Data Security for IoT Using Block chain

Y. RAJESWARI[1], P. LAVANYA[2], P. BHAVYASRI[3], B. AKHILA[4]
[1, 2, 3, 4] *Student, Vasireddy Venkatadri Institute of Technology, A.P, India*

Abstract- ***Internet of Things is creating new opportunities and providing a competitive advantage for different fields. One of the key challenges of IoT world is security. In this article, our attempt is to critically view the use of Block chain Technology to secure IoT. Block chain is a distributed database technology that provides very hard to tamper, ledger records. It allows storage of all transactions into immutable records and every record distributed across many participant nodes. The security comes from use of strong public key cryptography, strong cryptographic hash and complete decentralization. In this project, we develop an IoT application to monitor temperature and store it securely in the block chain. We use Raspberry Pi 3 Model B for implementing the project. The prototype can be extended to any type of application.***

Indexed Terms- Block chain; Internet of Things; privacy; security; smart contracts

I. INTRODUCTION

Internet of Things (IoT) is reshaping the incumbent industry to smart industry featured with data-driven decision-making [1].Internet of Things, as coined by Kevin Ashton [2], has revolutionized the world with its potential to build cost-effective applications. In the near future, IoT is going to influence almost every day-to-day item we use. With such an important role it plays in our life, there is a consensus that the security problem is of the first priority of IoT due to the accessibility and hardware/software constraints on IoT devices. Along with this, IoT faces challenges like heterogeneity of IoT system, poor interoperability, resource constraints of IoT devices and privacy vulnerabilities.

Although the IoT can facilitate the digitization of the information itself, the reliability of such information is still a key challenge. In this sense, a new technology that was born as the first decentralized cryptocurrency has the potential to offer a solution to the data reliability problem: Bitcoin, which has revolutionized the mechanisms in money transfers.

Bitcoin is supported by a protocol that details the infrastructure responsible for ensuring that the information remains immutable over time. This protocol is known as block chain.

A block chain [3] is essentially a distributed ledger spreading over the whole block chain system. An exemplary block chain consists of a number of consecutively-connected blocks. Each block (with the exception of the first block) in a block chain points to its immediately-previous block (called parent block) via an inverse reference that is essentially the hash value of the parent block.

A block chain is continuously growing with the transactions being executed. When a new block is generated, all the nodes in the network will participate in the block validation. This process is called mining and the nodes that perform mining are called miners. A validated block will be automatically appended at the end of the block chain via the inverse reference pointing to the parent block. In this manner, any unauthorized alterations on the previously-generated block can be easily detected since the hash value of the tampered block is significantly different from that of the unchanged block. The consensus mechanism in block chain is crucial for it to function correctly. The consensus mechanisms ensure that all the nodes in the block chain are synchronized with each other, and all the transactions in the blocks are valid.

Moreover, since the block chain is distributed throughout the whole network, the tampering behaviour can also be easily detected by other nodes in the network. Recently, several surveys on the convergence of block chain with IoT have been published. In particular, [4] gives a systematic literature review on block chain for IoT with the categorization of a number of use cases. The work of [5] presents a survey on IoT security and investigates

the potentials of block chain technologies as the solutions.

Being a fully transparent and decentralized system, block chain technology has emerged as an effective solution for solving the security issues related to IoT. The rest of the paper is ordered as follows: In Section 2 Literature review is given highlighting Block chain properties and its characteristics. Section 3 illustrates the importance of smart contracts in block chain showing results of a sample application of sensing room temperature. Finally in Section 4, Conclusion and Future work are presented.

II. LITERATURE REVIEW

Block chain has created a new revolution in this emerging world of technology and gained so much popularity through its features [6] that makes it so resistible. Below are the key features:

1. Immutability
2. Decentralized technology
3. Enhanced security
4. Distributed ledgers
5. Consensus

And these features are achieved through its varied architecture supported by various techniques and algorithms which are elaborated below.

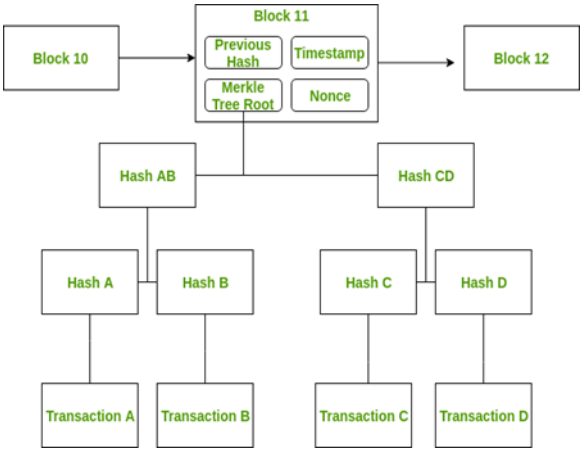
2.1 ARCHITECTURE:

- STRUCTURE:

The first block of a block chain is called the genesis block with no parent block. In brief, a block structure consists of the following information: 1) block version (indicating the validation rules to follow), 2) the hash of parent block, 3) Timestamp recording the current time in seconds, 4) Nonce staring from 0 and increasing for every hash calculation, 5) the number of transactions, 6) Merkle Root (i.e., the hash value of the root of a Merkel tree with concatenating the hash values of all the transactions in the block) as shown in the figure.

- NODES IN BLOCKCHAIN:

A block chain exists out of blocks of data. These blocks of data are stored on nodes [7] **(**compare it to small servers). Nodes can be any kind of device (mostly computers, laptops or even bigger servers). Nodes form the infrastructure of a block chain. All nodes on a block chain are connected to each other and they constantly exchange the latest block chain data with each other so all nodes stay up to date.



STRUCTURE OF BLOCKCHAIN

These nodes form a P2P network which facilitates in maintaining a decentralized database. There exists some other nodes called miners which participate in block validation and the process is called Mining.

2.2 TECHNIQUES AND ALGORITHMS:

- CRYPTOGRAPHY:

Cryptography provides techniques for transformation of data in order to render it useless for unintended receivers of the data. Block chain uses Public-key cryptography, one the cryptography techniques to achieve privacy and security.

Public-key cryptography (also called asymmetric cryptography) is a system that uses a pair of keys – a public key and a private key. The public key may be widely distributed, but the private key is meant to be known only by its owner. Every person in the network possesses both private and public keys. Anyone can use someone's public key to encrypt a message, but once encrypted, the only way to decrypt is by using the corresponding private key. This is one role of block validators before they add any transaction to the block chain.

- HASHING:

Hashing in block chain refers to the process of having an input item of whatever length reflecting an output item of a fixed length. This is regardless of the length of the input transaction. The output is what we call a hash.

A hash function, will take any transaction/data input and rehash it to produce an output of a fixed size. The process of using a given hash function to process a transaction is called hashing. Presently SHA-256 is the most secure hashing function that generates a 256 bit length hash for every input.

Merkle tree is a mathematical entity that is crafted as a tree of hashes of different blocks of data. This structure allows verification of arbitrary transaction in large volumes of data with a similar hash verification process used for a small amount of data. This method is very efficient and forms the core of the block chain. The root hash indicates the hash of the entire data set.

- CONSENSUS:

A consensus algorithm is a procedure through which all the peers of the Block chain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Block chain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Block chain is the one and only version of the truth that is agreed upon by all the nodes in the Block chain.

Various consensus algorithms [8-12] to achieve some specific objectives such as coming to an agreement, collaboration, co-operation and equal rights to every node etc. are as follows:

1. Proof of Work
2. Practical Byzantine Fault Tolerance
3. Proof of Stake
4. Proof of Burn
5. Proof of Capacity
6. Proof of Elapsed Time

Block chain networks cannot work function properly without the consensus algorithms to verify each and every transaction that is being committed.

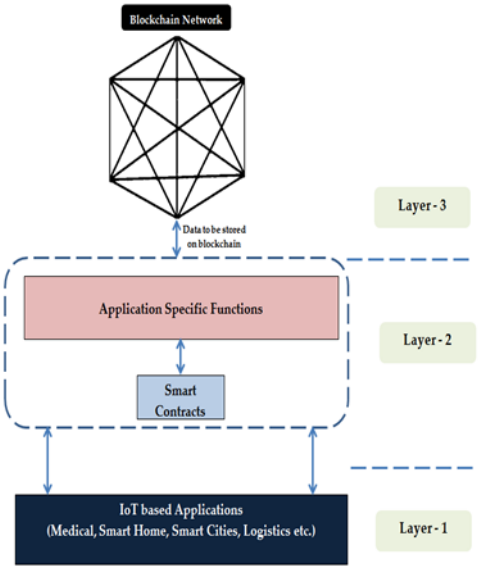
A comprehensive review on various mining and consensus mechanisms in block chain has been presented in [13].

III. SMART CONTRACTS

A Smart contract is a piece of code that contains a set of terms governing the transactions over the block chain network and executes these terms without any third-party intervention. A smart contract can be accessed by all its users using a contract's address generated by the block chain platform during its deployment stage. The combination of block chain and smart contracts has revolutionized the current business scenarios and this combination is termed by developers as Block chain 2.0.

Nick Szabo [14] proposed utilization of decentralized ledger for self-executing contracts. These contracts could be converted, stored and replicated by participants of BC. Non-availability of necessary technologies, especially the distributed ledger, caused a hindrance in the realization of the concept at that time. After the appearance of Bitcoin in 2008 and Ethereum [15] in 2014, it became possible to support the realization of a smart contract.

The application of smart contracts in this scenario is illustrated through a three layered architecture shown in the figure below:



THREE LAYERED ARCHITECTURE

Layer1 consists of IoT based applications, medical, smart homes, smart cities, logistics etc. Layer2 consists of application specific functions and smart contracts. Layer3 consists of a block chain network in which data is to be stored. A smart contract is an agreement between two people in the form of computer code. They run on the block chain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract processed by the block chain, which means they can be sent automatically without a third party.

Among the available block chain development platforms, the most popular are Ethereum, Hyperledger [16], and IBM Block chain [17]. For the evaluation of this model, Ethereum is being used as a platform. In order to reduce the computational costs and complexity, this model uses lightweight smart contracts instead of conventional consensus mechanisms [18] to record transactions and allow access to the resources.

Below are the steps to develop smart contract on ethereum:

1. Find an open source solidity contract as a starting point
2. Define the abstract token contract
3. Define the abstract store contract
4. Write test cases for test-driven development
5. Implement the smart contract code
6. Create a custom dev chain for testing

We considered an IoT application of sensing room temperature through temperature sensor aided by Raspberry Pi 3.

Solidity, the official programming language to build smart contracts in Ethereum based blockchains, is used to code the smart contracts and below figure represents the algorithm to validate the IoT device for the application we considered.

```
Storing IoT data in the Database
Input: deviceID, parameters
Output: Parameters are stored in the database and Transaction is recorded.
pragma solidity ^0.5.12;
mapping(address => bool) authorizedDevices;
 if( isDeviceAuthorized(deviceID))
   store the parameters in corresponding device's record;
   transaction is recorded in the blockchain;
   store the transaction hash and block number in the device record;
 }
else
  Revert the transaction;
   function public isDeviceAuthorized(address deviceID) public view return (bool approved)
{
    return authorizedDevices[deviceID];
}
```

ALGORITHM TO VALIDATE THE DEVICE

The data will be stored in the block chain network through smart contract. Initially, an array of Device Id's will be stored in the stack. Smart contacts checks whether the data is eligible to store in block chain network or not. It is done by checking the Application Id with the Device Id in the network. If the Application Id is in the array, then the data will be stored in the network. Otherwise, it reverts the transaction.

Finally we show up the result of recording the temperature through block chain after authentication of the device providing a secured record of data.

```
Connection Status: True
System Version : 3.7.3 (default, Oct  7 2019, 12:56:13)
[GCC 8.3.0]
Room Temperature: 28.2 in degree Celcius
0x4a741a95Ae2bb93fda2d84A71568C8CD85C45E7a
Balance :: 196873437500000000000
<web3._utils.datatypes.Contract object at 0x7f78495d9438>

AttributeDict({'blockHash': HexBytes('0xd3fc40f44c6a98a06bc73a8397117bb1906598b
'gas': 126753, 'gasPrice': 1000000000, 'hash': HexBytes('0x890cb52757542bddf265
0000000000000000000000001564', 'nonce': 47, 'to': '0x4dE0fFB255296e7A501860cb9C
dbde4a5cbd61a3c3686e509662ee53e21ccdeled'), 's': HexBytes('0x78d8d57f8205e9bfd0
AttributeDict({'blockHash': HexBytes('0xd3fc40f44c6a98a06bc73a8397117bb1906598b
from': '0x4a741a95ae2bb93fda2d84a71568c8cd85c45e7a', 'gasUsed': 26753, 'logs':
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000'), 'roo
0cb9c97d0e579884166', 'transactionHash': HexBytes('0x890cb52757542bddf265590f8b
b"\x89\x0c\xb5'W7+\xdd\xf2eY\x0f\x8bk\xd9\xcd?\xb5\xb7$\x0c\xe7>\x12\x97_b\x7f\
5476
User Authenticated...Allowed to Post Data
```

OUTPUT WINDOW

The above figure shows the output window indicating the recorded temperature along with some attributes like gas, transaction hash and authentication etc.

CONCLUSION

This paper aims to present the literature review on Block chain and Internet of Things and emphasized issues linked to an IoT atmosphere**.** IoT is the next immerging technology with the rise of high-speed network and intelligent network devices. Unfortunately, IoT devices are more prone to attacks and unable to protect themselves. In this paper, we highlighted the key concepts in block chain that has demanded the use of it in the field of IoT.

Also we highlighted the importance of smart contracts in block chain technology through illustrative figures indicating the concepts behind.

FUTURE WORK

We further aim more to practically implement blockchain properties on the internet of things for monitoring, error discovery, and automatic fault correction in high critical IoT systems. Moreover, simulation-based performance assessment can be conduct to demonstrate the scalability and effectiveness of the blockchain-based solutions.

This work can be further broadened to encompass social network applications so as to make blockchain inclusive in order to derive the benefits of both the applications resulting in secure social platforms.

REFERENCES

[1] P. Lade, R. Ghosh, and S. Srinivasan, "Manufacturing Analytics and Industrial Internet of Things," IEEE Intelligent Systems, vol. 32, no. 3, pp. 74–79, May 2017.

[2] Ashton, K. That Internet of Things Thing. RFID J. 2009, 22, 97–114.

[3] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 24 October 2019).

[4] M. Conoscenti, A. Vetr `o, and J. C. De Martin, "Blockchain for theinternet of things: A systematic literature review," in 2016 IEEE/ACS13th International Conference of Computer Systems and Applications (AICCSA), Nov 2016, pp. 1–6.

[5] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet-of-things security: a position paper," Digital Communications and Networks, vol. 4, no. 3, pp. 149 – 160, 2018.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang (2017), 'An overview of blockchain technology: Architecture, consensus and future trends.' Big Data (Big Data Congress) IEEE International.

[7] K. Christidis and M. DevetsikIoTis, (2016) 'Blockchains and Smart Contracts for the Internet of Things,' IEEE Access, vol. 4, pp. 2292–2303.

[8] Laurie, B.; Clayton, R. "Proof-of-Work" Proves Not to Work. Available online: https://www.cl.cam.ac.uk/~rnc1/proofwork.pdf (accessed on 21 February 2018).

[9] O'Dwyer, K.J.; Malone, D. Bitcoin mining and its energy footprint. In Proceedings of the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information andCommunications Technologies (ISSC 2014/CIICT 2014), Limerick, Ireland, 26–27 June 2014; pp. 280–285.

[10] Buterin, V. What Proof of Stake Is and Why It Matters. Available online: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/ (accessed on 10 January 2018).

[11] Patterson, R. Alternatives for Proof-of-Work, Part 2: Proof of Activity, Proof of Burn, Proof of Capacity, and Byzantines Generals, Bytecoin, 2015. Available online: https://web.archive.org/web/20170416212233/https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison (accessed on 10 January 2018).

[12] Ren, L.; Devadas, S. Proof of space from stacked expanders. In Proceedings of the 14th International Theoryof Cryptography Conference (TCC 2016), Beijing, China, 31 October–3 November 2016; pp. 262–285.

[13] Wang,W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.;Wang, P.;Wen, Y.; Kim, D.I. A Survey on ConsensusMechanisms and Mining Strategy

Management in Blockchain Networks. IEEE Access 2019, 7, 22328–22370.[CrossRef]

[14] Szabo, N. Formalizing and Securing Relationships on Public Networks. Available online: http://ojphi.org/ojs/index.php/fm/article/view/548/469 (accessed on 10 January 2018).

[15] Wood, G. Ethereum: A secure decentralisedgeneralised transaction ledger. EthereumProj. Yellow Pap. 2014,151, 1–32.

[16] Hyperledger: Open Source blockchain Technologies. Available online: https://www.hyperledger.org/(accessed on 24 October 2019).

[17] IBM Enterprise Blockchain Solutions and Services. Available online: https://www.ibm.com/in-en/blockchain (accessed on 24 October 2019).

[18] Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.