SURVEY ON BLOCKCHAIN TECHNOLOGY IN COLLABORATION WITH CLOUD PLATFORM

[1]Sushmitha M.S, [2]Sanjay H.M
[1]PG Research Scholar, [2]Assistant Professor
[1]Department of CSE,
[1]PES College of Engineering, Mandya, India

Abstract : Blockchain was invented in order to serve as the publicly auditable ledger of the cryptocurreny bitcoin. It acts as a financial tool that plays a major role in development of global economy. It has emerged as a backbone of new type of internet by the distribution of digital information. It was originally designed for the digital currency, bitcoin. Along with this, blockchain technology has provided the path to digitalize all the activities through cloud. Blockchain also provides security in the network via authentication of peers, generation of hash table and encryption. This article presents the survey on blockchain technology with advantages, disadvantages, collaboration of cloud with blockchain and its challenges.

IndexTerms **- Blockchain, Cryptocurrency, Bitcoin, Digital currency, Cloud.**

I. INTRODUCTION

Blockchain technology is a type of open distributed ledger that is used to register the transactions that take place between two participants. Each block consists of hash table of the previous block, transaction data and timestamp. To validate new blocks and to promote inter node communication, blockchain manages peer to peer network. Data contained in every block cannot be altered without altering later blocks. They are authenticated based on self interest. Each Block in blockchain contains valid data transaction which is encoded into hash tree. Each block contains previous block hash function helps in linking the two blocks. This linkage of blocks results in a chain. This repetitive process shows the integration of current and previous block. Blockchains are typically built by the addition of new blocks onto the older one instead of overwriting the old one. Since blockchain is decentarlized, it uses ad-hoc network for message passing. Since blockchain provides high rate of security, there is a continuous research on blockchain for secure communication only between peers and not involving third parties. Due to openness attribute, it gives clarity about the data which can be revealed when needed for the applications. Due to these pros, they can be applied in financial and ICT computational environment like computational cloud. Cloud computing provides developers to use virtual resources infinitely with an option of pay per use and when needed and avoids the industry to invest much more capital on resources. Once the applications are launched on resources of cloud, users can access those applications from anywhere and anytime using mobile devices and desktop machines. Data centre provides resources, virtual centralization of applications and data. There is not yet been a secure solution to host large applications even cloud computing helps in optimize the usage of resource. In next section we discuss about generic model and blockchain network characteristics.

II. ORIGIN OF BLOCKCHAIN

As mentioned above, blockchain technology is a decentralized, distributed open ledger used to register the transactions that are grouped into blocks. Each block (current block) is linked to other block (previous block) after validation and consensus decision. While authenticating transactions, single point of failure caused by third party has overcome. Blockchain model provides many features of P2P model. This model provides high security standards and faster transactions since they are automated and accepted by multiple agents. Transactions can be made publicly accessible since it reduces the cost of security related tasks and thus hackers find difficult to exploit vulnerabilities of the system. Following figure (1) shows the basic components of blockchain P2P architerture.

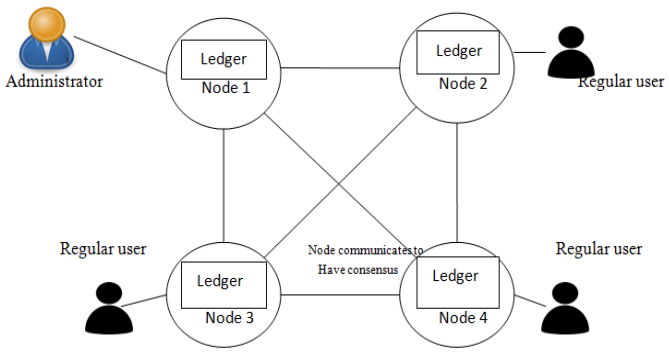

Fig 1: Blockchain distributed architecture

2.1 Hash Function

Hash functions play a major role in blockchain model. These functions are used in encrypting the data contained in the block. With the use of hashing process, almost all the input which is in the form of text or images of any size is processed. The main aim of hashing process is to compute unique static sized output called 'message digest'. Based on input, corresponding message digest output is generated. Two inputs cannot generate identical output and hence hash algorithm is a collision resistant.

The fast computing Secure Hash Algorithm with an output size of 256 bits (SHA-256) is widely used algorithm in blockchain model.

2.2 Ledger

Ledger consists of set of transactions. Each node consists of local copy of this set of transactions called the ledger. In the same way blockchain consists of set of nodes. Swapping of services and products are stored historically in ledgers. In large centralized database, ledgers are replaced by records with the use of new computing methods. These records are produced by a group of users who assign the operation of such databases to trusted external agents who actually owns the data and ledgers. However this centralized ledger has few cons:

i. The centralized agent suffers from single point of failure of the entire system which means the user needs a backup system in case of failure or loss.
ii. Central third party agent should validate each and every committed transaction and hence validity is monitored by owner and all the users must trust the owner.
iii. Even if some transactions are lost due to failure, all users must believe the central agent about the completion of ledger. However third party trusted agents and industry do backup transactions based on their and users interest, validate committed data including valid transaction.

2.3 The Blocks

Every node present in blockchain may obtain transaction performed by the participants. These transactions are the transferred into other nodes in the blockchain network. The committed transactions wait in the queue of transaction pool until all the transactions are added to the block chain network. This updating of nodes is performed by the mining nodes and thus a block contains valid transactions. Invalid transactions are rejected in block chain. The participant who started the transaction should cryptographically sign the transaction to guarantee its legality which indicates that each of them have access to private key. Hash table is generated when a block is created (518 digest- blocks). A minute change in input data results in a large change in hash table. In order to ensure security in block chain, each node's hash table is shared among every other node in the network.

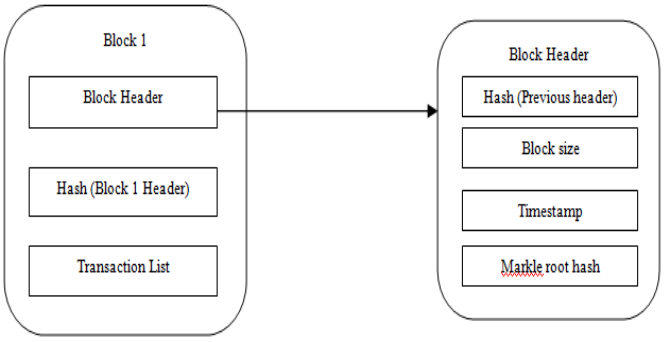

Fig 2: Model of a block

Each block in block chain consists of following components:
(i) Block height
(ii)Current block hash value
(iii)Previous block hash value
(iv)Markel root hash table
(v)Timestamp
(vi)Block size
(vii)A list of transactions

Markel tree is a data structure which is used to store hash value. Markel tree root hash consists of group of data present in Markel tree. Validity of the data or transaction is verified using this root. Figure 3 shows the representation of Markel tree

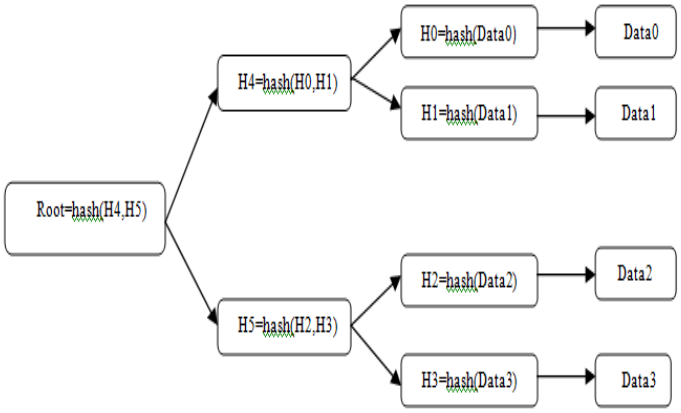

Fig 3. Markel tree

2.4 Blockchain Operation

Each node present in the block chain is owned by several organizations. The nodes in the network may communicate with each other and coordination among nodes and validation of all transactions does not require any authority. Several algorithms were used to solve the problem of consensus. The participant sends a transaction requests to block chain network to perform desired operation. As a result, one or multiple ledgers register each transaction and these transactions cannot be modified and thus immutability of block chain is achieved.

2.5 Security in Blockchain

Asymmetric key cryptography is most popular cryptographic method used in block chain network. This cryptographic model consists of a pair of public and private key which is used for signing the transactions and verifying the signatures. This process is carried out as explained below:

(i)Transaction digital signature is generated with help of private key.

(ii)Verification of signature generated by private key is done with the help of public key.

As the name itself suggests, public key is known to many participants who doesn't affect to security of the system and private key is known only to key owner. Asymmetric key cryptography assures that with the help of public key, private key cannot be determined.

III. CLOUD PLATFORM AND BLOCKCHAIN COLLABORATION

Cloud computing consists of huge range of virtualized services like hardware resources and software resources. Hardware resources comprises of CPU, network and storage. Software resources comprises of databases, load balancers message queuing system. These virtualized services are termed as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud services are launched in data farms (data centres). Cloud platform is divided into three types based on security and privacy issue, resource and data management. They are (i) Public cloud (ii) Private cloud and (iii) Hybrid cloud. Public data does not assure for the protection of user's data but provides unlimited access to data and resources. Private cloud is owned by organization and assures for data protection and only authorized and authenticated users are allowed to access resources. Hybrid cloud is the integration at upper level public cloud of many private clouds providers into a combined global infrastructure. The main problem in this model is to attain an agreement private cloud providers to work under compact public cloud standard. Thus distributed private cloud providers which are connected using standard P2P network is more realistic with respect to many cloud models which is shown in the figure below:

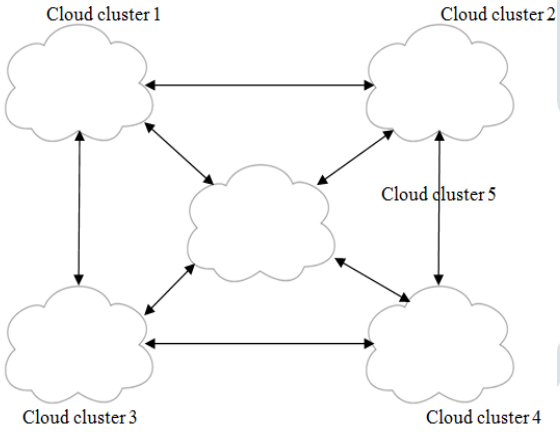

Fig 4. Many Cloud Based P2P Architecture

In order to improve security policy, both block chain and cloud platforms are combined since both models are similar. There are two ways to integrate cloud with block chain:

(i)Usage of clouds for the development of applications of block chain and supporting the coordination with private clouds to provide storage, replication and access to transactional data.

(ii)To improve security, data and user management in clouds, block chain methods are used.

IV. CHALLENGES FACED DURING COLLABORATION OF CLOUD AND BLOCKCHAIN TRANSACTION AND DATA

There are a vast number of transactions in block chain. Large number of data gets generated and there should be data processing services to manage and scale those large data. For dynamically changing requirements, scalability and elasticity are the two main features provided by cloud platforms. Public cloud provides unlimited access for customers to large scale resourcesand they have pay only for the required resources. Private cloud should be optimized to handle large data sets. From security point of view, cloud abstract physical location of data. To have efficient implementation block chain algorithm should be tuned whose impact on deployed application is minute. Block chain system must store and process data in permitted locations by abiding the rules of data sovereignty and users must be able to access those locations. Access permission is by cloud service provider to users. System resilience and fault tolerance are the other two issue of block chain. Block chain do not suffer from single point of failure i.e., failure of one node will not cause an entire system to fail. This is achieved with the help of cloud where the cloud replicates the data in the data centre and using multiple software application. Thus security of block chain system is improved by implementing block chain algorithm in cloud. In distributed cloud environment, software is centralizes and data is stored on local data server. Oracle Block chain Service Project(Oracle 2017) and iEx.ec Project(iEx.ec, 2018) is the recent examples of collaboration of block chain in cloud platforms.

V. NEW INNOVATION IN BLOCKCHAIN IN CLOUD PLATFORM

Block chain is a novel methodology helps in finding user obscurity using electronic wallet in large scale cloud. Electronic wallet must be installed in block chain system while finding obscurity of users and later it should be deleted securely from the system to protect user's data being accessed by third parties. Another idea is to use block chain algorithm for secure data and task scheduling in cloud. This is n important research topic.

VI. PROS AND CONS OF BLOCKCHAIN

6.1 Pros

Decentralized property is the major advantage of blockchain technology. It means the system do not require third part to take decision. Members of blockchain participate to discuss and take decision. Since each transactions in blockchain is verified, authorized and processed independently there is no risk of securing the database which usually get hacked. Blockchain achieve transparency, trust, faster processing and immutability since each transaction or data is recorded and cannot be changed. Due to decentralized property of blockchain data cannot be altered. Blockchain technology is traceable because it shows the occurrence of problem and corrects themselves if necessary. Reasons for blockchain security are person who enters blockchain system is provided with unique identity and the creation of hash table for each node where there is no chance for changing the information of hash table. Single public ledger helps to overcome the complications faced by participants.

6.2 Cons

Main disadvantage is energy consumption. Excess of power is required to maintain ledger, transparency, immutability, signature verification using cryptographic scheme. Next problem is the opportunity to split the chain. Nodes operating in old software do not accept transaction in new chain. This chain is creating with the same history as the chain, which is based on old software and called as fork. Another disadvantage is between quality of nodes and costs for users.

VII. CONCLUSION

Blockchain is a financial technology which is used to perform virtual financial transactions using cryptocurrencies in ICT environments. Participants store their transaction details in blockchain P2P network which effectively uses the allocated resources. Blockchain algorithm in collaboration with cloud platforms are used to improve security and privacy issue. In this paper gives an idea about importance of collaboration of cloud and blockchain which is used to improve the trust, security of data, user management and also challenges faced during collaboration of cloud with blockchain. This paper addresses the pros and cons of blockchain.

REFERENCES

[1] Quoc Khanh Nguyen, Quang Vang Dang, 2018. Blockchain Technology for the Advancement of the Future 4th International Conference on Green Technology and Sustainable Development (GTSD).

[2] Julija Golosova, Andrejs Romanovs, 2018. The Advantages and Disadvantages of the Blockchain Technology, 978-1-72811999-1/18/$31.00 ©2018 IEEE.

[3] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba, 2017. Blockchain Technology Innovations, IEEE Technology & Engineering Management Conference (TEMSCON).

[4] Jin Ho Park, Jong Hyuk Park, 2017. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, www.mdpi.com/journal/symmetry.

[5] 2017. Cloud Customer Architecture for Blockchain,Cloud Standards Customer Council.

[6] Quoc Khanh Nguyen, 2016. Blockchain – A Financial Technology For Future Sustainable Development, 3rd International Conference on Green Technology and Sustainable Development.