IOT Security Issues Via Blockchain: A Review Paper

Conference Paper · March 2019

DOI: 10.1145/3320154.3320163

CITATIONS
53

READS
6,849

3 authors, including:

Abid Sultan
Dalian University of Technology
11 PUBLICATIONS **74** CITATIONS

SEE PROFILE

Muhammad Azhar Mushtaq
University of Sargodha
12 PUBLICATIONS **84** CITATIONS

SEE PROFILE

IOT Security Issues Via Blockchain: A Review Paper

Abid Sultan
Department of CS & IT
University of Sargodha, Sub-Campus Bhakkar, Pakistan
+92-453-220072
Abidsultan006@gmail.com

Muhammad Azhar Mushtaq
Department of CS & IT
University of Sargodha, Sub-Campus Bhakkar, Pakistan
+92-453-220072
Azhar.mushtaq@uos.edu.pk

Muhammad Abubakar
Department of CS & IT
University of Sargodha, Sub-Campus Bhakkar, Pakistan
+92-453-220072
Abubakar.shibly@gmail.com

ABSTRACT
In the past few years block chain has gained lot of popularity because blockchain is the core technology of bitcoin. Its utilization cases are growing in number of fields such as security of Internet of Things (IoT), banking sector, industries and medical centres. Moreover, IoT has expanded its acceptance because of its deployment in smart homes and city developments round the world. Unfortunately, IoT network devices operate on limited computing power with low storage capacity and network bandwidth. Thus, they are extra close to attacks than other end-point devices such as cell phones, tablets, or PCs. This paper focus on addressing significant security issues of IoT and maps IoT security issues in contradiction of existing solutions found in the literature. Moreover issues that are not solved after implementation of blockchain are highlighted.

CCS Concepts
• Computer systems organization → Embedded and cyber-physical systems → Embedded systems.
• Networks → Network properties → Network reliability

Keywords
Blockchain, IoT, Network Security, Data security, LLNs &POW

1. INTRODUCTION
In today's era, technologies have revolutionized the living standard of our society. This is often because of innovation in communication and semiconductor technologies, which permit devices to be connected over a network and alter the way of connectivity between machines and humans. Such a trend is usually noted as Internet-of-Things (IoT) [15].

With the fast rise of brilliant devices and high-speed networks, the IoT has gained wide acceptance and fame because it uses the standard called low-power lossy networks (LLNs). These LLNs have the potential to use the limited resource by consuming very low power [1] [2]. The devices in IoT may be controlled remotely to perform the specified function. The data sharing among the devices takes place through the network that uses the standard protocols of communication. The well-connected devices or "things" vary from easy wearable accessories to huge machines which contain detector (Sensor) chips [14].

ICBCT 2019, March 15–18, 2019, Honolulu, HI, USA

ACM ISBN 978-1-4503-6268-9/19/03…$15.00
DOI: https://doi.org/10.1145/3320154.3320163

However, as it becomes popular the connectivity between devices is increasing, and also the computing infrastructure can become additionally complicated. This complication can give a rise to vulnerabilities for the cyber-attacks. In IoT, the physical devices are placed in unsecured environments which could be defenceless from hackers thus giving them the opportunity to alter the information that transmits over the network. Therefore, device authorizations and information root would be a vital issue.

In last few years blockchain has begun as the technology that have many characteristics to solve different issues faced by IoT network devices. Blockchain keeps a distributed database of records. In which proof of work between the network nodes is completely deprived of a

third party. This will help in solving the problem of single point of failure. Network transaction records are immutable and can be founded via the history of IoT network which finally helps to get the attraction by trust of public in the IoT network. This Public trust have a vital role for the public financial transactions, introductory for a new world of distributing economy in the Internet of Things domain [8] [14] [3] [18].

The blockchain is sequences of blocks that hold all transaction record occuring in a blockchain network. As described in figure.1 each block contains block header and block body/ transaction counter. Block header contains the following;

1. **Block version** which indicates the software version and validation rules.
2. **Merkle Tree root hash** represents the hash value of the transaction and summary of all transaction.
3. **Timestamp** consists of current universal time since January 1970.
4. **N-Bits** define the number of bits required for transaction verification.
5. **Nonce** is any 4-byte number which starts from 0 and increases for every hash of the transaction.
6. **Parent block hash** holds the hash value which indicates the previous block.

Transaction counter is capable of covering all the transaction and a maximum number of the transaction depends upon the block size [12].
Blockchain technology referred as a public ledger and all completed transactions are recorded in a list of blocks. This chain of blocks grows as new blocks are added to chain continuously. Public key cryptography and distributed consensus algorithms implemented for user security. The blockchain technology has key characteristics of decentralization, persistency, anonymity, and auditability. With these characteristics, blockchain can save the cost and increases the effectiveness [12].

This paper is ordered as follows. Section 2 covers the Blockchain properties where as section 3 highlights its characteristics. Different security necessities and issues are

covered in section 4 and section 5 provides the solution of security issues using blockchain. Section 6 describes the problems that are not solved by blockchain. Finally in Section 7 conclusion and future work is presented.

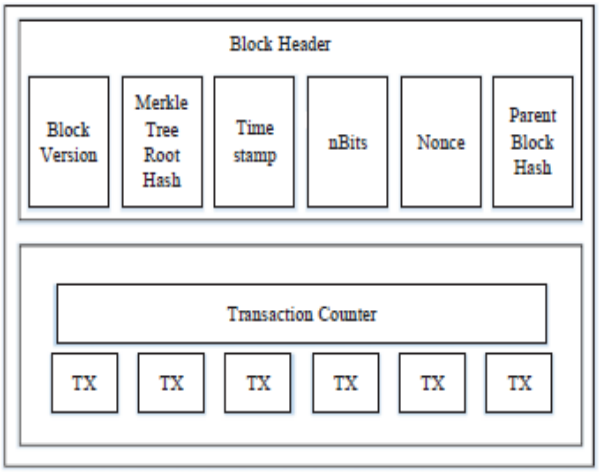

Figure 1. Block Architecture [12].

2. BLOCKCHAIN PROPERTIES

2.1. Blockchain Working Steps

1. Nodes communicate with the blockchain network via a combination of private & public keys. Theuserusesitsown private key to digitally sign its own transactions and then can access the network via the public key. Each signed transaction is broadcast by a node that makes the transaction [3].

2. The transaction is then verified by all nodes within the blockchain network except the node that makes the transaction. During this step, any invalid transactions are discarded. It's known as verification.

3. Mining is the third step in which every legitimate transaction is collected by the network nodes during a fixed time into a block and implements a proof-of-work to find a nonce for its block. Once a node finds a nonce, it broadcasts the block to all participating nodes [4].

4. Each node collects a newly generated block and confirms whether the block contains (a) legal transactions and (b) declares the accuracy of parent block by utilizing the hash value. After the completion of confirmation, nodes will add the block to the blockchain and apply the transactions to bring the blockchain up-to-date. In case, if the block is not confirmed, the projected block is rejected. This ends the existing mining round [3].

2.2. Verification

Blockchain technology ensures the elimination of the duplication issues by taking assistance from asymmetric cryptography which contains a public and a private key. The private key is kept secret from other nodes whereas the public key is shared among all other nodes [5]. Moreover, the transaction (step 1) is digitally signed by a node that creates the transaction which is broadcasted to the entire blockchain network. All receiving nodes will verify the transactions by decrypting the signature with a public key of the initializing node. The transaction is verified by the verification of signature which indicates the initializing node is not modified.

2.3. Proof-of-Work (POW)

The proof-of-work (figure 2) contains the process of finding a value that is hashed with Secure Hash Algorithm 256. The typical work needed is exponential within the variety of zero bits needed and confirmed by running the hash algorithm. In an exceeding blockchain network, all nodes implement the proof-of-work for every mining process by increase a nonce value within the block till a value is founded that offers the block's hash desired bits. Once the system unit effort has been spent to satisfy the proof-of-work, the block can't be modified until not redoing the work.

Blockchain feature distributed IoT information management can provide users the choice of sharing the information with third party entities. The target is to supply a distributed information access model for IoT, that ensures that user-data isn't assigned to centralized entities or corporations [4].

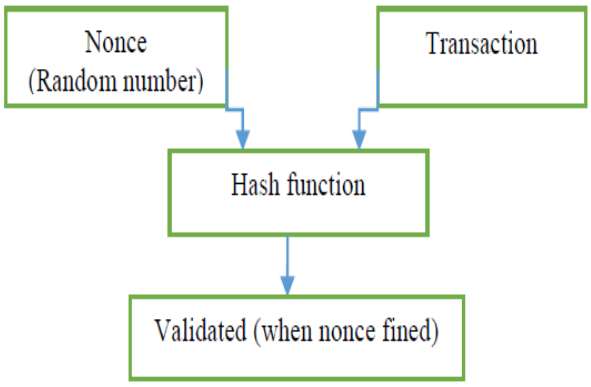

Figure 2. Proof of Work.

3. CHARACTERISTICS OF BLOCKCHAIN

3.1. Decentralization

In centralized transaction processing environment, each transaction needs to be validated through the centralized trusted party (e.g., banking system), that result into high-cost and low performance at the central point. With respect to the centralized IoT model, the third party is no longer needed in the blockchain. Consensus algorithms in blockchain are used to maintain data integrity and consistency [12].

3.2. Persistency

Once a transaction record is validated by a miner node (special nodes that validate the transaction) in a blockchain network its copy is broadcast on the entire network and that record is not deleted or rollback from entire blockchain [12].

3.3. Anonymity

In Blockchain, nodes interact with the network using a public key that addresses the node on the entire blockchain network by keeping the real identities of the user as a secret [12].

3.4. Security

Blockchain uses the asymmetric cryptographic technique to secure the entire network. Asymmetric or public key cryptography contain 2 keys one public key and second private key. **The public key** is used by the node to address the blockchain network and the **private key** is used by the node to sign the transaction that it initiates. The identity of transaction creator node is verified by using its public key.

3.5. Scalability or More Addressing Space

AS scalability is concerned blockchain contains 160-bit address space as compared to 128 bit in IPv6. These 160-bits are generated by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain has 4.3 billion more Addresses over IPv6 [8].

3.6. Resilient Backend
Every distributed node within the blockchain IOT network maintains a replica of the whole ledger. This helps in safeguarding the network form any potential failures and attacks [10].

3.7. High Efficiency
Since the transaction removes the involvement of the third party and may proceed in low-trust condition, the time spent to verify a transaction will be decreed whereas the efficiency will be increased [11].

3.8. Transparency
Changes made to public blockchain network are publicly viewable by all participants in the network. Moreover, all transactions are immutable, meaning they cannot be altered or deleted [9].

3.9. Smart Contract
The smart contract is one of the most efficient aspects of the Ethereum introduced by Nick Szabo in 1994 [7]. Using smart contract programs are written in which access rights and different policies are defined. Many programming languages are supported by Ethereum to write smart contracts such as Solidity [13].

4. SECURITY NECESSITIES FOR IOT OR ISSUES

4.1. Data Privacy
Because of a diversified integration of services and network, the data recorded on a device is vulnerable to attack by compromising nodes existing in associate IoT network. Moreover, an attacker can access the data without owner permission [14].

4.2. Data Integrity
In a centralized client-server model, the attacker may gain unauthorized access to the network and change the original data or information and forward it. For example, X sends data to Y, Z the middle guy might get data first and forward the data after modification [14].

4.3. Third Party
Data collected in a centralized environment is stored and controlled by a third centralized entity that may miss use this data or provide it to someone else.

4.4. Trusted Data Origin
In IoT environment, it is difficult to know the origin of data and data might be altered during the transmission by anyone.

4.5. Access Control
Access control is one off the main issue in IoT network. It is difficult to define in IoT network that which node has the right to access and perform a different function with data.

4.6. Single Points of Failure
Continuous growth of centralized networks for the IoT based infrastructure could expose single-points-of-failure. As all data of the entire network is stored and verified by a central authority in the case, if the central point fails or goes down the whole network is disturbed [14].

4.7. Scalability
IoT connects a large number of sensors and other devices for information sharing and a large number of applications via the internet. It challenges the structure and the rapid growth of the system to meet scalability.

4.8 Illegal use of Personal Data.
IoT device are basically sensors and implanted chips that gather individual, important information and convey it through the internet. The gathered information is stored in a central database of any firm. This data exposes the personal performance of users; confidentiality of users is at risk as firms might use the data illegally [16] [6]. An example of such confidentiality misuse is PRISM Surveillance program.

4.9 IOT Network Information Sharing.
The information gathered by IoT network devices are recorded distinctly for the purpose of analysis. Information sets may contain IoT devices network data load or their functioning logs. To confirm the efficiency of tools and tests, open accessibility of information plays a vital role. So, every time these information sets are openly shared their integrity is significant.

5. BLOCKCHAIN SOLUTIONS FOR IOT

5.1. Data Integrity
The blockchain is a peer-to-peer network in which all nodes have the same copy of records. When a transaction is initiated, initiator node signs the transaction with its private key and sends to other nodes for validation. All other miner nodes take part invalidation process and try to find nonce. The node which finds the nonce first has the right to validate and get a reward. Moreover, the newly created block will be broadcasted to all other nodes of the entire network. Once the record is loaded in blockchain it cannot be modified or deleted [10].

5.2. Data Privacy
Consortium blockchain used to provide data privacy in a blockchain network. As in figure.3,nodes used for a particular purpose are combined together to form a private network/sidechain. Each sidechain is responsible to manage its own IoT data. Nodes that are participating in one sidechain are not allowed to take part in the validation process of other sidechains. In order to access the data of consortium blockchain network the node first need to register and become part of that sidechain network. Consortium blockchain has access control and prevents unauthorized access [6].

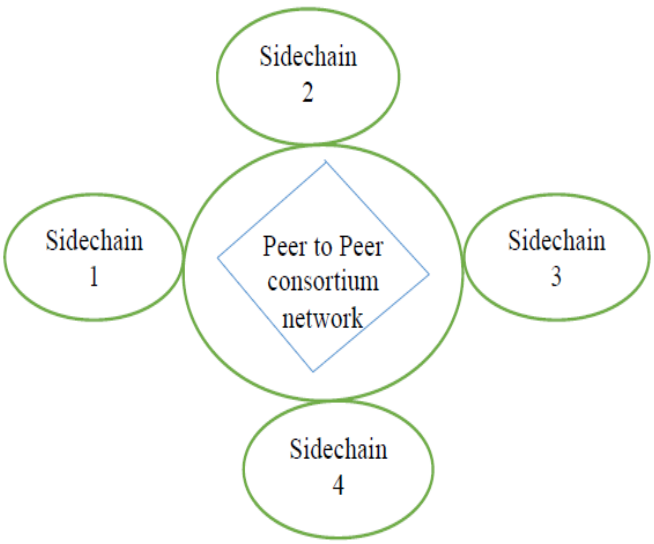

Figure 3. Consortium Blockchain Network.

5.3. Addressing Space
Blockchain contains 160-bit address space as compaired to 128 bit in IPv6. These 160-bits are generated by ECDSA (Elliptic Curve Digital Signature Algorithm). Blockchain has 4.3 billion more addresses than IPv6 thus providing more addressing spacing than IPV6 address [8].

5.4. Trusted Accountability.

Every operation record must be uploaded to the blockchain network. This gives every operation an identity and each operation is traceable. When an abnormal behaviour is detected in an entity, blockchain will be used for an additional investigation [10].

5.5. Fault Tolerance

Decentralized devices are less likely to fail accidentally because they rely on many separate components. The blockchain is a point to point decentralizing network, in it, every device has the same copy of a record that's why the failure of a single node has no effect on the network. So, blockchain prevents from a single point of failure.

5.6. Trusted Data Origin

In order to track data in the blockchain network, a unique id is assigned to each IoT device. Data collected from a device is associated with its id and after calculating a hash on data, the data is submitted to the entire network. This becomes the basis for trusted data origin [10].

5.7. Removing Third-Party Risks

Blockchain technology makes the devices capable of performing operations without the intermediary or third party, thus making it risk-free from a third party [4].

5.8. Access Control

By using smart contract, programs for blockchain can be developed in which access rights and different policies are defined. Example a rule is set when the meter reaches to 135 KW, devices will enter in energy saving mode [7].

5.9 Illegal Use of Personal Data.

Illegal use of personal data can be prohibited with the use of blockchain. As Blockchain Peer to Peer (P2P) storing systems can verify and record all actions accomplished on IoT network data [16]. The aim is to deliver decentralized storage wherever operators can have command over their data as an alternative of any centralized intermediary authority. So the privacy is more stretched to numerous levels [6] where 'Consortium blockchain' for IoTs is proposed.

5.10 IOT Network Information Sharing.

As the size of IOT network information sharing is increasing, thus the fundamental storage cost will also increase. So information sets are kept in distant origins and a centralized server is preserved which will lonely kept the references to these origins. Moreover Blockchain is used to keep RIM (Reference Integrity Matrix) of information set. As the Blockchains have Immutability feature, and accessibility of the RIM with all IoT network devices in Blockchain, ensured the Integrity of RIM. Every time an obligatory Information Set is taken from the origin, its Integrity can be confirmed by comparing its RIM being maintained on Blockchain [17].

In Table 1 characteristics of blockchain are highlighted through which problems of IoT can be tackled.

6. BLOCKCHAIN IMPLEMENTATION PROBLEMS.

Anonymity

Blockchain is a distributed network; anonymity is significant to protect privacy. Appropriately, blockchain provides pseudonymity means the users don't have a real-world ID. The users have a Public key which is used to achieve transactions on this distributed network. Using this ID a user can be found via a combination of these Ids and IP addresses related with them. Moreover, when a user uses more than one Public key it can be traced by checking whether the different addresses belong to the same user. Solution to the Anonymity is a future work [16].

7. CONCLUSION

This paper aims to present the literature review on Blockchain and Internet of Things and emphasised 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, the different properties and characteristics of the blockchain network are highlighted such order to remove the issues in IoT. Moreover issues that are not solved after implementation of blockchain are highlighted.

7.1 Future Work

We further aim 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.

Furthermore, as IoT devices are in openly reachable areas and actually below the control of an opponent, a blockchain based solution can be implemented that will assure the safety and confidentiality of the information kept in the devices. This will also address in decreasing the option of the hardware and software of an IoT device from being compromised if the device is accessible to everyone.

Table.1 IoT issues and Blockchain characteristics that solve them

IOT Issues	Blockchain Characteristics							
	Decartelization	**Persistency**	**Anonymity**	**Scalability or More Addressing Space**	**Resilient Backend**	**High efficiency**	**Transparency**	**Smart contract**
Data Privacy	✓		✓					✓
Data Integrity	✓	✓						✓
Third party	✓				✓	✓		
Trusted Data Origin	✓	✓					✓	
Access control						✓	✓	✓
Single Points of Failure	✓				✓	✓		
Scalability				✓				
Illegal use of Personal Data	✓							

8. REFERENCES

[1] L. Atzori, A. Iera and G. Morabito (2010) 'The Internet of Things: a survey', Computer Networks 54 2787–2805.

[2] D. Giusto, A. Iera, G. Morabito and L. Atzori (2014) 'The Internet of Things', 20th Tyrrhenian Workshop on Digital Communication, Springer Publishing Company, Incorporated.

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

[4] S.Nakamoto.(2008).'Bitcoin:A.PeertoPeer.electroniccashsystem,'https://bitcoin.org/bitcoin.pdf.

[5] M. Pilkington. (2016).'Blockchain technology: Principle and applications,' Research Handbook on Digital Transformations.

[6] M.S. Ali, K. Dolui and F. Antonelli, (2017) 'IoT data privacy via blockchains and IPFS' International Conference on the Internet of Things (ACM, New York).

[7] M. Gord,(2016), Smart Contracts Described by Nick Szabo 20 Years ago now becoming Reality, Bitcoin Magazine.

[8] A. M. Antonopoulos, (2014). 'Mastering Bitcoin. First Edition'. O'Reilly Media,USA.

[9] T. Chollet, J. Castiaux, M.Bruneton and L. Sainlez(2013),(2015),(2016),'Continuous interconnected supply chain using blockchain and internet of things supply chain traceability' , deloitte blockchain.

[10] X.Liang, J.Zhao, S.Shetty and, D.Li, (2017) ,'Towards data assurance and resilience in IoT using blockchain', Conference Paper.

[11] Yu Zhang and Jiangtao Wen (2015), 'An IoT electric business model based on the protocol of bitcoin'. ICIN. IEEE, pp. 184–191.

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

[13] Seyoung Huh, Sangrae Cho and Soohyung Kim (2017),'Managing IoT Devices using Blockchain Platform', ICACT2017 February 19 ~ 22.

[14] M.A. Khan and K. Salah (2017) 'IoT security: Review, blockchain solutions, and open challenges', Future GenerationComputer.Systems, https://doi.org/10.1016/j.future.2017.11.022

[15] M. Banerjee, J. Lee and K.-K.R. Choo (2017),'A blockchain future to Internet of Things security: A position paper', Digital Communications and Networks,doi: 10.1016/ j.dcan.2017.10.006.

[16] M. Conoscenti, D. Torino, A. Vetr, D. Torino, and J. C. De Martin , (2016) 'Blockchain for the Internet of Things : a Systematic Literature Review,' IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)

[17] M Banerjee, J. Lee, and K. K. R. Choo (2018). 'A Blockchain future for internet of things security: a position paper,' Digit. Commun. Networks, vol. 4, no. 3, pp. 149–160.

[18] Swan, (2015). 'Blockchain Blue Print for a new economy. First Edition' O'Reilly Media,USA.