International Journal of Scientific & Engineering Research Volume 10, Issue 3, March-2019
ISSN 2229-5518

A study on the use of block chaining in internet of things

Author : Parvathy Viswanath

Asst. Professor, CCST for Women, Karalmanna, Palakkad

ABSTRACT: The internet of things is a system of interrelated computing devices, mechanical and digital machines and people that are provided with unique identifiers and the ability to transfer data over a network without requiring any interactions. A block chain is a distributed technology that was majorly associated with bitcoins and they form a chain of blocks. Every block contains information and data packed together which are also verified. The blocks are then validated and added to the chain in previous blocks. These block chains can be associated with internet of things in order to ensure authentication, data privacy and maintenance. This paper includes a study on how the capability of block chaining is made use in IoT in order to ensure high security and robustness against attacks.

Keywords: cryptocurrency ,integrity,cryptography .Internet of things(IoT)

1.Introduction

As IoT is growing day by day, it is essential to build a proper set of protocols, architecture and enhanced security mechanisms. Now a day's IoT completely rely on client server paradigm connecting cloud servers through internet. When we use block chain technology along with IoT, we are able to track, coordinate, carry out transactions and store information from a large amount of devices, enabling the creation of applications that require no centralized cloud.

When block chain technology was used in bitcoin, there was no distinction between the terms and those two were used interchangeably. As new technologies were introduced, a variety of uses for block chaining was also introduced .Block chaining was experimented in different uses like peer-to –peer aspect to deliver messages.

The cryptocurrencies those used block chaining revolutionized the electronic payments. In the case of a cryptocurrency, the blockchain acts as a account that stores all transactions that have been performed. This means that the blockchain grows continuously by adding new blocks every certain time intervals. Every node owns a copy of the whole blockchain, which also contains information about user addresses and balances. IoT and cryptocurrencies share common properties since in an IoT system there are many entities that do not trust each other during transactions.Those advantages of block chaining can be made use in IoT.

This paper includes the study on how block chaining is carried out, how it can be

implemented in IoT and the shortcomings and challenges of current BIoT applications.

2.How block chaining is carried out?

To use a blockchain, a Peer toPeer network should be created and a method of asymmetric cryptography is performed for transactions. Block chaining can be distinguished as public and private. In public blockchains anyone can join the blockchain without the approval of third-parties where as in private blockchains, the owner will restrict network usage. Many private blockchains are also permissioned in order to control which users can perform transactions, carry out smart contracts.

3.Properties of blockchaining

3.1 Decentralization-A global network of computers uses blockchain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one central authority. Decentralization means the network operates on a user-to-user basis.

3.2 P2P exchange-In IoT most communications go from nodes to gateways that route data to a remote server or cloud but block chaining make use of peer to peer communication.

3.3 Payment system-Payment system doesnot require any third parties as this can enhance the security feature as well.

3.4 Transparent and incorrupatble-Transparency data is there in the network , as by definition it is public.It cannot be corrupted by altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

3.5 Time-stamping - Timestamping is the process of securely keeping track of the creation and modification time of a document. It allows interested parties to know, without a doubt, that a document in question existed at a particular date and time. In blockchain, every block is time-stamped making it.

3.6 Cryptography - Bitcoin uses Elliptic Curve Cryptography - which means that the Network can verify that a transaction was sent by the person who holds the private key without them revealing their identity.

4. Adapting block chaining in iot

Apart from cryptocurrencies and smart contracts, blockchain technologies can be applied in different areas where IoT applications are involved like sensing , data storage , identity management, timestamping services, mobile crowd sensing , cyber law and security in mission-critical scenarios . Block chain can also be used in IoT agricultural applications. The system is

based on the use of Radio Frequency Identification (RFID) and a blockchain to enhance food safety and quality. Apart from all these, IoT devices can be managed through a blockchain [2]. Such researches proposed a system able to control and configure IoT devices remotely.

IoT security can also be enhanced by block chain technology. It can be improved remote attestation. This verification can be performed by managing the TCB measurements obtained by using ARM TrustZone [3] and a blockchain, where they are stored securely.

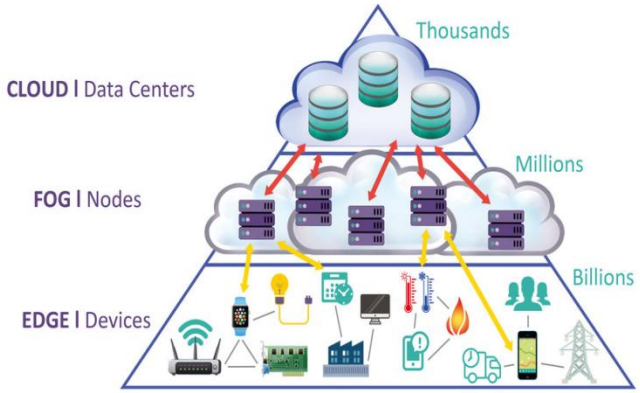
Blockchain technologies provide many benefits to IoT, but, since they are exclusively created for it, advantageous portions of it should be adapted.Inorder to use them, several researchers introduced BIoT performance in different scenarios.Many characteristics were checked but more concise algorithms were taken under consideration.

Earlier IoT was working under cloud platform but there were some short comings like when the cloud is down , it may affect the whole system.As the whole set of systems are connected to each other, even if a single IoT device is affected, it may lead the whole network to go down due to Denial of Service (DoS)[11] attacks or by eavesdropping private data .

But when we adapt blockchain in IoT, it do not rely upon any central server or cloud and all transactions done through it is verified by using cryptographic techniques.

Block chaining can be used in IoT by using different architectures.A multilayer architecture was discussed in ‘‘A blockchain based new secure multi-layer network model for Internet of Things” prepared by C. Li and L.-J. Zhang.In this architecture,IoT ecosystem can be divided in to levels and we can can use block chainin in each one. By the use of this architecture , it gives the power of cloud and security of block chaining.

“Block chain as a service for IoT”, written by M.Samaniego and R.Deters discussed a different approach where BloT applications used the cloud as well as fog computing architecture .Other architecture was introduced which was based on edge computing which supports distribution automation control systems. These systems can have a two layered architecture where the bottom layer can control the devices connected in IoT and the layer on the top will supervise the bottom layer.



Another architecture made use of software defined network[10] inorder to improve network performance and monitoring. This architecture combines cloud and fog

computing .Cloud is used to perform computation tasks and datas are accessed through fog computing. Different architecture introduced by different authors reduced the delay and improved throughput and security in IoT network

5.Algorithms used for cryptography in Iot

RSA algorithm is slow and power consuming[8] when it is used in IoT devices. RSAcan be combined with Elliptic Curve Diffie-Hellman Exchange[9], recommended by the National Institute of Standards and Technology for Transport Layer Security . A 2048-bit key is the minimum size considered for high security.Apart from RSA algorithms, we have to use hash functions.These hash functions are also key in a blockchain-based system, since they are required to sign transactions. Therefore, hash functions for IoT applications should be fast and secure. The most popular blockchain hash functions is SHA-256d.

Inorder to track modifications on the blockchain,transactions have to be both signed and timestamped. So it may require timestamping server as well. One of the recently proposed system is the use of a decentralized timestamping service or the distribution of its keys .

6. Privacy and security

Every user in block chain is identified by either public key or hash .It is possible for third parties to analyze such transactions and infer the actual identities of the participants. Inorder to solve some challenges a use of permissioned block chain for securing and managing multiple IoT nodes is proposed by D. W. Kravitz and J. Cooper,it provides a distributed identity management solution .It increases the security and protection against attacks by symmetric key rotation and those keys are locally on the device and they are never moved from it. But as we are rotating keys, identity verification comes more important .For that a mechanism called Device Group Membership can be employed. In this mechanism it groups all devices handled by a user together and when the user carries out a transaction , it will be reflected on the block chain as it is performed by a device that belonged to the user's group.

A different approach that which can enhance the security and privacy by providing automatic authentication systems for IoT applications where scalability is needed and where device heterogeneity and mobility are common. Privacy can be enhanced by mixing different techniques .While considering security ,three things have to be taken care of. They are confidentiality, integrity and availability. Confidentiality management can be carried out by taking care of private and public keys. With respect to integrity , it must be indicated that the foundations of a blockchain are designed to store information that cannot be modified. Another characteristic of security is availability as block chaining is designed to be distributed systems and it allows to work even when some nodes are under attack.

7.Conclusion

This paper included the advantages of using block chaining in Iot but there are some drawbacks like

Adoption rate-Sudden adoption of BIoT applications are not possible because users or devices are identified by addresses, but they are not linked to them. But later governments may demand a strong link between real-world and online identity. This can lead to disadvantage to the system.

Usability-Every application developed with block chain should have a user friendly interface otherwise that can be a bigger disadvantage.

Mining boycott –Miners may not be able to decide whether a transactions is present in the block chain or not. Therefore, miners have to be chosen wisely and, when smart contracts have been signed, misbehaviors should be sanctioned

Smart contract enforcement and autonomy-There are no legal rules implemented inorder to enforce smart contracts and to resolve the disputes properly.

BIoT is still in it's dawning stage so inorder to broader the use we require additional technological research advances to address all those growing demands.

References:

[1] A Review on the Use of Blockchain for the Internet of Things

TIAGO M. FERNÁNDEZ-CARAMÉS , (Senior Member, IEEE), and PAULA FRAGA-LAMAS , (Member, IEEE)

[2] ''Managing IoT devices using blockchain platform,'' by S. Huh, S. Cho, and S. Kim, in Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT), Bongpyeong, South Korea, Feb. 2017, pp. 464–467.

[3] ARM TrustZone. Accessed: Apr. 10, 2018. [Online]. Available: https://www.arm.com/products/security-on-arm/trustzone

[4] ''Securing user identity and transactions symbiotically: IoT meets blockchain,'' by D. W. Kravitz and J. Cooper, in Proc. Global Internet Things Summit (GIoTS), Geneva, Switzerland, Jun. 2017, pp. 1–6

[5] "Block chain as a service for IoT", written by M.Samaniego and R.Deters

[6] ''A blockchain based new secure multi-layer network model for Internet of Things" prepared by C. Li and L.-J. Zhang

[7] ''Use of honeypots for mitigating DoS attacks targeted on IoT networks,'' by M. Anirudh, S. A. Thileeban, and D. J. Nallathambi in Proc. Int. Conf.

Comput.,Commun.SignalProcess.(ICCCSP), Chennai,India,Jan.2017, pp. 1–4.

[8] ‘‘A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications,’’by] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo Sensors, vol. 17, no. 9, p. 1978, Aug. 2017.

[9] NIST.Accessed:Apr.10,2018.[Online].Available:https://www.nist.gov

[10] ‘‘Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing,’’ by K. Dolui and S. K. Datta, in Proc. GlobalInternetThingsSummit(GIoTS),Geneva,Switzerland,Jun.2017, pp. 1–6.

[11],‘‘Use of honeypots for mitigating DoS attacks targeted on IoT networks,’’ by M. Anirudh, S. A. Thileeban, and D. J. Nallathambi in Proc. Int. Conf. Comput.,Commun.SignalProcess.(ICCCSP), Chennai,India,Jan.2017, pp. 1–4.