SEYBOLD Report
ISSN: 1533 - 9211

DOI: 10.5281/zenodo.6875840

BLOCKCHAIN ARCHITECTURE USING SLIDING WINDOW FOR INTERNET OF THINGS

Prasanna Kummari
Assistant Professor, Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad, India

A. Susmitha
U.G Student, Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad, India, prasanna.swec02@gmail.com

A. Pravallika
U.G Student, Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad, India, prasanna.swec02@gmail.com

Ch. Jayasri
U.G Student, Department of Electronics and Communication Engineering, Sridevi Women's Engineering College, Hyderabad, India, prasanna.swec02@gmail.com

Abstract: Internet of things is a concept that interrelates the devices that are connected to one or the other network for the purpose of exchanging the data with the other systems and devices without the necessity of human to machine interaction. Nowadays, privacy and security are the two major concerns in IoT and also the crucial security requirements of IoT cannot be guaranteed by the existing security structures due to the restraints in memory and CPU of the IoT devices. There is also another disadvantage which is the centralized security architecture which means to a database that is located or situated at a single point or single server but whereas it has a limitation of single point of attacks and also defending against this limitation is very costly. So a decentralized security architecture is required for IoT and it is designed in such a way that it meets the limitations caused by the centralized security architecture. So an important concept called Blockchain comes into the picture where the Blockchain is a decentralized security architecture which is very much suitable for different applications. However, Blockchain is not suitable in its original form due to low scalability and high complexity. So we propose a Sliding window blockchain architecture which helps in many ways such as in modifying the traditional Blockchain architecture to suit IoT applications. This proposed Sliding window blockchain architecture will make use of previous blocks to form the has h of the next block and also the hash values altogether are responsible in sliding window block chain architecture performance is analysed on a real time data stream generated from smart home testbed. Finally, the overall results shows the advantages of this proposed Blockchain architecture that is increased security and minimization of the memory overhead.

Keywords: Blockchain, Internet of Things, smart home, security, sliding window.

1. Introduction

Blockchain is an immutable distributed information. It supports traceability and audibleness of huge scale systems, including IoT. This immutableness could also be at odds with new legislation such as the EU General information Protection Regulation (GDPR) which supports the proper to be forgotten by removing information from third party records once it's served its purpose. With the growing scale and prevalence of net of Things sensors in our daily lives, trusting these sensors and systems to deliver reliable information whereas maintaining our security and privacy may be a crucial thought. The IoT network architecture needs suburbanised and light-weight approaches for delivering trust, whereas most typical approaches area unit either centralised or computationally demanding. There exist 2 varieties of blockchains: (i) permis- sioned and (ii) permissionless A permissioned blockchain may be a non-public blockchain which needs pre verification of the participants inside the network UN agency area unit assumed to understand one another whereas

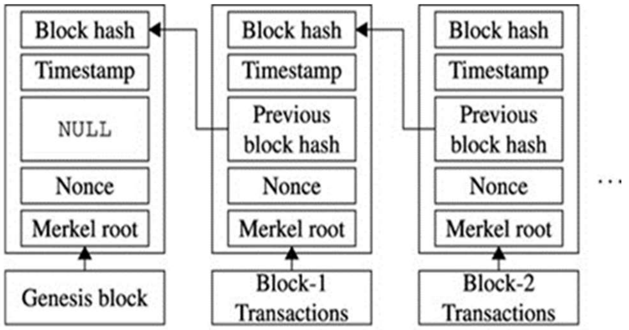


Figure 1: Blockchain Architecture

, a permissionless blockchain may be a public blockchain. ancient blockchain approach isn't appropriate Prescilla K, Sarath adult male, and Manoj. B. S. area unit with the Department of astronautics, Indian Institute of house Science and Technology, Thiruvananthapuram, Asian nation 695547.for IoT with period of time information streams due to their computation-ally complicated Proof- of-Work (PoW). As the process time will increase, blockchain security becomes impossible to be used for IoT. the 2 major challenges concerned in applying blockchain to IoT environments include: (i) process quality and (ii) scalability. The process quality depends on diffificulty level and Merkle tree size. Merkle tree may be a tree in which each leaf node is tagged with the hash of a transaction information and each non-leaf node is tagged with the cryptographic hash of the labels of its kid nodes. Merkle tree grows with the quantity of transactions created and, thereby, increasing the time consumed for Proof-of- Work, which is a smaller amount favorable for AN IoT network. measurability refers to the boundaries on the quantity of transactions a blockchain will process inside a specific period. Bitcoin may be a widespread example of a blockchain. Bitcoin blockchain may be a payment system that doesn't place confidence in a central authority to secure and control its funds. every block in a very Bitcoin blockchain has restricted block size. In Bitcoin, the block size is limited to one MB and a block is strip-mined each 10 minutes. Interestingly, the present literature [3] suggests blockchain as one of the info security and privacy algorithms that may be enforced for IoT

DOI: 10.5281/zenodo.6875840

applications because of its distributed architecture. during this paper, we tend to propose a replacement blockchain architecture for IoT environments, particularly within the context of sensible home applications. a sensible home monitors, analyzes, and reports the state of the house. sensible homes use devices connected to IoT to change and monitor in-home systems. sensible home are often thought-about because the smallest unit of a sensible town. the protection standardization of a sensible home supports a sensible town and contrariwise.

2. METHOD

The window Blockchain (SWBC) utilizes a window that slides through the blockchain for every block addition. The window at first consists of one block and will increase up to n blocks as defined by the window size. The blocks within the sliding window area unit used whereas making a replacement block. within the planned SWBC design, the block hash is generated by hashing the blocks inthe window as shown in Figure three. the scale of the sliding window determines the amount of recent past blocks wont to perform the hash update function. The window blockchain incorporates a computational overhead of (n) for a continuing difficulty of mining, wherever n is that the variety of blocks within the window used for the hash updatefunction. window improves the immutability of the blockchain records. A false miner needs previous (n 1) blocks and therefore the window size n to mine a block. The window size is kept secret and sent solely to the miners in conjunction with the genesis block. The restricted a part of the chain, i.e., the recent n blocks is keep within the memory of IoT device and therefore the whole blockchain is keep during a private cloud. once the window slides, the older block comes out of the window (block B1 as shown in Figure 3(b)) and is deleted from the IoT device memory. Therefore, the memory overhead to store the blocks in IoT device is reduced. The SWBC structure and its comparison with a Bitcoin blockchain area unit mentioned within the following sections.

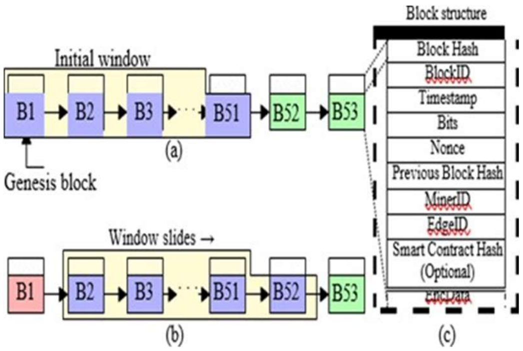


Figure 1:Sliding window blockchain design

A. Siding window Blockchain structure

Figure 3(c) shows the window block structure. The SWBC block consists of block hash, blockID, timestamp, bits, nonce, previous block hash, minerID, and edgeID. Block Hash is generated by hashing current block and former (n − 1) blocks. The BlockID represents a novel ID of a block. solely the members area unit allowed to access the block ID of the new side block. The field Timestamp shows the time at that the block is created. the sphere Bits represents the issue level of mining. the issue level of mining is decided by the amount of initial zeros of the hash value. every zero is diagrammatic by four bits. The difficulty levels area unit diagrammatic as follows: Level 1 (4 bits), Level two (8 bits), Level three (12 bits),Level 4 (16 bits), and Level five (20 bits). because the variety of zeros will increase, the issue level of mining (i.e., computation time) will increase apace. A high difficulty level for POW ends up in a rise in computing resources, that makes Bitcoin blockchain not appropriate for IoT [17]. Also, toreduce the entire computation time to mine the blocks, the issue level may be chosen randomly between one and five. The time being worth represents the iteration that the proof of labor gets solved . The Previous block hash is that the hash of the previous block that inherits the properties of previous n blocks, wherever n is that the size of the window. MinerID represents the ID of the entry and EdgeID represents the ID of the sting device. Smart Contract Hash represents the hash worth of the smart contract accepted by all the miners. Smart contract hash field is elective andactivating this field secures the good contract from reentrancy attack. good contract hash field isn't enclosed in our exper- iment. The EncData consists of sensing element data encrypted exploitation the Advanced secret writing Standard algorithmic rule with arcanum based mostly Key Derivation operate (PBKDF2)

3. RESEARCH RESULT

Figure 1: Home screen

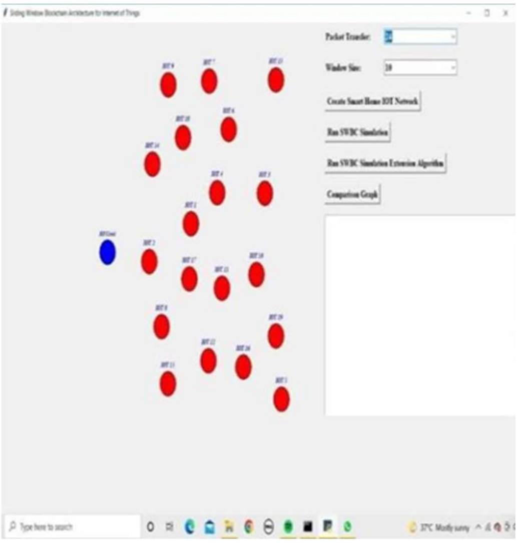
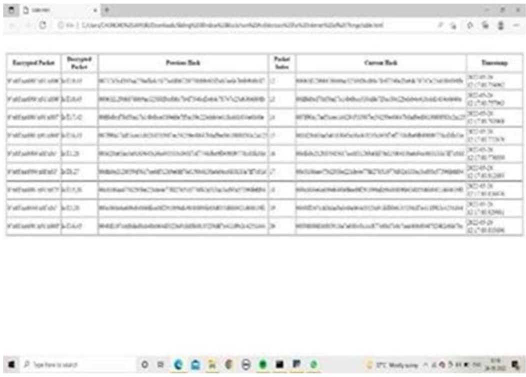

Sliding Window Blockchain Architecture for Internet of Things
Packet Transfer:
Window Size:
10
Create Smart Home IOT Network
Run SWBC Simulation
Run SWBC Simulation Extension Algorithm
Comparison Graph
Type here to search
37°C Mostly sunny

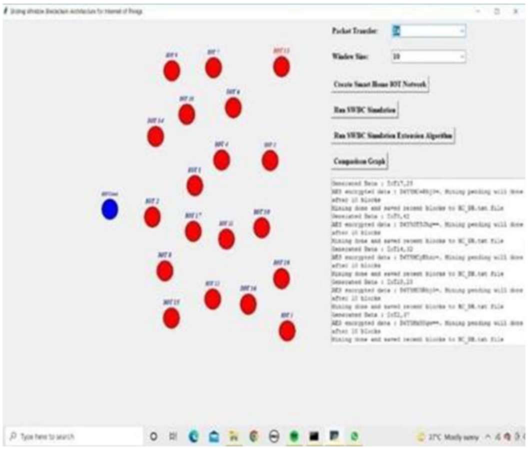
Figure 2: Creation of smart home network

DOI: 10.5281/zenodo.6875840



Encrypted Packet	Decrypted Packet	Previous Hash	Packet Index	Current Hash	Timestamp
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure 3: SWBC Simulation

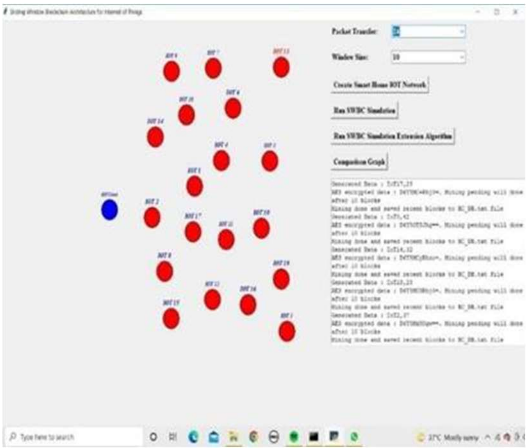

Create Smart Home IOT Network
Run SWBC Simulation
Run SWBC Simulation Extension Algorithm
Comparison Graph

Packet Transfer:

Window Size: 10

```
Generated Data : 1:f17,25
AES encrypted data : b4T0BC+8bj0=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f3,42
AES encrypted data : b4TkUT53hg==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f14,32
AES encrypted data : b4TYBCyBhz=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f23,23
AES encrypted data : b4T0HC3Bhj0=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f2,27
AES encrypted data : b4TS8a5Qg==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

Figure 4: Blocks store at IoT memory


Create Smart Home IOT Network
Run SWBC Simulation
Run SWBC Simulation Extension Algorithm
Comparison Graph

Packet Transfer:

Window Size: 10

```
Generated Data : 1:f17,25
AES encrypted data : b4T0BC+8bj0=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f3,42
AES encrypted data : b4TkUT53hg==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f14,32
AES encrypted data : b4TYBCyBhz=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f23,23
AES encrypted data : b4T0HC3Bhj0=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : 1:f2,27
AES encrypted data : b4TS8a5Qg==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

Figure 5: SWBC Simulation Extension Algorithm

DOI: 10.5281/zenodo.6875840

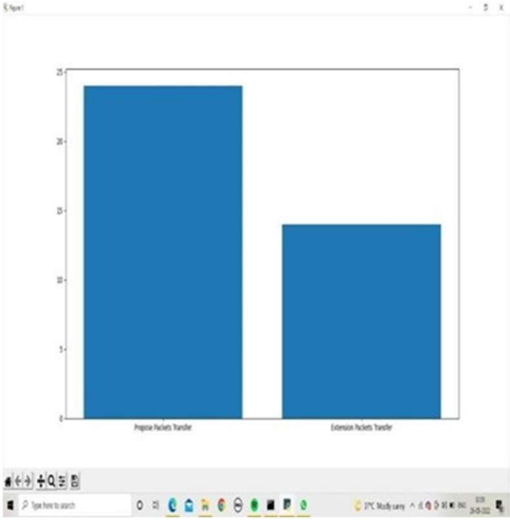


Figure 6: Comparison Graph

4. DISCUSSION OF THE RESULT

In this paper author is describing thought to provide security to IOT devices exploitation Blockchain technology as this technology supports decentralized knowledge storage which implies knowledge can be hold on at multiple nodes compare to centralized storage wherever knowledge is hold on at single centralized server. localised knowledge storage provides facility of receiving knowledge from any out there node and it's strong security wherever one knowledge store can verify hash price of all nodes. Verification of all nodes hash is computation intensive and its can't be applied to IOT little devices thanks to memory, CPU and energy consumption restrictions. to beat from this drawback author introduce slippy window technique wherever the window size are going to be fixed and every one Blockchain dealing hash values will be hold on in window and if window size exceeded then previous dealing blocks are going to be slided or removed and maintain solely recentblocksdue to this method memory storage and knowledge transfer overhead are going to be reduced. during this paper author is exploitation device and different devices for implementation however we tend to don't have any devices or sensors therefore I implement this project as simulation

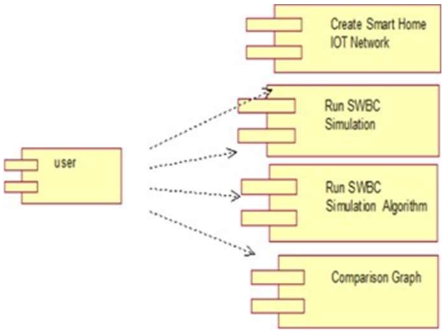


Figure 1: Process flow

DOI: 10.5281/zenodo.6875840

5. CONCLUSION

IoT devices face constraints on resources such as computational capability, energy sources, and memory. Therefore, the standard security algorithms are not feasible for IoT. We proposed a sliding window blockchain that meets the requirements of a resource constrained IoT network by reducing the memory overhead and limiting the computational overhead. From the experimental results, we observed the following: (i) The computational time of PoW for each level of difficulty increases exponentially. (ii) The total block addition time increases with the increase in the number of miners in the group. (iii) As the window size increases, the hash computation time increases linearly. (iv) A random selection of difficulty for each block in a blockchain reduces the total block addition time. Future work can be carried out to analyse the impact of a variable size sliding window. New consensus algorithms can be developed to suit the IoT environment. Furthermore, energy consumption of the blockchain can also be analyzed to draw more insights on energy resources required for an IoT device

REFERENCES

[1] S. Kulkarni, “The great thing about the blockchain,” Open supply for You, vol. 06, pp. 22–24, June 2018.T. M. F. Carames and P. F. Lamas, “A review on the utilization of blockchain for the web of Things,” IEEE Access, vol. 6,
pp. thirty-two 979–33 001, May 2018.

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in web of Things: challenges and solutions,” arXiv preprint arXiv:1608.05187, August 2016.

[3} IoT Agenda, “Smart home or building,” Apr 2018. [On- line].Available: https://internetofthingsagenda.techtarget.com/definitio n/ smart-home-or-building

[4] L. Jiang, D. Y. Liu, and B. Yang, “Smart home analysis,” in Proceedings of 2004 International Conference on Machine Learning and IP, vol. 2, August 2004, pp. 659– 663.

[5} The institute.ieee.org, “Towards a definition of the In- ternet of Things (IoT),”May 2015. [On- line].Available: https://iot.ieee.org/images/files/pdf/IEEE IoT towards Definition web of Things Revision1 27MAy

[6] J. Wan, X. Gu, L. Chen, and J. Wang, “Internet of Things for close aided living: Challenges and future opportunities,” in International Conference on Cyber- Enabled Distributed Computing and information Discovery (CyberC), October 2017, pp. 354–357.

[7] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, “Novel anonymous key institution protocol for isolated sensible meters,” IEEE Transactions on Industrial physical science, vol. 67, no. 4, pp. 2844– 2851, April 2020.

[8] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman, and
T. Y. Lin, “The role of prediction algorithms within the MavHome sensible home design,” IEEE Wireless Communications, vol. 9, no. 6, pp. 77–84, December
2002.

[9] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, “Blockchain primarily based credibleness verification technique for IoT entities,” Security and Commu- nication Networks, vol. 2018, pp. 1–11, June 2018.

[10] C. Lee, L. Zappaterra, K. Choi, and H. A. Choi, “Securing sensible home: Technologies, security challenges, and security necessities,” in IEEE Conference on Communications and Network Security, October 2014, pp. 67–72.

[11] P. Treleaven, R. G. Brown, and D. Yang, “Blockchain technology in finance,” Computer, vol. 50, no. 9, pp. 14–17, Sep 2017.

[12] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and
V. Santamar´ıa, “To blockchain or to not blockchain: that's the question,” IT Profes- sional, vol. 20, no. 2, pp. 62–74, March 2018.

[13] P. A. Laplante and B. Amaba, “Introducing the web of Things department,” IT skilled, vol. 20, no. 1, pp. 15–18, Gregorian calendar month 2018.

[14] C. Esposito, A. D. Santis, G. Tortora, H. Chang, andK. R. Choo, “Blockchain: A cure-all for health care cloud- based knowledge security and privacy,” IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, Gregorian calendar
month 2018.

[15] N. Kshetri, “Can blockchain strengthen the web of Things,” IT skilled, vol. 19, no. 4, pp. 68–72,
July/August 2017.

[16] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards associate degree optimized blockchain for IoT,” in Proceedings of the Second International Confer- ence on web of Things style and Implementation. ACM, August 2017, pp. 173–178.

[17] J. Shen, C. Wang, T. Li, X. Chen, X. Huang, and Z.H. Zhan, “Secure knowledge uploading theme for a sensiblehome system,” info Sciences, vol. 453, pp. 186– 197, July 2018.

[18] K. Christidis and M. Devetsikiotis, “Blockchains and sensible contracts for the web of Things,” IEEE Access, vol. 4, pp. 2292–2303, Gregorian calendar month 2016.

[19] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentral- ized computation platform with warranted privacy,” arXiv preprint arXiv:1506.03471, 2015.

[20] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain primarily based knowledge integrity service framework for IoT knowledge,” in 2017 IEEE International Conference on net Services (ICWS), June 2017, pp. 468–475.

[21] A. Bahga and V. K. Madisetti, “Blockchain platform for industrial web of Things,” Journal of software system Engineering and Applications, vol. 9, no. 10, p. 533,
October 2016.

[22] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel,A. Roger, and R. Sirdey, “Towards higher accessibility and responsibility for IoT updates by suggests that of a blockchain,” in 2017 IEEE European conference on Security and Privacy Workshops (EuroS PW), April 2017, pp. 50–58.

[23] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, “A blockchain- primarily based trust system for the web of Things,” in Proceedings of the 23nd ACM on conference on Access management Models and Technologies. ACM, June 2018, pp. 77–83.

[24] P. Otte, M. de Vos, and J. Pouwelse, “Trustchain: A sybil-resistant ascendable blockchain,” Future Generation laptop Systems, pp. 12–23, July 2017.

DOI: 10.5281/zenodo.6875840

[25] Feng Tian, “A provide chain traceability system for food safety supported HACCP, blockchain & web of Things,” in 2017 International Conference on Service Systems and repair Management, June 2017, pp. 1–6.

[26] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everyplace - a use-case of blockchains within the company supply-chain,” in 2017 IFIP/IEEE conference on Integrated Network and repair Management (IM), May 2017, pp. 772–777.

[27] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a sensible home,” in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),March 2017, pp. 618–623.

[28] M. Samaniego and R. Deters, “Blockchain as a service for IoT,” in 2016 IEEE International Conference on web of Things (iThings) and IEEE inexperienced Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE sensible knowledge (SmartData), December 2016, pp. 433–436.

[29] B. Kaliski, “Password-based cryptography specification version a pair of.0,”Network working party, RSA Laboratories, pp. 1– 34, Sep 2000.

[30] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An summary of blockchain technology: design, consensus, and future trends,” in 2017 IEEE International Congress on huge knowledge (BigData Congress), June 2017, pp. 557–564