SECURITY AND PRIVACY SOLUTIONS BASED ON BLOCKCHAIN FOR INTERNET OF THINGS(IOT)

[1.]LINGAM GAJJELA,[2.]D.SRINIVAS,[3.]K.BHARATH KUMAR
[1.]ASSISTANT PROFESSOR,[2.] ASSISTANT PROFESSOR,[3.] ASSISTANT PROFESSOR
[1,2,3] COMPUTER SCIENCE AND ENGINEERING
[1,2,3] NARSIMHAREDDY ENGINEERING COLLEGE,MAISAMMA GUDA,HYDERABAD

ABSTRACT

The most popular problem solving technology in recent years is Blockchain Technology. It solves most of the issues in banking sectors industry zones in recent years because of its features and reliability and services. It is creating new opportunities and providing a competitive advantage for business in current and new markets. IoT generate, collect and produce huge data, due to this it face security and privacy issues, for services and potential data. Blockchain has provide services to IoT solutions by creating applications to solve the security and privacy issues. 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 decentralization capacity, facilitates interactions, it enables new transaction models, and allowing autonomous coordination of the devices. This Paper intention is to provides the structure of blockchain and its operation, it also analyze the use of blockchain and explain how it provides security and privacy in IoT

Key Terms: Blockchain,Decentralization,Cryptosystem

1. INTRODUCTION

Block Chain is a Thriving list of records, called blocks, which are linked using cryptography.The Block contains timestamp of the previous block cryptographic hash code and transaction data like merkele tree root hash.The design of a blockchain is resistant to modification of the data. BlockChain can record two parties transctions in efficiently and in a verifieable and permanat way by using DISTRIBUTED LEDGER. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol,a blockchain for inter-node communication and validating new blocks.Once recorded ,the data in any given block cannot be alterd retoactively without alternation of all subsequent blocks,which requires consensus of the network majority. Although blockchain records are not altarable,blockchain may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.Decentralized consensus has therefore been claimed with a blockchain. Blockchain Technology was introduced in 2008 by Satoshi Nakamoto to serve as the public transction ledger of the cryptocurrency bitcon.The invention of the blockchain for bitcoin made it the first digital

currency to solve the double-spending problem without the need of a central sever or trusted authority.The bitcoin design has inspired other applications,and blockchain which are readable by the public are widely used by cryptocurrencies.Blockchain is considered a type of payment rail private blockchains have been proposed for business use.Sources such as the computer world called the marketing of such blockchains without proper security model snake oil.

2. BLOCKCHAIN STRUCTURE

Blockchain is public ledger, decentralized and distributed and it is used records many computers transactions so that any involved record cannot be altered retrospective, without any alteration of subsequent blocks. It verifies allowed participants audit transactions individually and relatively inexpensively. The blockchain database is managed autonomously using distributed time stamping and peer-to-peer network. They are authenticated by mass collaboration powered by collective self interests. Such a design facilitates robust workflow where participants uncertainty regarding data security is marginal.

2.1 Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain linking the two.

2.2 Blocktime

The blocktime is the average time it takes for the network to generate one extra block in the blockchain. Some blockchain create a new block as frequently as every five seconds.By the time of block completion,the included data becomes verifiable.

2.3 Hardforks

A hard fork is a rule cahnge such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid.

2.4 Decentralization

The decentralized blockchain use ad-hoc message passing and distributed networking.Peer-to-Peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit. likewise,it has no central point of failure. Blockchain security methods include the use of publickey cryptography Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. Messages are delivered on a best effort basis. Mining nodes validate transactions, add them to block they are building and then broadcast the completed block to other nodes.Blockchain use various time stamping schemes ,such as proof of work , to serialize changes.

2.5 Openness

Open blockchain are more user friendly , which , while open to the public, still require physical access to view.

2.6 Permissionless

Blockchain network is that guarding against bad actors is not required and no access control is needed.Directly the applications can be added to the network without approval. Bitcoin and other cryptocurrencies currently secure their blockchain by requiring new entries to include a proof of work.

2.7 Pemissioned

Permissioned blockchain use an access control layer to govern who has access to the network.

3. HOW BLOCKCHAIN WORKS?

The main working processes of blockchain are as follows:

1) The sending node records new data and broad casting to network.
2) The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block.
3) All receiving node in the network execute proof of work (PoW) or proof of stake (PoS) algorithm to the block.
4) The block will be stored into the chain after execut-ing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block.

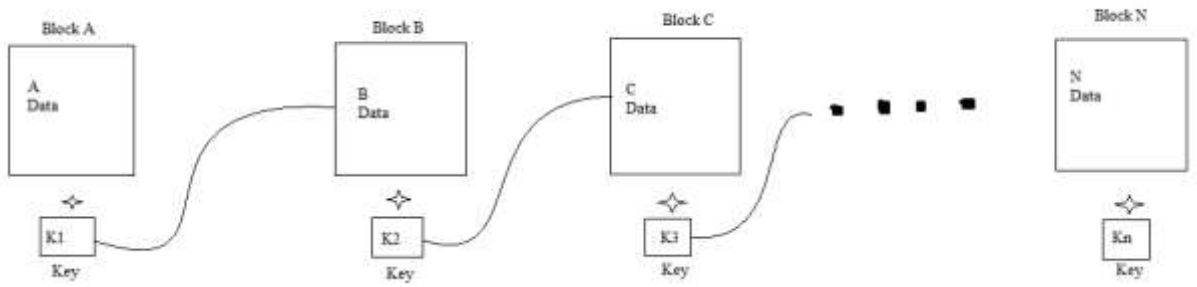


Fig: Working Model of Blockchain Technology

3.1.The Structure of Blockchain

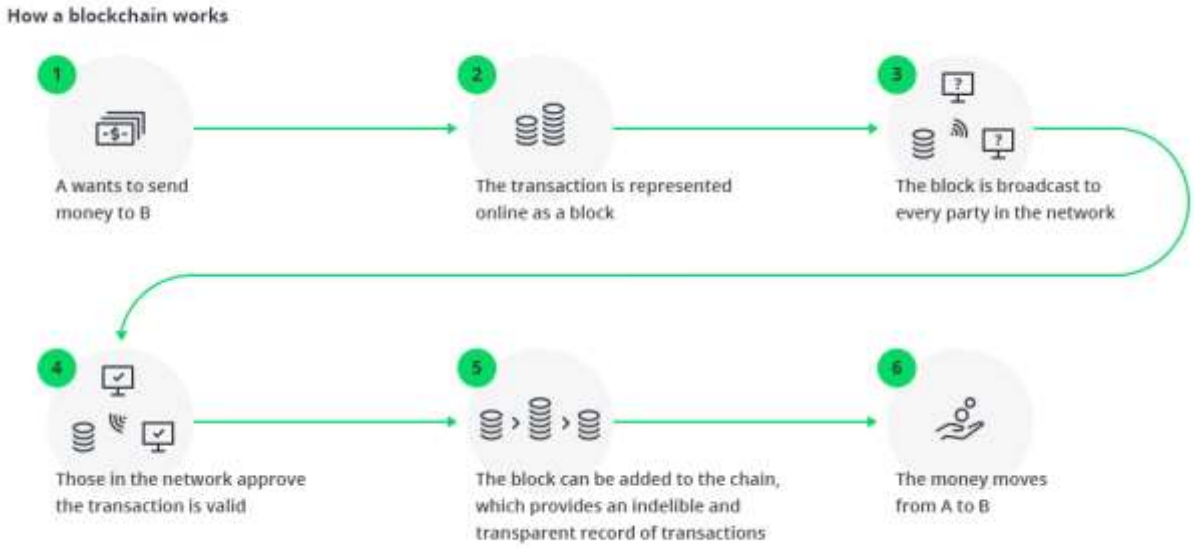
Generally in the block, it contains main data, hash of pre-vious block, hash of current block, timestamp and other information. Figure 1 shows the structure of block.

Main data: Depending on what service is this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record.

Hash: When a transaction executed, it had been hash to a code and then broadcast to each node. Be-cause it could be contained thousands of transaction records in each node's block, blockchain used Merkle tree function to generate a nal hash value, which is also Merkle tree root. This nal hash value will be record in block header (hash of current block), by using Merkle tree function, data transmission and computing resources can be drastically reduced.

Timestamp: Time of block generated.

Othe r Information: Like signature of the block, Nonce value, or other data that user done.



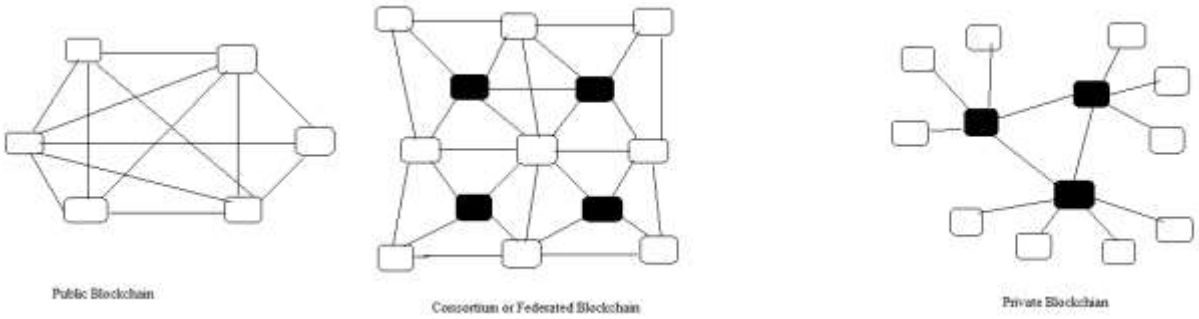
4. TYPES OF BLOCKCHAIN

There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.

1. Public Blockchain: Is the blockchain of the public.Here no one is in charge and anyone can participate in reading/writing/auditing the blockchain. Another thing is that these types of blockchain are open and transparent hence anyone can review anything at a given point of time on a public blockchain. Example Bitcoin, Litecoin

2. Private Blockchain: Is a private property of an individual or an organization.Unlike public blockchain here there is an in charge who looks after of important things such as read/write or whom to selectively give access to read or vice versa.Here the consensus is achieved on the whims of the central in-charge who can give mining rights to anyone or not give at all.

3. Consortium Blockchain: It means the node that had authority can be choose in advance, usually has partnerships like business tobusiness, the data in blockchain can be open or private, can be seen as Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains. Figure 3 shows consortium blockchains.



5. APPLICATIONS

Blockchain technology can be integrated into multiple areas.

5.1 Digital identity

Blockchains provide an opportunity to establish a strong system for digital identity. Because it is not based on accounts and permissions associated with accounts, it is a push transaction, and ownership of private keys is ownership of the digital asset, this places a new and secure way to manage identity in the digital world that avoids exposing users to sharing too much vulnerable personal information.

5.2 Tokenization

For the purposes of authenticating a unique physical item, the items are paired with a corresponding digital token. This essentially means tokens are used as to bind the physical and digital worlds. These digital tokens are useful for supply chain management, intellectual property, and anti-counterfeiting and fraud detection.

5.3 Inter-organizational data management

Blockchain technology represents a revolution in how information is gathered and collected. It is less about maintaining a database, more about managing a system of record.

5.4 For governments

Governments have an interest in all three aspects components of blockchain technology.
Firstly, there's the ownership rights surrounding cryptographic key possession, revocation, generation, replacement, or loss.

5.5 Cryptocurrencies

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are blockchain-based.

5.6 Smart contracts

Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is automated escrow. An IMF staff discussion reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general. But "no viable smart contract systems have yet emerged." Due to the lack of widespread use their legal status is unclear.

5.7 Banks

Major portions of the financial industry are implementing distributed ledgers for use in banking, and according to a September 2016 IBM study, this is occurring faster than expected.

Banks are interested in this technology because it has potential to speed up back office settlement systems.

5.8 Blockchain with video games

Blockchain technology is also develop video games are ex: *Huntercoin* Cryptokitties Robot Cache

6.CHALLENGES TO SECURE IoT DEPLOYMENTS

Internet of Things ecosystem— device manufacturer, solution provider, cloud provider, systems integrator, or service provider—you need to know how to get the greatest benefit from this new technology that offers such highly diverse and rapidly changing opportunities. Handling the enormous volume of existing and projected data is daunting.

The Problem with the Current Centralized Model

To perform the functions of traditional IoT solutions without a centralized control, any decentralized approach must support three fundamental functions:

- Peer-to-peer messaging
- Distributed file sharing
- Autonomous device coordination

Blockchain technology is the missing link to settle scalability, privacy, and reliability concerns in the Internet of Things. Blockchain technologies could perhaps be the silver bullet needed by the IoT industry. 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 decentralized 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.

The ledger is tamper-proof and cannot be manipulated by malicious actors because it doesn't exist in any single location, and man-in-the-middle attacks cannot be staged because there is no single thread of communication that can be intercepted. The decentralized, autonomous, and trustless capabilities of the blockchain make it an ideal component to become a fundamental element of IoT solutions. In an IoT network, the blockchain can keep an immutable record of the history of smart devices. This feature enables the autonomous functioning of smart devices without the need for centralized authority. As a result, the blockchain opens the door to a series of IoT scenarios that were remarkably difficult, or even impossible to implement without it.

In this model, the blockchain will treat message exchanges between devices similar to financial transactions in a bitcoin network. To enable message exchanges, devices will leverage smart contracts which then model the agreement between the two parties.Using the blockchain will enable true autonomous smart devices that can exchange data, or even execute financial transactions, without the need of a centralized broker. This type of autonomy is possible because the nodes in the blockchain network will verify the validity of the transaction without relying on a centralized authority.One of the most exciting capabilities of the blockchain is the ability to maintain a duly decentralized, trusted ledger of all transactions occurring in a network. This capability is essential to enable the many compliance and regulatory requirements of industrial IoTapplications without the need to rely on a centralized model.

7 . CONCLUSION

In recent days, everywhere observing the IoT devices for communication in different applications. Uses in IoT devices Security playing crucial role. IoT security paying a lot of attention from both Industry and Academics. In present, the existing solutions for IoT security were not good enough and suitable. Because It Consume very high energy and large processing time,So these two factors are overhead for IoT security.In order to find the best solution for IoT security we use Blockchain (BC) technology. In blockchain, blocks are use to store the data for particular IoT device. The block will maintain the Database-Ledger. It work on the distributed network. The government have to make corresponding laws for this technology, and enterprise should ready for embrace blockchain technologies, preventing it brings too much im-pact to current system.When we enjoy in the advantage of blockchain technologies bring to us, in the same time, we still have to stay cautious on its influence and security issues that it could be have.

8. REFERENCES

[1] J.Bonneau,A.Miller,J.Clark,A.Kroll, and E.W.Felten, sok:Research perspectives and challanges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy,pp.104{121,May 2015}

[2] A.Chakravorty, T.Wlodarczyk and C.Rong,"Privacy preserving data analytics for smarthomes in Securitry and Privasy workshops(SPW),2013 IEEE.IEEE,2013,pp.23-27.

[3] S.Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." 2008

[4] S.King,"Primecoin: Cryptocurrency with prime number proo-of-work," july 7th,2013.

[5] A. Dorri, S.S .Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and solutions,"

[6] A. Narayanan, J Bonneau, E. Felten, A.Miller , and S.Goldfeder ,Bitcoin and cryptocurrency technologies. Princeton University Pres,2016

[7] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Cap-cum,\Tampering with the delivery of blocks and transctions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Commumications security(CC'15),pp.692{705,New York,NY,USA,2015.

[8] E. Heilman, A .Kendler,A. Zohar and S. Goldberg, \Eclipse attacks on bitcoin's peer-to-peer network," in 24th USENIX Security Smposium,pp. 129{144, Washington, D.C.,2015

[9] G. Karame ,\On the security and scalability of bit-coins blockchain," in Proceedings of ACM SIGSAC conference on computer and communications Security(CCS'16),pp.1861 {1862.New York ,NY,USA,2016.

[10] S. King and S. Nadal, PPcoin: Peer-to-Peer Crypto-Currency with proof-of-stak,2012