IoT with Blockchain Technology & B-IoT Applications: Review

Ankita Mandore, SSBT's COET, Jalgaon,
Archana Shinde, SSBT's COET, Jalgaon

1. Abstract

In the Internet of Things, also commonly known as IoT, the blockchain & Peer to Peer approaches will play a very important role in the development of data intensive & decentralized applications running on billions of devices, which also preserves the privacy of users. The aim of this survey is to check if these approaches can be used for fostering a private by design & decentralized IoT. To start with, many literatures were reviewed about the blockchain technology to know about its current applications. Then, its current adaptability, degree of integrity & anonymity was documented. Many cases were found in the literature where blockchain technology was used. Four cases were found where this technology was explicitly designed for IoT. The advent of smart living spaces was also perceived to be attributed to the fast emerging of IoT. When it was combined with blockchain technology, many innovative business models can be brought into reality. This paper aims to report our recent progress in investigating the architectural issues for blockchain-driven IoT services & their applications.

2. Introduction

This technology environment brings a paradigm shift in our professional & personal life. As a connected environment, IoT adds customer value & loyalty. [8.1] Today, IoT is being implemented everywhere which is of human concern like smart city, smart environment, security, smart business process, smart agriculture, home automation & healthcare. [8.7] It's just start of Internet of Things & looking at the speed with which its progressing, we can safely say that it will become a non-avoidable part of our life. But security & privacy is still a concern. Blockchain technology is introduced to create secured Internet of Things environment. Here, we started by explaining about BC then proceeded with its applications followed by the ecosystem made up by BC technology & ended with a design to secure Internet of Things using BC. [8.2]

In this paper, we have presented about how we can adapt blockchain for specific needs of IoT for developing Blockchain based IoT (B-IoT). First, we have described the basics of blockchain, which is followed by few of the B-IoT applications in our regular life. Our sole purpose of doing this study was to emphasize how blockchain will affect traditional cloud centered IoT applications. [8.9]

2.1. IoT (Internet of Things)

IoT is now getting into maturity. We can easily observe that IoT will be the next big thing in the internet related technology. [8.6] The main question of having millions of different devices deployed across the world is "how will you handle all". There is access management technology in Internet of Things, but it is made up on the centralized model technique which gives us another type of the technical limitation to manage those devices worldwide. [8.1]

With a predicted 18 billion devices by 2022 [8.1], IoT has become a technology with large influence across many vertical markets. IoT services will provide global reach across millions of simple & sometimes tiny devices. Besides that, the constrained capabilities of many IoT devices, as well as the current access control systems based on centralized & hierarchical structures, create new challenges in the IoT domain. [8.6] Centralized access control system was designed to meet the needs of traditional human-machine oriented Internet scenarios where devices are within the same trust domain, which usually requires centralized access management. However, some IoT scenarios are much more dynamic than the traditional scenarios in which IoT devices may be mobile [8.10] & belong to various management communities during their lifetime. On the other hand, IoT devices can be managed by several managers at the same time. Moreover, many IoT devices & constrained managers will be too limited [8.11] in terms of CPU, memory & battery resources to be able to operate properly using the current systems. [8.8]

2.2. Blockchain

A blockchain technology can be define as a distributed ledger whose data are shared among a network of peers. Blockchain technology is considered as the main contribution of Bitcoin. [8.4] It is used to solved a longer-lasting financial problem known as the double-spend problem. Bitcoin provides the solution which consist in looking for the consensus of most mining nodes, who append the valid transactions to the blockchain. [8.6] Although the concept of blockchain was the very important tool for a cryptocurrency, it is not necessary to develop a cryptocurrency to use a blockchain & build decentralized applications. A blockchain is a chain of timestamped blocks that are linked by cryptographic hashes. [8.1] In order to use a blockchain, it is required to create a P2P network with all the nodes interested in making use of such a blockchain. Every node of the network receives two keys: a public key, which is used by the other users for encrypting the messages sent to a node, & a private key, which allows a node to read such messages [8.11]. In these two different keys are used that are one for encrypting & another for decrypting. In practice, to sign BC transactions, we use a private key & Public key works like a unique address. User having proper private key is only able to decrypt the messages encrypted with the corresponding public key. This is called asymmetric cryptography.

2.3. B-IoT

Since the start of Bitcoin in 2008[8.1], blockchain technology is the next revolutionary technology. Though blockchain started off as a core technology of Bitcoin, its use cases are expanding to many other areas including finances, IoT, security & such [8.12]. Now a days many private & public sectors are diving into the technology [8.13]. Aside from that, as software & hardware improve, we would see the beginning of IoT. & those IoT devices need to communicate & synchronize with each other. But in situations where more than thousands or tens of thousands of IoT devices connected, we expect that using current model of server-client may have some limitations & issues while in synchronization. [8.15] So, we propose using blockchain to build IoT system. Using blockchain, we can control & configure IoT devices. “Remote Sensing Applications public key cryptosystem” is used to handle the keys. Here, Separate device store a private key & Ethereum saves public key.

3. Related Work

The transition to a data-driven world is being accelerated by the pace of the technological advances of an Internet enabled global world, the rise of societal challenges, & an increasing competition for scarce resources. In this ecosystem, blockchain can offer to IoT a platform for distributing trusted information that defy non-collaborative organizational structures. [8.1] This review examined the state-of-the art of blockchain technologies & proposed significant scenarios for B-IoT applications in fields like healthcare, logistics, smart cities or energy management. [8.2] These B-IoT scenarios face specific technical requirements that differ from implementations involving cryptocurrencies in several aspects like energy efficiency in resource-constrained devices or the need for a specific architecture.

The aim of this work was to evaluate the practical limitations & identify areas for further research. [8.2] Moreover, it presented a holistic approach to B-IoT scenarios with a thorough study of the most relevant aspects involved in an optimized B-IoT design, like its architecture, the required cryptographic algorithms or the consensus mechanisms. [8.8]

Furthermore, some recommendations were provided with the objective of giving some guidance to future B-IoT researchers & developers on some of the issues that will have to be tackled before deploying the next generation of B-IoT applications. We can conclude that, as in any technological innovation, there is no one size fits all solution for a B-IoT application. [8.9]

4. Methodology

4.1. Determining the need for using a blockchain

Before delving into the details on how to make use of a blockchain for IoT applications, it must be emphasized that a blockchain is not always the best solution for every IoT scenario. Traditional databases or Directed Acyclic Graph (DAG) based ledgers may be a better for certain IoT applications. Particularly, in order to determine that the use of a blockchain is suitable, a developer should make a decision if the following characteristics are necessary for an IoT application: Decentralization. IoT applications demand decentralization when there is not a trusted centralized system. However, many users still trust blindly certain companies, government agencies or banks, so if there is mutual trust, a blockchain is not required. P2P exchanges. Within IoT nearly all conversations go from nodes to gateways that route data to a remote server or cloud. Communications among peers at a node level are actually not very common, except for specific applications, like in intelligent swarms or in mist computing systems. There exist some additional examples that bring up conversation together with nodes at the identical level, as it happens in fog computing with local gateways. Payment system. Some IoT applications may need to achieve economic transactions in company of third parties, yet many applications do not. Moreover, economic transactions can still be carried out through traditional payment systems, although they usually imply to pay transaction fees & it is necessary to trust banks or middlemen. Public sequential transaction logging. Many IoT networks collect data that need to be timestamped & stored sequentially.

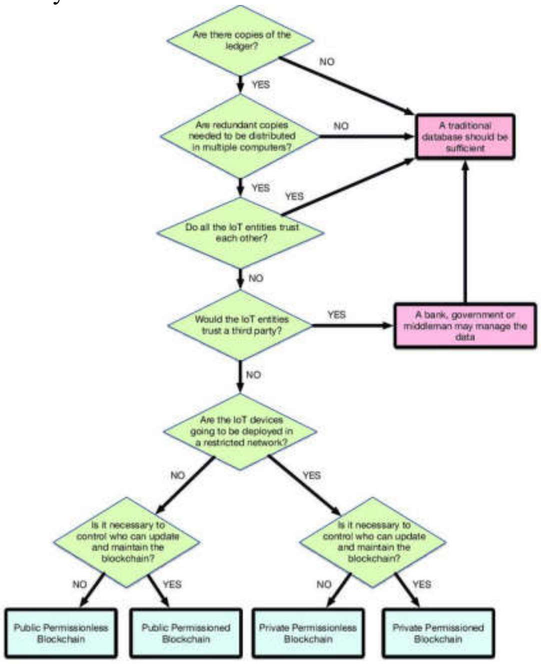
Are there copies of the ledger?
NO
YES
Are redundant copies needed to be distributed in multiple computers?
NO
A traditional database should be sufficient
YES
YES
Do all the IoT entities trust each other?
NO
Would the IoT entities trust a third party?
YES
A bank, government or middleman may manage the data
NO
Are the IoT devices going to be deployed in a restricted network?
NO
YES
Is it necessary to control who can update and maintain the blockchain?
Is it necessary to control who can update and maintain the blockchain?
NO
YES
NO
YES
Public Permissionless Blockchain
Public Permissioned Blockchain
Private Permissionless Blockchain
Private Permissioned Blockchain

Figure 1: A Generic Flow Diagram to find the type of Blockchain depending on the characteristics of IoT system.[8.8]

4.2. Overview of the decentralized access control system in IoT

The architecture proposed in this paper describes a new decentralized access management system where access control information is stored & distributed using blockchain technology. All the entities will be part of blockchain technology except for IoT devices & management hub nodes. Nodes in a blockchain network must include a copy of the blockchain. The blockchain can be considerably large in size & will keep increasing over time. The majority of IoT devices will not be able to store blockchain information due to their constrained nature. Consequently, our architecture does not include IoT devices in the blockchain and, alternatively, defines a new node called management hub that requests access control information from the blockchain on behalf of the IoT devices. In addition to that, the solution involves a single smart contract that defines all the operations allowed in the access control system. That contract is unique & cannot be deleted from the system. Entities called managers interact with the smart contract in order to define the access control policy of the system.

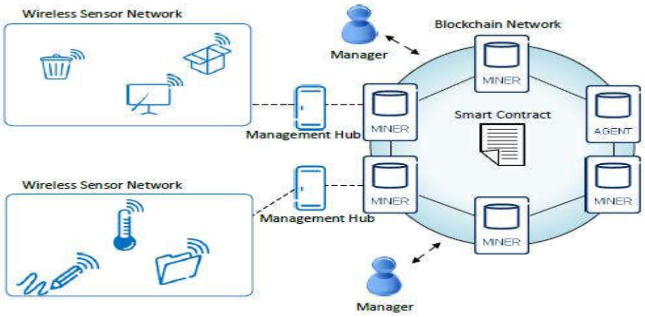

Figure 2: Decentralized Access Control System[8.1]

4.3. System Architecture

The architecture of our system is as shown in Figure 2. The architecture is divided into six different components as explained below one by one:

4.3.1. Wireless Sensor Networks:

A wireless sensor network is a communication network that allows constrained connectivity in applications with limited power & light requirements. Further, the IoT devices belonging to the wireless sensor network are limited in their computational power, memory, and/or energy availability. IoT devices do not belong to the blockchain network.

4.3.2. Managers:

A manager is an entity responsible for managing the access control permissions of a set of IoT devices. Normally, managers are considered lightweight nodes in our system. Lightweight nodes do not store the blockchain information or verify the blockchain's transactions as the miner nodes do. As a result, constrained devices can also become managers in our system without representing an impediment to their hardware limitations.

4.3.3. Agent Node:

The agent node is a specific blockchain node in our architecture responsible to deploy the only smart contract in our system. The agent node is the owner of the smart contract during the lifetime of the access control system. Once the smart contract is accepted into the blockchain network, the agent node receives an address that identifies the smart contract inside the blockchain network. In order to interact with the smart contract, all the nodes in the blockchain network need to know that smart contract's address.

4.3.4. Smart Contract:

The access management system described in this paper is governed by the operations defined in a single smart contract. This smart contract is unique & cannot be deleted from the system. Hence, all the operations allowed in the access management system are defined in the smart contract & are triggered by blockchain transactions. The smart contract & its operations are also globally accessible. In addition to that, it has to be taken into consideration that managers are the only entities with the ability to interact with the smart contract in order to define new policies in the system.

4.3.5. Blockchain Network:

The blockchain network in our architecture is a private blockchain for the sake of simplicity. We chose a private blockchain since all the elements of the prototype are more dimensioned, providing us more reliable results when evaluating the system.

4.3.6. Management Hubs:

As mentioned before, IoT devices do not belong to the blockchain network. The majority of IoT devices are very constrained in terms of CPU, memory & battery. Those limitations restrict IoT devices to be part of the blockchain network. Being part of the blockchain network implies keeping a copy of the blockchain locally & a track of the network transactions..

4.4. B-IoT Applications

4.4.1. Smart Cities

In smart cities, different types of electronic equipment are used for different applications. For example; in monitoring system, cameras are used. In transportation system, sensors are used. We can find many such applications in day to day life. Unknowingly, people are already using it. In the reference no. [8.15], the author has presented about how a potential smart city will look like in 2020 & some of its features. Different aspects of a smart city include smart energy, smart citizens, smart mobility, smart buildings, smart healthcare, smart technology, smart governance, smart infrastructure & smart security & finally the education. In the following image, we have shown features of smart cities:

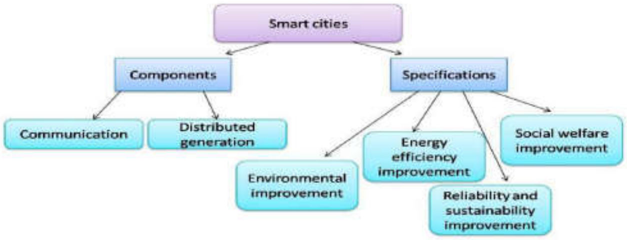
Smart cities
Components
Specifications
Communication
Distributed generation
Environmental improvement
Energy efficiency improvement
Reliability and sustainability improvement
Social welfare improvement

Figure 3: Key Aspects of Smart Cities

4.4.1.1. Internet of Things for Smart Cities

The Internet of Things means a network employing the standard communication protocols as mentioned in reference numbers 8.16 & 8.17. Internet is its convergence point. Most important notion of Internet of Things is that most of the objects are measurable & smart. Smart means they can modify the situation as per their logic. Internet of Things is also empowered by the expansion of communication equipment like mobile phones. It also includes other facilities like appliances, landmarks & foodstuff [8.18, 8.19]. They together are able to collaborate for achieving some joint objective. Most important characteristic of Internet of Things is 'effect of IoT on the life of a consumer.' [8.15]. As a next step, communication between different sensors ought to be wireless as its very costly to connect millions of sensors through cabling.

4.4.2.Smart Home

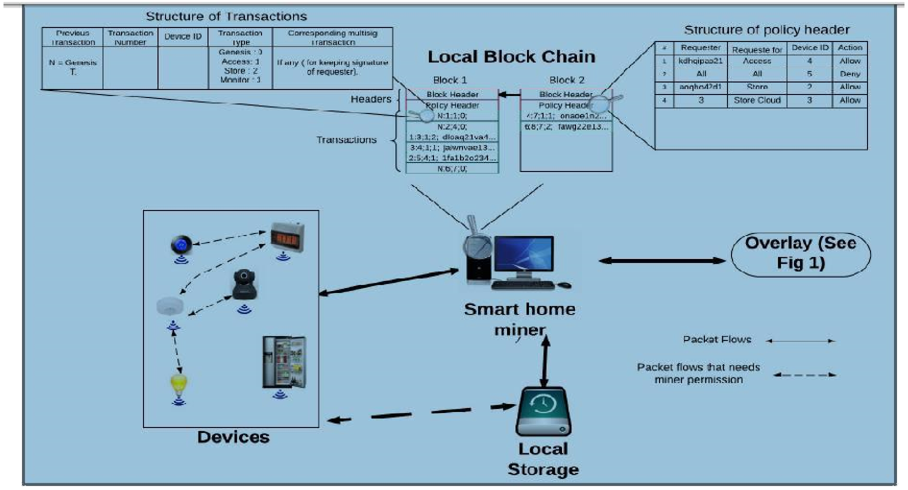

Figure 4: Overview of the Smart home

4.4.2.1. Initialization

Here, we described steps for of adding policy header & devices to the local Blockchain. While adding any device in a smart home, miner creates a genesis transaction. It shares a key with the device it is connecting to with the use of generalized "Diffie Hellman" [8.10]. It stores the key shared between the device & miner in the genesis transaction. For defining the policy header; home-owner generates own policies as per the proposed policy structure, shown in Figure 4 as above. The policy header is then added to the first block.

4.4.2.2. Transaction Handling

A smart device has the ability to communicate directly with no deviation with entities out of smart home & also with each other. Every single device inside the home may ask data from a further internal device to be present with a service. For example, motion sensor provides data to a bulb when somebody enters the home & then bulb turns on the lights automatically. For accomplishing user control over smart home transactions, miner assigns a shared key to the devices which then interact to other devices. While allocating a key, either policy header is checked by miner or owner‘s permission is taken. After that, the shared key is distributed by the miner between different devices so that they can interact within themselves.

4.4.2.3. Shared overlay

If a person has two or more homes, then home-owner is required to have different storage & miners. In such a case, we can define a shared overlay. It helps in cost reduction as well as optimizes overheads. It consists of more than one smart home which homeowner can handle like a single home only.

5. Discussion

Our research indicates that this technology is already being used in a systematic approach. Most of the big MNCs are already using this technology to produce the superior output. The interesting part of this technology is that the designing options are more & set protocols as compared to it are very less. This technology is now allowing to use Internet of Things in practice. A pilot project is run initially to check for the unpredictability, if any in this technology. This helps in taking proper precautions well before time & do modifications in the technology if needed. This will help in the mass use of IoT in the future. BC-based architecture incurs computational & packet overhead on the smart home devices & the miner for providing improved security & privacy [8.13]. For comparing overheads of architectures based on the blockchain, a different scenario was simulated which handles the transactions with no hashing, blockchain & encryption. It is known as “base method”. 3 z1 mote sensors were simulated. Home miner directly received the data from those z1 mote sensors. Every simulation ran for 3 min. Final result was calculated as the average of all results over time.

6. Future Work

It is very clear that new technology of Internet of Things is benefitting the smart cities. It will be foolish to deny the applications of IoT in smart cities. The main objective of us for this review was to study different features & specifications of this technology. We also studied about how we can incentivize the use of IoT so that people start using it. The accomplishment of the Internet of Things substructures will create loads of opportunities in smart cities in near future.

7. Conclusion

We can conclude that, as in any technological innovation, there is no one size fit all solution for a B-IoT application. Nevertheless, the adoption of this technology opens a wide area of applications that could disrupt the industry & probably, the economy. Different components related to a smart home & a smart city were reviewed in this research. Different processes in relation to it were discussed. Its privacy & security related research was also discussed in this paper.

8. References

8.1. Oscar Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT”, Journal of internet of things class files, vol. 14, no. 8, march 2018

8.2. Ali Dorri, Salil S. Kanhere, Raja Jurdaky & Praveen Gauravaramz, “Blockchain for IoT Security & Privacy: The Case Study of a Smart Home”, 2ND IEEE PERCOM Workshop on Security Privacy & Trust in The Internet of Things 2017

8.3. Saber Talari I, Miadreza Shafie Khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti & João P. S. Catalão, “A Review of Smart Cities Based on the Internet of Things Concept”

8.4. Marco Conoscenti Antonio, Vetr`o Juan Carlos & De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review” 978-1-5090-4320-0/16/$31.00 ©2016 IEEE

8.5. Jie Lin, Wei Yuy, Nan Zhangz, Xinyu Yang, Hanlin Zhangx & Wei Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security & Privacy & Applications” 2327-4662 (c) 2016 IEEE.

8.6. Jyotiranjan Hota1 & Pritish Kumar Sinha, “Scope & challenges of Internet of Things: An Emerging Technological Innovation”, 978-1-4799-8433-6/15 IEEE

8.7. Madhusudan Singh, Abhiraj Singh & Shiho Kim, “Blockchain: A Game Changer for Securing IoT Data”

8.8. Tiago M. Fernández, Caramés Paula Fraga, Lamas, “A Review on the Use of Blockchain for the Internet of Things” vol. 6, 2018

8.9. X. Sun & N. Ansari, Edgeiot, “Mobile edge computing for the internet of things”, IEEE Communications Magazine, vol. 54, no. 12, pp. 22–29, December 2016.

8.10. X. Sun & N. Ansari, “Dynamic resource caching in the IoT application layer for smart cities”, IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2017.

8.11. Everis Next, “17 Blockchain Disruptive Use Cases”, 02 June 2016. Web. 03 Jan. 2017.

8.12. A. Shelkovnikov, “Blockchain applications in the public sector”, Deloitte, 2016

8.13. “Strategic Opportunity Analysis of the Global Smart City Market.”, Available online: http://www.egr.msu.edu/~aesc310web/resources/SmartCities/Smart%20City%20Market%20Report%202.pdf (accessed on 24 February 2017).

8.14. Atzori L.; Iera A.; Morabito G., “The Internet of Things: A survey.”, 2010, 54, 2787 2805.

8.15. Internet of Things in 2020: Roadmap for the Future. Available online: http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_ECEPoSS_Workshop_Report_2008_v3.pdf (accessed on 24 February 2017).

8.16. Six Technologies with Potential Impacts on US Interests Out to 2025. Available online: https://fas.org/irp/nic/disruptive.pdf (accessed on 24 February 2017).

8.17. Alamri A.; AnsariW. S.; Hassan M. M.; Hossain M. S.; Alelaiwi A.; Hossain M. A., “A Survey on Sensor-Cloud: Architecture, Applications, & Approaches.”, 2013, 9, 917923.