

Building a trust using Blockchain enhances trust among business networks [16]. The key attribute of IoT devices are limited processing power and their purpose is to supply data to physical objects. The heavy processing requirements may use more battery power which can able to harm the operation of IoT. BC builds its trust through the following three attributes

A. Distributed BC

For every shared and updated transaction between the nodes connected in the Blockchain the distributed immutable ledger can be used [15]. Central server not utilized to manage the data and all this is done in real-time scenario. The important feature is that all the authorization is done via Permissions or Cryptography and this ensures security over distributed BC [17].

B. Transparent

This can be said transparent because each node and participant in BC has individual copy of Block data and its hash. Each node has access to transactions happened during block mining [18]. Moreover they themselves can verify the identities and validators without any need for mediators.

C. Consensus-based Algorithms

It define that all relevant network participants must agree that until or unless all the transaction is valid. This is done only through the use of consensus algorithms [19].

III. LIGHTWEIGHT BLOCKCHAIN AND IOT

A. Hash function and Encryption

Transactions and each resource in network are available ensuring security through digital signature or keys. Public key cryptography used to encrypt and decrypt messages [20]. Public key and Private keys are generated where public key shared across users but the private key is secret key and only owner can access it.

Message transmitted requires both public and private key to decrypt and validate the signature before considering it to be valid transaction. Hash function defined is the mathematical function which can take input and generate encrypted data and its fingerprint. Functions are applied to input data and it will process then finally will generate unique output [21]. Major advantage of the Hash produced is to validate data integrity and ensure data in not tampered in between. Also always hash size to be same irrespective of the input data [22]. Few Examples are SHA-256 [23] and RIPEMD160 [24].

Encryption through hashing helps the data to be protected from intruders by changing the valid data to transformed version, so that no one can understand or decrypt without the original keys used to transform data. The mathematical function used for changing the values randomly depends on key size and permutation and combination of transformation within the system. These functions are irreversible and can only be decrypted again by a function.

B. Peer-To-Peer Network (P2P)

It's familiar that Blockchain network has been generated to be a decentralized consensus network and hence no need of entrusting the third party. In a smart home connection nodes use two transaction namely successful connections established and summary of the established connection. There can be 2 way connection, Inbound where data requested and outbound where data provided. Each of the connection named as T_Max and T_Min. T_Max can keep track of 64 established addresses [29]. Address selected by node count and its randomized value sk

Count = Hash (sk , group , hash (sk, input ip)%4) % 64 (1)

Group defined as 16 IP address prefix. New block IP address of the overlay added to the count whenever new connection established [25]. Block Manager calls hash function to generate new block whenever existing blocks are filled and no space for new entry [26].

IV. CONSENSUS MECHANISMS

A. PoW - Proof of work

To avoid cyberattacks proof of work (PoW) effectively used. Here in order to allow anyone to change or add any block to chain, Member has to solve a cryptographic puzzle and show that, node is eligible to participate in block chain.

This comes with cost of solving the puzzle in terms of Computational requirements and power consumption [27]. Examples Bitcoin computational difficulty is about 17.26T. Work is on the following activities; one, PoW should be computationally complex and demanding but solvable.

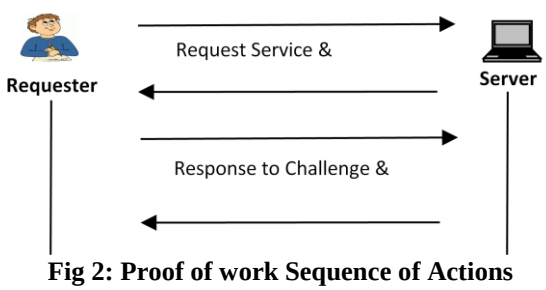

Fig 2: Proof of work Sequence of Actions

Second, actual verification and validation of the computational work to be easily verifiable; when first minor decrypt the problem, minor will be rewarded with reward coin. After all above validation block is added to the BlockChain. Actual work is as follows, nonce – an arbitrary number added to message and hash function to encrypt the message. This is repeated until answer to the problem is arrived. Bitcoin uses SHA-256 hash algorithm.

PoW difficulty as in BitCoin 17.26T adjusted for every k blocks and average time taken is limited to 10 minutes [28]. PoW is on the guidelines on no minor should hold more than 50 % of block chains processing power since it leads to controlling and changing the chain.

B. PoS - Proof of stake

Proof of Stake brought up as an alternate to PoW, where it consumes more computational resources and power. PoS categorized as public BC consensus mechanism and it involves selecting a particular node as validator based on their Economic stake in the Blockchain.

PoS uses distributed way of mining call Forge, Node ios randomly selected as the % of stake is more, this might create a problem of majority owner takes up Forging. Yes Its true but minors get reward points to how much they mine and also loose the coins if the approve the invalid transactions. So PoS requires less than PoW energy requirement since it's based on ownership of state in Blockchain and anyone can be selected as validator instead of computational puzzle [29].

Many stake based consensus algorithms followed, Example Chain-based proof of stake selects validator node randomly in a selected timeframe of 10 seconds for creating a block and it should point to any previous blocks [30].

The following table represents the various consensus algorithm comparisons, usage and energy consumption.

Table I. Comparison of consensus algorithm

Types of consensus algorithms	Blockchain Type	Peer network Scalability	Power Consumption
PoW - Work	Open	High	No
PoS – Stake	Open	High	Partial
PBFT	Permissioned	Low	Yes
DPOS	Open	Low	Partial
Ripple	Open	High	Yes
Tendermint	Permissioned	Low	Yes

C. PoA-Proof of Activity

The PoA(Proof of Activity) method rewards for sustaining the network to the participating stakeholders. Advantages over PoS are where it punish non-active stakeholder. i.e It uses both PoW and PoS to validate and add blocks to chain. Initially PoW is used to create a new block and then changes to PoS to add new transactions to the block.

Using this approach both block minor and validator equitably rewarded. Based on the stake a minor has in BC, selected for signing the block and ensuring the chain is valid. If signed block seems invalid then coins are withdrawn as punishment [31]. Therefore, It provides security against 51% attack by ensuring both stake and mining power should be greater than 51% to be able to forge into malicious transactions in the chain.

V. STRUCTURE OF BLOCK AND BLOCK HEADER

BlockChain is handled by different minors and nodes. Each transaction from nodes are validated by peer-to-peer authentication mechanism [32]. So requirement of common central authority is eliminated [33]. The Fig 3 represents the structure of the block, transaction and hash.

In addition to block headers information, SmartHome has its own cloud storage whereby all the transactions are pushed to cloud through powerful SmartHome Manager which is capable of handling huge data traffic. This helps in protecting the security and privacy of data generated in SmartHome. Time taken by each node to generate new block in SmartHome given below

T_max = T_min * N_blocks / (Time target * N_blocks)

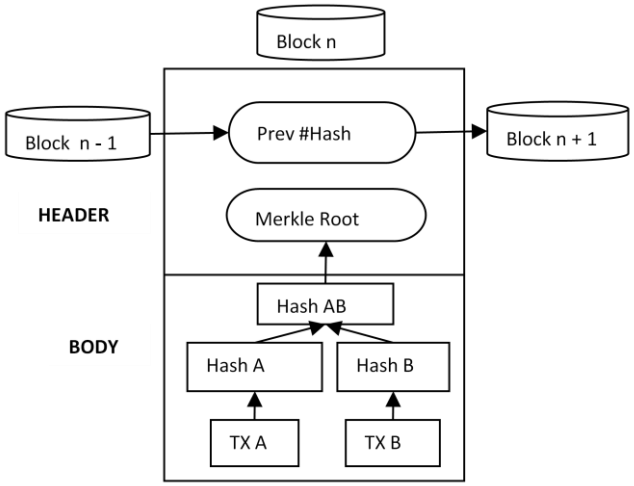

Fig 3: Structure of block

A. Merkle tree

A binary tree with its hash value of leaf nodes. Each of the node and leafs are validated against publically revealed root values [34]. Binary hash trees effectively utilized by BlockChain to ensure the privacy and security of data stored in BC[35]. Each of the node and leafs are tagged by Hash values and its children's are searchable through one-way functions. Search operation is completed by

$2 * \log_2 n$, where n is transactions storied in nodes

Tree provides efficient mechanism of retrieving the values of transactions and also to find if given transaction found in the Block through hash values. Search operation starts from leafs and then towards the root.

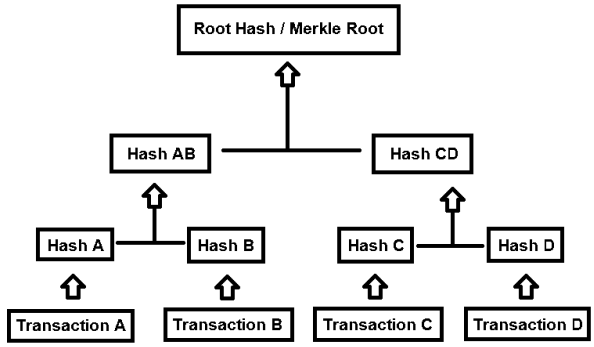

Fig 4: Merkle Root

To store the values of transaction in each Block, Hash # value of each transactions arrived like A, B..n and then Both hash value of A & B are together added to a single hash of AB. This operation repeated for entire Hash Tree to find out the Hash of the Block. For example, the hash value generated by SHA-256 is as follows,

Tx Hash A

ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

Tx Hash B

3e23e8160039594a33894f6564e1b1348bbd7a0088d42c4acb73eeaed59c009d

Therefore this transaction A and transaction B combined together and generate a single hash (AB).

Tx Hash(AB)

29efd862964bb39dacc7a263c5db9f8187f6f7264ef9190b42aa8f3099bf9ad6

Hence the Transaction hash AB and transaction hash CD combined together and generate a single unique hash (ABCD). This hash is determined as the Merkle Root and it is communicated to the various nodes.

VI. OPTIMIZATION OF BLOCKCHAIN AND SMARTHOME

SmartHome is the connected Home where number of IoT devices is connected to a SmartHome Device and all the data generated by Home are added to immutable Ledger of BlockChain through lightweight BC. Here we introduce the concept of overlay network. Each device provided with its own node id and transactions generated by it forwarded to SmartHome Device.

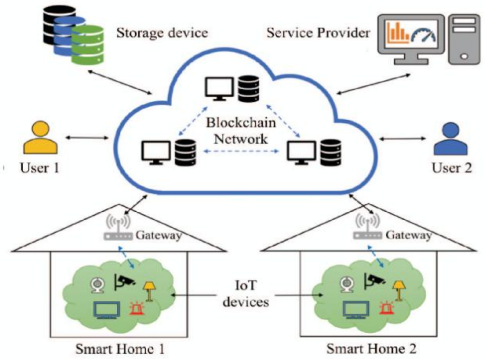

Fig 5: BlockChain connected with SHD

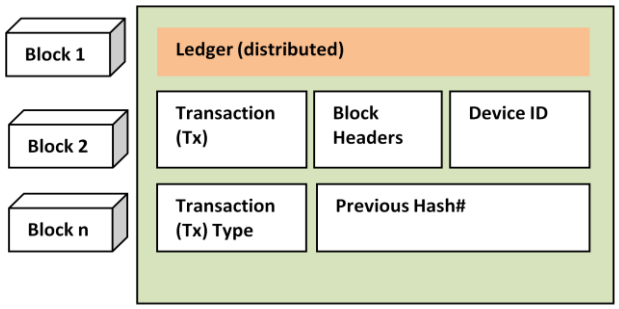

Fig 5: Distributed Ledger associated with blocks

Through encryption and SmartHome Device has high computational power to add it to BlockChain.

The block consists of Transaction ID, Previous Transaction ID, Primary Key of Requester, and Signature of Requester, Primary key of Requestee and signature of Requestee. On every request, Primary key and signature are validated and once authorized to get the values then we respond with the resources asked for.

The Local Block Manager uses Diffie-Hellman distribution of keys among the nodes. This method generates and distributes shared local key that are allowed to share data between local IL. The local transactions are encrypted between two entities that are associated with the transaction. Any kind of devices connected to the network is able to generate data and store it in Blocks. Same block is available over the common medium to reuse and called wherever required in the network.

The key transactions are a) Genesis b) Access c)Store and d) Monitor.

a) Initially the node block must create a common 'genesis transaction', this transaction set out as the initial point of the ledger among public Blockchain.

b) Then it generates a 'store instruction' to store data in cloud.

c) The 'access instruction' generated to access the devices.

d) Real time data can be obtained from the 'monitor instructions'.

Hence all this transaction / instructions are managed by Smart Home Device (SHD) which is in the overlay network. In SHD the transaction flow and data flow are done separately.

The smart home device handles all the transaction which is inbound and outbound from network. All the transactions are handled through shared key to ensure data security in the smart Home devices.

The SHD initiates the mining process through consensus method and initial block is conveyed to all the nodes on the network. SmartHome is having a Ledger and its policy to maintain authorization request from different devices. Following figure represents the Distributed Ledger associated with various blocks.

In the method of having lightweight BC in Smart Home provides more security in the form of immutable nature of BC and also external nodes cannot interfere in the home network unless it has valid primary key and authorization token to get into BC.

No service provider can tamper the data because control device in Smart Home ensures data flow between the devices is as per the authorization.

Also to improve the security in SmartHome on realtime basis, we can include Okta based REST service authorization with multiple methods of gateway signon and device identification, This will be an added advantage on top of SmartHome layer and external Denial of Attacks is eliminated through Okta Adaptive Multi-Factor Authentication(AMFA).

A. Transaction Validation & Authentication

SmartHome nodes generate transactions to validate itself from the SHD, and then Authentication of its credentials and previous hashes takes place. If the node raising the request has wrong credentials then its performance score is reduced by one otherwise credibility score increased. This ensures each node is performing mining at responsible way in a given mining duration.

When the number of devices is scaled and this might delay the validation and authentication process; so new concept of considering credibility factor is devised to ensure only limited transactions are validated against the block and authentication passed.

B.SmartHome Device Performance

Performance of SHD is essential since it acts as a central authority to provide required computational power to ensure local Blockchain. Each of the device addition and removal go through SHD, it ensures only authorized device id's are added to smart network and it is used for authorization factor.

Table II. Device Registration Table

SmartNode ID	Hardware Id	Avg. Rate of mining / Hr	Authorization Token
SN0001	XX-F1-G4-1	25	Read, Write
SN0002	AS-RD-G3-2	50	Authenticate

Rate of mining is revised based on consensus mechanism and its peers credibility rating against the node.

C. Cloud Data Storage

Each node is enabled to read and write the data to cloud using standard encryption algorithms. Identity management services in the form of CA, Token generation are used to ensure the authentication and data is secured. Private clouds like Amazon, Azure can be connected for public data storage.

VII. RESULTS AND DISCUSSION

This section describes the findings on our SmartHome implementation and simulation results. Practical implementation constrained due to practical implementation of proposed approach. BlockChain introduced in IoT devices brought down the security risks through effective identity management and authentication. Following are the list of possible attacks on IoT devices and how this approach eliminates the risks.

A. Confidentiality in Node Connections

Through effective hardware and smart node id, this methodology ensures the data confidentiality between nodes and also not allows any intruder to get copy of it. When intruder tries to get into system, all other nodes and SmartHome Device will not have Authentication entry in common shared table thereby eliminates the risk of data sharing to passive attacker.

B. Integrity of Data

Each node has the credibility factor and as and when wrong data shared between nodes or to central authority, Credibility ranking of the node is reduced and Block/Transaction generated is removed from SmartHome.

Below is the performance evaluation data, setup done through NS3 for 35 nodes. We calculated Authentication time and credibility raking mechanism to ensure it is not causing latency in IoT network.

Table III. Performance Results for Authentication & Credibility Factors

Message Type	No of Nodes	Avg. Time in Sec
Authentication	10	0.230
	30	0.552
	35	0.610
Credibility Update	10	0.110
	30	0.240
	35	0.265

C. Block Size Evaluation

Block size plays a crucial role since low computational power of IoT devices and routing between nodes to ensure valid transactions are stored in Blocks. Block size improves or reduces the latency or performance of the entire SmartHome. Simulation using 0.3MB to 3 MB used as the block size performed and latency increased with the number of devices. When number of devices added, due to parallel transmission latency stabilized.

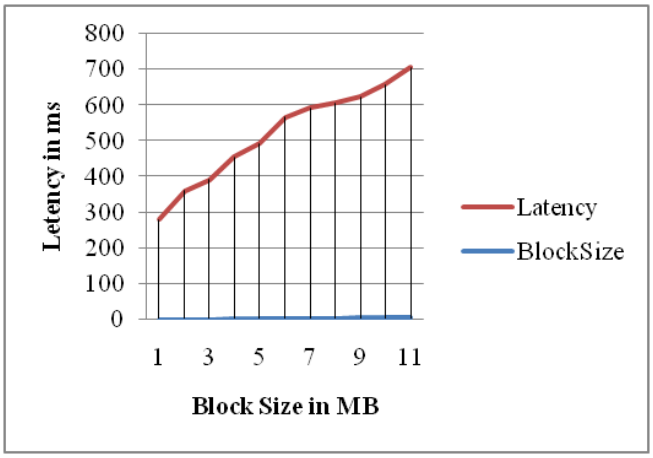

Fig 5: BlockSize and Latency

VIII. CONCLUSION

SmartHome is inevitable in current century and requires Smart solutions to ensure Privacy, Security in the IoT devices in SmartHome. This work explained the importance BC method of decentralized data storage, authentication and powerful mechanisms that can provide state-of-art security and privacy to SmartHome. SmartHome Device responsible for local BC and can handle privacy issues; each node with Authentication and Privacy ensures data Security. Encryption with BlockChain in proposed system acts dual security guards in SmartHome. BC combined in IoT environment provides the flexibility of handling large data volume in secure way between IoT applications and consumers. When the IoT network expands with exponential number of devices it requires Smart Home Manager to provide better traffic within network. So IoT and BlockChain shall be approach to tackle privacy Issues. Ensuring better response time and power consumption in a given BC is priority and can be taken up as a future work.

REFERENCES

1. Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the age ofmobility and smart devices in smart homes. In Privacy, Security, Risk and Trust(PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). IEEE, 819–826.
2. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In IEEE Symposium on Security and Privacy (SP), 2016, pages 839–858. IEEE, 2016.
3. A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in Proceedings of the 2nd IEEE/ACM International Conference on Internet-of-Things Design and Implementation, IoTDI 2017, pp. 173–178, ACM, Pittsburgh, PA, USA, April 2017.
4. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions, 2016,” https://arxiv.org/abs/1608.05187.
5. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, Kona, Big Island, HI, USA, March 2017.
6. A. Baliga, “Understanding blockchain consensus models,” Tech. rep., Persistent Systems Ltd, Tech. Rep, Tech. Rep., 2017.
7. Block Hashing Algorithm—Litecoin WiKi, accessed on Mar. 15, 2016. [Online]. Available: https://litecoin.info/Block_hashing_algorithm
8. P. Brody and V. Pureswaran, ‘‘Device democracy: Saving the future of the Internet of Things,’’ IBM Institute for Business Value, Tech. Rep., Sep. 2014. [Online]. Available: http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/
9. L. Baird, “Hashgraph consensus: fair, fast, byzantine fault tolerance,” Swirlds Tech Report, Tech. Rep., 2016.
10. A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Proceedings of the 2nd IEEE Security and Privacy Workshops, SPW 2013, pp. 23–27, USA, May 2013.
11. Christin N, Edelman B, Moore T (2015) ‘Bitcoin: economics, technology, governance’ Journal of Economic Perspectives, 29(2): 213-38.
12. M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2016, IEEE, Agadir, Morocco, December 2016.
13. M. Conoscenti, A. Vetro, and J. C. De Martin, “Peer to peer for privacy and decentralization in the internet of things,” in Proceedings of the 39th IEEE/ACM International Conference on Software Engineering Companion, ICSE-C 2017, pp. 288–290, IEEE, Buenos Aires, Argentina, May 2017.
14. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
15. A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, “On the security and performance of Proof of Work blockchains,” in Proceedings of the 23rd ACM Conference on Computer and Communications Security, CCS 2016, pp. 3–16, Austria, October 2016.
16. E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoins peer-to-peer network,” In USENIX Security, pp. 129–144, 2015.

17. A. Kiayias and G. Panagiotakos, "On trees, chains and fast transactions in the blockchain," IACR Cryptology ePrint Archive, vol. 2016, p. 545, 2016.
18. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk:The blockchain model of cryptography and privacy-preserving smart contracts," in Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp. 839–858.
19. T. H. Kim, "A Study of Digital Currency Cryptography for Bbusiness Marketing and Finance Security," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 1, pp. 365–376, 2016.
20. N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" IT Professional, vol. 19, no. 4, Article ID 8012302, pp. 68–72, 2017.
21. S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," self-published paper, August, vol. 19, 2012.
22. I. B. C. L. A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoins proof of work via proof of stake," 2014.
23. C. Natoli and V. Gramoli, "The Blockchain Anomaly," in Proceedings of the 15th IEEE International Symposium on Network Computing and Applications, NCA 2016, pp. 310–317, IEEE, November 2016.
24. A. Norta, "Creation of smart-contracting collaborations for decentralized autonomous organizations," in International Conference on Business Informatics Research. Springer, 2015, pp. 3–17.
25. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2017.
26. M.Pilkington, Blockchain technology: principles and applications. research handbook on digital transformations, F. X. Olleros and M. Zhegu, Eds., 2016.
27. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
28. L. Ren, "Proof of stake velocity: Building the social currency of the digital age," Self-published white paper, 2014
29. F. d. O. Sergio, J. F. da Silva Junior, and F. M. de Alencar, "The blockchain-based internet of things development: Initiatives and challenges," ICSEA 2017, p. 39, 2017.
30. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
31. A. Tapscott and D. Tapscott, "How blockchain is changing finance," Harvard Business Review, vol. 1, 2017Wu L., Du X., Wang W., Lin B. An out-of-band authentication scheme for internet of things using blockchain technology; Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC 2018); Maui, HI, USA. 5–8 March 2018; pp. 769–773.
32. G. Zyskind, O. Nathan et al., "Decentralizing privacy: Using blockchain to protect personal data," in Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015, pp. 180–184.
33. G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proceedings of the IEEE Security and Privacy Workshops, SPW 2015, pp. 180–184, IEEE, May 2015Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," Work Pap.–2016, 2016.
34. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen and Huaimim Wang,"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE 6th international congress on Big Data.
35. Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015, pp. 184–191, IEEE, France, February 2015

AUTHORS PROFILE

Mrs. D.M Sheeba, Completed MSc in 2012 at Sun College of Engineering and Technology, Kanniyakumari and at present working as an Assistant Professor in Dept of Computer Science, New Prince Shri Bhavani Arts & Science College, Chennai. She is currently pursuing PhD in Computer Science at VISTAS, Pallavaram. Her Area of interest and research includes Network Security, and Cryptography, Internet of Things. She has been actively taken part and presented and published various papers in International and National Conferences in his research area.

Dr. S. Jayalakshmi working as Professor in the Department of Computer Applications, Vels Institute of Science, Technology and Advanced studies (VISTAS), Pallavaram, Chennai. She has more than 14 years of experience in both Industry and Educational Institute. Her area of research includes Natural Language Processing (NLP) and Data Mining. She has published more than 25 Research Papers in National and International journals. She is interested in writing textbooks for the students to make them understand any concept in an easy way. She is a recognized supervisor, guiding M.Phil. and PhD scholars.