RESEARCH ARTICLE OPEN ACCESS

Block Chain & Internet of Things: Security, Challenges, Research Issues

D.Salma Faroze
Department of Computer Science and Engineering
CBIT College Proddatur, And Pallavolu
Andhra Pradesh - India

ABSTRACT
Blockchain, the foundation of Bitcoin, has received extensive attentions recently. It serves as an immutable ledger which allows transactions take place in a decentralized manner. Each block contains a timestamp and a link to a previous block. By design and by purpose blockchains are inherently resistant to modification of the data. Although there are some studies on the security and privacy issues of blockchain, there lacks a systematic examination on the security of blockchain systems. However, this emerging technology has a great potential in the most diverse technological areas and can significantly help achieve the Internet of Things view in different aspects, increasing the capacity of decentralization, facilitating interactions, enabling new transaction models, and allowing autonomous coordination of the devices.

Keywords:- Bitcoin, Timestap, Decentralized, BlockChain

I. INTRODUCTION

The aim at providing consistency criteria to capture the correct behavior of current blockchain proposals in a unified framework. Security solutions and privacy should be implemented according to characteristics of heterogeneous IoT devices. The technology can be used to authenticate, authorize, and audit data generated by devices. It has an ability to establish new foundations for both economic and social systems. Blockchain is named that way because it is basically an endless chain of blocks. Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service, or transaction.

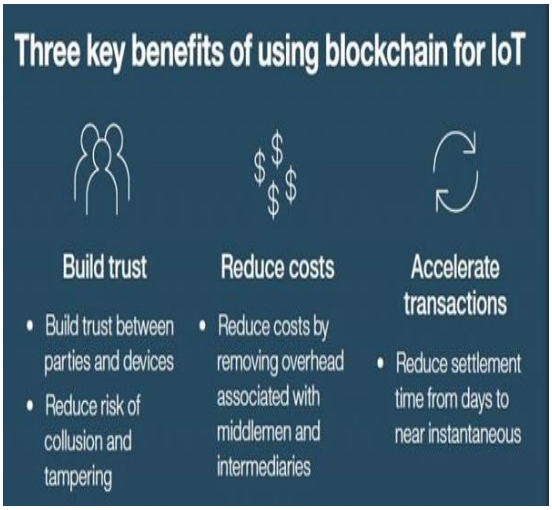
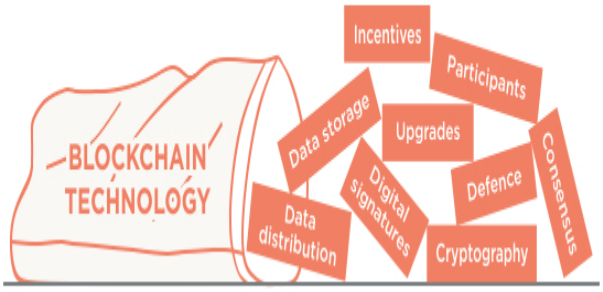


Fig: Introduction to BlockChain



II.SCOPE AND OBJECTIVES

The study analyzes its principles of work, technical specifications and features of Blockchain, as well as identifies economic, social and technical implication provided by the technology.In the scope of blockchain and IoT it's interesting to look at the combination of blockchain and the Internet of Things as it's used in insurance and will increasingly be, moving beyond the pure telematics model to the

connection of real-time IoT data in various perspectives for various intelligent automated insurance policy applications. This could be for security and control reasons with ongoing optimization, predictive maintenance improvements and AI-enabled ways to further enhance the decision-making while enabling again new applications when, for instance combined with digital twins.

Fig: Block Chain Using IOT

III. OVERVIEW OF BLOCKCHAIN & IOT

Internet-of-Things comprises of computation, communication, sensing, and actuation functionalities, and such functionalities are distributed throughout the network. The Blockchain technology uses the combination of cryptography, a consensus algorithm, and a distributed ledger to create a decentralized and trustworthy platform. **IoT**—the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.**Blockchain**—an encrypted, distributed computer filing system designed to allow the creation of tamper-proof, real-time records. The combination of the Internet-of-Things and blockchain technology has enormous potential to change many of the processes we all rely on today, but when combined, have even greater potential.The security issues with regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management. We outline security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions.

BlockChain	**IoT**
Resource Consuming	Mostly devices are resource restricted
Block mining is time consuming	Demands low latency
BlockChain scale poorly with large networks	IoT is expected to contain a large number of nodes
BlockChain has high bandwidth consumption	IoT devices have limited bandwidth and resources

Table: Differences of Blockchain and IOT

IV. CHALLENEGS BASED ON BLOCKCHAIN AND IOT

A decentralized consensus mechanism may offer myriad benefits are information neutrality, authenticity, fault tolerance, security, etc. To support and operate with the blockchain, network peers have to provide, the following functionality: routing, storage, wallet services and mining. Storage capacity and scalability have been deeply questioned in blockchain. In this technology, the chain is always growing, at a rate of 1MB per block every 10 min in Bitcoin, and there arecopies stored among nodes in the network. The IoT is transforming and optimizing manual processes to make them part of the digital era, obtaining volumes of data that provides knowledge at unheard of levels. This knowledge is facilitating the development of smart applications such as the improvement of the management and the quality of life of citizens through the digitization of services in the cities.
Currently, any failure in an IoT ecosystem exposes multiple devices, huge amounts of highly personal data (for example, smart home devices have access to intimate details about our lives and daily routines), supply chain partners and the community as a whole. Such security flaws typically revolve around three areas: authentication, connection, and transaction. Devices that verify, connect or spend improperly with other devices are all major concerns.

V. ARCHITECTURE

Blockchain technology can be used in tracking billions of connected devices, enable the processing of transactions and coordination between devices; allow for significant savings to IoT industry manufacturers. This decentralised approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on. The cryptographic algorithms used by blockchains, would make consumer data more private. In this paper, we propose a new architecture for arbitrating roles and permissions in IoT. The new architecture is a fully distributed access control system for IoT based on blockchain technology. The architecture is backed by a proof of concept implementation and evaluated in realistic IoT

scenarios. The approach was exemplified in a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home. In this paper we delve deeper and outline the various core components and functions of the smart home tier. Each smart home is equipped with an always online, high resource device, known as "miner" that is responsible for handling all communication within and external to the home. A typical smart home setting where a user, Alice has equipped her home with a number of IoT devices including a smart thermostat, smart bulbs, an IP camera and several other sensors. The proposed architecture shown includes three tiers, namely the smart home (or more generally the local network), the overlay network, and the cloud storage. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains.

VI . LIMITATIONS AND BENEFITS

Due to the security reasons, this program was made in such a way that any block or even a transaction that adds to the chain cannot be edited which ultimately provides a very high range of security. The blockchain is a giant, distributed computer. Miners provide network security. The format of Blockchain designs in such a way that it can easily locate any problem and correct if there is any. It also creates an irreversible audit trail. As per the studies as an average cost of the Bitcoin transaction is $75-$160 and most of this cost is covered by the energy consumption. There are very fewer chances that this issue can be resolved by the advancement in the technologyThe consumption of power in the Blockchain is comparatively high as in a particular year the power consumption of Bitcoin miners was alone more than the per capita power consumption of 159 individual countries. Keeping a real-time ledger is one of the reasons for this consumption because every time it creates a new node, it communicates with each and every other node at the same time.

VII. SECURITY

Blockchain technology follows a decen-tralized architecture, wherein all the devices in the network coordinate and cooperate with each other through pre-defined protocols. Thus, the devices stay connected to the blockchain network for participat-ing in the consensus process. This always-connected feature makes IoT devices potentially more susceptible to security attacks. Blockchain technology is highly secure because of the reason each and every individual who enters into the Blockchain network is provided with a unique identity which is linked to his account. This ensures that the owner of the account himself is operating the transactions.

VIII. CONCLUSION

the state-of-the-art of existing blockchain protocols designed for Internet of Things (IoT) networks. We provided an overview of the application domains of blockchain technologies in IoT, e.g., Internet of Vehicles, Internet of Energy, Internet of Cloud, and

Fog computing. Through extensive research and analysis that was conducted, we were able to classify the threat models that are considered by the blockchain protocols in IoT networks, into five main categories, namely, identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks.

IX. FUTURE WORK

IoT technology will play an increasingly important role in our society for the foreseeable future, in both civilian and military (adversarial) contexts, including the Internet of Drones, Internet of Battlefield Things and Internet of Military Things. Not surprisingly, IoT security is a topic of ongoing research interest. A great mention towards Blockchain has been recently devoted by

both researchers and companies, due to its high applicative power, mainly relying on the idea that Blockchain can implement a public, shared ledger without dedicating any trusted entity.

REFRENCES

[1] .F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Commun. Surveys & Tut., vol. 18, no. 3, pp. 2084–2123, Mar. 2016.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] D. Wilson and G. Ateniese, “From pretty good to great: Enhancing PGP using bitcoin and the blockchain,” in Network and System Security. Springer International Publishing, 2015, pp. 368–375

[4] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved on December 1, 2017 from the website https://bitcoin.org/bitcoin.pdf

[5] Nick Szabo. Smart Contracts, 1994. Retrieved on 2nd November from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[6] Konstantinos Christidis, and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, vol.

[7] A. Ukil, S. Bandyopadhyay and A. Pal, "IoT-Privacy: To be private or not to be private," in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on., Toronto, 2014.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [8] Decker, Christian, Jochen Seidel, and Roger Wattenhofer., "Bitcoin Meets Strong Consistency.".

[9] J. Buchmann, "Introduction to cryptography.," Springer Science & Business Media, 2013. [10] T. Project. [Online]. Available: https://www.torproject.org/. [11] de Montjoye, Yves-Alexandre, et al. , "openpds: Protecting the privacy of metadata through safeanswers," PloS one 9.7 (2014)..