Blockchain for IoT Application: Challenges and Issues

M.Padma, N. KasiViswanath, T.Swathi

Abstract--- Since from the last decade, Blockchain technology has developed a new crypto-economy and has been converting the financial industry. Reliability, persistence, scalability, the power of enduring is factors of an IoT solution. On the other hand, Blockchain is an experimental and investigational type of technology, and not proven. Blockchain burns up and then face the problems while IoT solutions, once deployed, are handled for years. The main motivational ideas i.e. decentralized trust and distributed record are capable of distributed and the large-scale Internet of Things (IoT) applications. Moreover, in this domain, the uses of Blockchain beyond crypto-currencies are very less and far due to the lack of acceptance and integral framework challenges. In this paper, we illustrate the opportunities for uses of Blockchain of IoT and study the concern challenges and issues in Blockchain based IoT applications.

Index Terms-Blockchain Technology, Internet of Things (IoT), crypto-economy.

1. INTRODUCTION

Blockchain can be seen as a distributed database of transactions communicated by each company on the network. Blockchain technology is expressed in bit coin - a digital currency, made and managed world-wide. The use of Blockchain technology in the IoT can lead to many innovations and solve the problem of trust and compliance in a connected world. We can work with a wide range of connected devices. Many of these may have first-time interactions, such as a home automation device, such as a security signal, and be integrated with various devices from different manufacturers.

IoT is a huge ecosystem that will play. Thousands of manufacturers generate billions and billions of connected devices, multiple platforms, multiple connectivity options and, of course, many Blockchain entries in multiple geographies to complete the life of the device. The real challenge is not the technology, but the mutual recognition of the IoT ecosystem, its use and government initiatives to create the Blockchain regional registry. After use, it can also assist in other uses, such as security and compliance, such as devices that cannot be exceeded by geographical limits. There are lots of challenges around authenticity in this simple use case and everything in the end boils down to trust between the devices and who maintains that trust.

This paper illustrations Blockchain assertions for the IoT and describes Blockchain problems and limitations by correlating IoT architectural elements with Blockchain. Besides, the paper analyses key design issues for application developers who develop and implement programs among the Blockchain and IoT applications.

2. BLOCKCHAIN FRAMEWORK

IoT applications are air quality control, smart cities, supply chain management and production line monitoring. The Internet is a combination of computer, communication, detection and execution functions, and all these features are distributed over the network. The IoT

Final Component Layer: Last component layer consists of sensors, integrated low-power platforms, wireless Communication technologies and power supplies. The low-power platform of integrated IoT serves as a sensor center and one or more wireless technologies. IoT platforms are usually provided for those environments which are very difficult to access the data. It is therefore important that the component last longer in the battery or a recovery condition. The IETF defines components in this layer as a very limited projector with limited processing and storage capabilities, known as Class 0 components. The end layer of the component is a layer with limited architectural resources IoT applications.

Figure 1. The framework of the Internet-of-Things applications

Edge-component Layer: Component layer has the function of collecting data from the terminal sensor. This layer consists of a network gateway, in which incoming and outgoing communications form the last component layer. In addition, in this layer, many parameter data would be the same as real-time application requirements. The components of this layer are best suited for the operation, access and storage of components at the end of the track.

Server or backend layer: The role of the cloud-back-end server is to store and visualize functionalities. An IoT application's end user creates an infrastructure network that allows you to Access information. Web servers, databases, data analysis engines used in databases, are available on

Revised Manuscript Received on February 22, 2019.

M.Padma, Assistant Professor, CSE Dept., GPREC, Kurnool, AP, India

Dr. N. KasiViswanath, Professor, HOD, CSE Dept., GPREC, Kurnool, AP, India

T.Swathi, Assistant Professor, CSE Dept., GPREC, Kurnool, AP, India

websites. The components which are used at these highest levels maintain maximum processing and storage capabilities in the stack.

3. OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY

This section describes the most important aspects of Blockchain technology.

Cryptographic Digital Signature: In order to generate a signature for Blockchain transactions, Public key cryptography is mainly deployed by Blockchain. Accusers' engage in transactions digitally by login with their private key. Information of the Blockchain network verifies the transaction using the user's public key to ensure that the sender has signed the transaction. Initial components or components that stop recording record transactions when they make a deal.

Distributed Ledger: Blockchain uses shared storage to maintain information of transactions. All network platforms keep complete transactions or a subset of operations. All nodes in the network reach a consensus (using a consensus algorithm) before transactions are recorded in the main ledger, which makes the flowchart remain constant.

Consensus algorithm: To execute transactions, Blockchain does not depend on centralized servers. Instead, Blockchain uses the client-server model, and all network decisions are made by users using a consensus protocol.

3.1 Principles of Blockchain Technology

Distributed Database: in this section access each party without an intermediary can directly check their trading partner data.

Peer-to-Peer Transmission: Transmission has been made directly among peers, not through the central node. Each node stores information and sends it to all other nodes.

Transparency: All transactions and related value are noticeable to everyone who has access to the System. Every user in the Blockchain has a unique alphanumeric address representing more than 30 characters.

Irreversibility of Records

As soon as the transaction has been committed and the accounts are updated, the records cannot be altered or modified as they relate to all the transaction records that were before them. Many algorithms and IT procedures are applied to ensure that the record in the database is permanent, arranged in chronological order and accessible to all network users.

Table 1. Shows the Components of Blockchain.

Full node	• Validate Transactions and blocks • Strictly follow the rules of the Blockchain framework • Maintain the copy of Blockchain
Light Node	• Verify transactions without downloading the complete Blockchain • Downloads only header of the blocks • Uses simplified payment verification(SPV) for verification
Hardware Wallet	• Holds the Private and Public keys • Implement algorithm to generate digital signature and perform transactions

4. OPPORTUNITIES

In this section, we will describe the Possibilities to use the technology of Blockchain technology in the Internet of Things.

• **Privacy/anonymity:** Blockchain transactions using the digital identity generated by public key cryptography and the hash algorithm. IoT applications with confidential information can use this mechanism to hide the true identity of the network.

• **Exchange of information and calculation of money:** exchange of financial and computer data: use of intelligent city sensors related to crowds for providing digital services to city residents. Money can be essential for attracting members of the community to smart cities and applications to use advanced resources.

• **Registration of accounts for accounts and audits:** IoT data applications are transported using an infrastructure belonging to different organizations. Supply chain monitoring focuses on tracking and monitoring resources all over the supply chain.

• **Smart agreement:** Nick Szabo presented the concept of a smart contract [2] as an alternative to conventional paper contracts. The contract is an intelligent digital system built into the system, which is executed if the contractual conditions of the contract are met. A mediation contract for smart, autonomous transactions between the parties to exchange assets or unreliable work with members of a blockbuster network. For example, IoT applications can use intelligent sensor data transport with those that belong to multiple parts and the data that the sensors are supposed to sell.

5. CHALLENGES AND ISSUES

5.1 Challenges of Blockchain in IoT

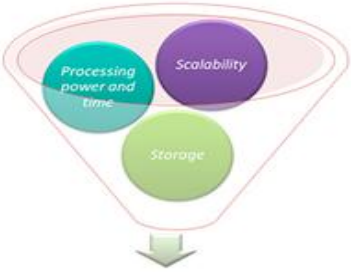

Figure 2. Challenges of Blockchain n IoT

Scalability Issues: The size of the Blockchain registry, which over time can increase centralization, and require some archival management that blocks Block chain's future technology [9].

Power and processing time: It is necessary to implement encryption algorithms for all objects involved in Blockchain IoT ecosystem because IOT ecosystems are very different and offer very different peripheral computing capabilities, and all of them will not be identical. You can run encryption algorithms at the desired speed.

Storage will be an obstacle: Blockchain eliminates the need for a central server to store transactions and device

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IDs, but the main ledger must be stored in the nodes themselves, and the lead ledger will increase over time. It goes beyond the capacity of many smart devices, such as a sensor with very low storage capacity.

5.2 Risk in IoT Using Blockchain

We are currently discussing issues that arise when applying the IoT blockbuster.

Figure 3 : Risk in IoT Using Blockchain

Vendor Risks: The Blockchain-as-a-Service (BaaS) Market is Still Rising; The Company must carefully choose a vendor who can perfectly build applications that properly address the risks associated with the blockbuster.

Security Credentials: Most current systems do not offer multi-factor authentication. In addition, losing your account private keys may result in loss of funds or data from this account. This risk should be carefully evaluated.

Legal and Compliance Principle: This has no legal precedent or agreement, which pretenses serious problems to IOT producers and service providers.

• **Resource Constraints:** IoT platforms have very few resources to compute exchange and store resource information, but Blockchain needs a lot of resources. Low power class IoTs require less than 10KB of data memory and less than 100 KB of program memory [3], but the Blockchain node requires GB of data memory. [4] In addition, numerical requirements for consistency algorithms, such as job testing, far outweigh the capacity of IoT components that are limited by low power sources. Therefore, current Blockchain technologies are not suitable for low-power IoT components due to their resource requirements. In Figure 1, terminal components and components fail to run Blockchain processes, and the server layer is ideal for current Blockchain technologies. Such an approach could combine the centralized deployment of IoT with a decentralized Blockchain set because the IoT deployment server layer acts as an access point for the block circuit network.

• **Bandwidth Requirements:** Blockchain platforms need to be integrated with other platforms on the network to participate in the consensus process. As the consensus process is decentralized, network platforms exchange information about the kiosk's success in order to check the transaction and create new blocks. IOT components running in the last component layer have strict bandwidth limits, which also mean that the current solutions are not suitable for the final components. Edge components and servers may have sufficient bandwidth, but it's important to keep in mind that bandwidth requirements in the chart may exceed the program bandwidth requirements of their own, with fewer resources in the current protocol circuits.

• **Security:** Blockchain technology is consistent with decentralised architecture, in which all network components work together and interact with predefined protocols. Therefore, components remain connected to the block network to participate in the consensus process, and always connected function makes IoT components more reliable to security and privacy attacks.

• **Transaction Cost:**Typically, blockade technologies used include transaction costs and are used to provide nodes in the consolidation process. The IoT component cannot contain all data from multiple blocks, since the data storage costs in the block are deducted. If you want to put IoT component data in this block, you may need to add this to reduce transaction costs, but in this case it's important to make sure that the aggregation process does not delete the transaction costs. Relevant information. On the other hand, architecture can be used as data that is transmitted outside Blockchain, and important business records are passed for testing purposes and in the source circuit.

• **Permission Vs Public:** Modern block diagram technologies can be classified as public block diagrams and can be divided into two categories. Public locking circuits like Bitcoin and Ethereum allow anyone to join the network without permission [6]. Anyone who wants to take part can simply download and install the required frames. This type of block technology requires particular resources for a consensual process. Allowed block strings consist of authorized network members. Therefore may be this type of Blockchain suitable for IoT applications connecting to the number of well-known organizations, as there are authorized members on the network that offers the ability to reach a quick consensus protocol and better performance.

6. CONCLUSION

This research review's purpose is to help the reader to understand a different aspect of Blockchain technology, which had a prominent impact on cryptographic currency applications. Supply Chain and IoT monitoring applications, these are promising basic structures of blocking technologies. In this paper we have discussed the framework of the Internet-of-Things applications. Then we offered the option of applying Blockchain IoT. Furthermore we have presented several Research challenges and Opportunities of Blockchain in IoT.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
2. N. Szabo, "Smart contracts," Unpublished manuscript, 1994.

3. C. Bormann, M. Ersue, and A. Keranen, "Terminology for constrained-node networks," Internet Requests for Comments, RFC Editor, RFC 7228, May 2014, http://www.rfc-editor.org/rfc/rfc7228. Txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7228.txt
4. (2018) Running a full node. https://bitcoin.org/en/full-node# minimum-requirements.
5. T. Project. [Online]. Available: https://www.torproject.org/.
6. de Montjoye, Yves-Alexandre, et al., "openpds: Protecting the privacy of metadata through safeanswers," PloS one 9.7 (2014).
7. Jøsang, Audun, and Jochen Haller., "Dirichlet reputation systems," in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on., 2007.
8. https://datafloq.com/read/iot-and-blockchain-challenges-and-risks/3797
9. http://naveenbalani.com/index.php/2016/07/blockchain-and-enterprise-iot/.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication