International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Blockcloud: Integrating Blockchain Security Features in Cloud Computing

Rajashree V Biradar , Girish Kumar D

Abstract: ***Financial technology is the next generation emerging technology, which has drawn the attention of most of the business enterprises. Both blockchain and cloud computing are the two main contemporary parts of Financial technologies. Blockchain provides security for the data through authentication of peers in order to share digital cash, encryption and hash value generation. As per the global financial industry's prediction, the security related blockchain technology will be increasing beyond 20 billion by 2020. Blockchain technology is used beyond crypto currency and cloud computing is also shifting to meet the changing requirements of industry revolution 4.0. Since Cloud Computing has deployed all its platform for availability and efficiency. This paper discusses about blockchain technology and also enlighten how it's features can be adopted in cloud computing.***

Keywords : Blockchain, Cloud Computing, security, efficiency, authentication.

I.INTRODUCTION

Blockchain will be the next generation industry revolution for financial sector and the applications of blockchain has reached beyond crypto currency [1]. In blockchain secure communication takes place between the peers who are participating in the network without the involvement of third party authority as performed in cloud computing. In blockchain each peers maintains a public ledger which consists of all the transactions that are performed within the network and this also helps to avoid hacks made during the virtual cash transactions.

In blockchain a transaction is initiated by the source node, verified by each node in the network and then the transaction is queued to the list of unconfirmed transactions which forms a block. Once the block is created, then all the nodes will append the block to their chain, in turn updating their ledgers. This acts as a trusted mechanism [2] which eliminates single point failure, need for third part authority by ensuring security for virtual cash.

Cloud computing has been implemented by many companies because of its efficiency, in which security and privacy are the two important buzz words that are widely discussed in terms of confidentiality, authentication, integrity and so on [3]. Cloud computing provides wide range of services to all the clients based on their requirements, which is on-demand pool of services (SaaS, IaaS, PaaS). Blockchain as a service (BaaS) can be considered as next generation feature of cloud computing, which is the combination of blockchain and cloud computing technologies. BaaS can be adopted by all the companies which have adopted cloud environment without any involvement of an IT expert, which in turn can benefit their business needs.

Revised Manuscript Received on April 18, 2020.
* Correspondence Author
Dr. Rajashree V Biradar*, Dept of CSE,BITM, Ballari, Affiliated to VTU, Belagavi, Karnataka, India.
Mr. Girish Kumar D, Dept of CSE,BITM, Ballari, Affiliated to VTU, Belagavi, Karnataka, India.

II. RELATED STUDY

2.1 Blockchain

In blockchain all the peers or users needs to maintain a ledger which consists all the transactional data and also update the ledgers in order to ensure integrity whenever there is a new transactions. To verify the reliability of every transaction, encryption technique is used by all the peers present in the blockchain network. Hence the dependency of third party and single point failure is resolved. Broker free is one of the key characteristics of blockchain thereby removing unnecessary fees that is caused by the involvement of third party authority as in cloud and the information of all the transactions are known to each and every peer present in the network. This makes difficulty for the attacker to hack the data, which in turn reduces the security expenses. Here all the transactions are recorded, verified automatically by huge participation, by using an open source the system can easily been implemented and connected, Hence all the records can be openly accessed by the public which in turn reduces the regulatory or third party costs[4].

The blockchain is organized in such a way that it stores data in a way which is similar to that of distributed database and also structured in such a way that making arbitrary manipulations is very difficult. Since all the members have a copy of each transactions and verify each block in blockchain, here each block contains a header and body. Each block contains hash value of the previous block along with the header of current block and index keys are used to search a block in the blockchain. The hash values which are stored in the block of each peer are affected because of previous blocks and hence it makes difficult to alter or delete the registered data block by the hacker. Hacking the data block can only be done if 51% of peers are attacked simultaneously at a time, and this kind of situation is very difficult in reality.

Blockchain technology uses public key for verification purpose using a hash function, which is used for both encryption and decryption process in ensure security for the data block. Here ECDSA (Elliptic Curve Digital Signature Algorithm)

is use for verifying the e-signature which is generated between users during each transaction to check if the data is altered or not. By using public key as users account information, enables peers to know who has sent and how much to other peer. There is no way for accessing data regarding the peers in the network [5-7]. In bitcoin transaction, hash function is used to check the integrity of each data block which contains transactional details and this is done by verifying the transaction by using hash value for public key encryption. Using root hash value of each transaction, we can check if the weather bitcoin data is altered or not [8, 9].

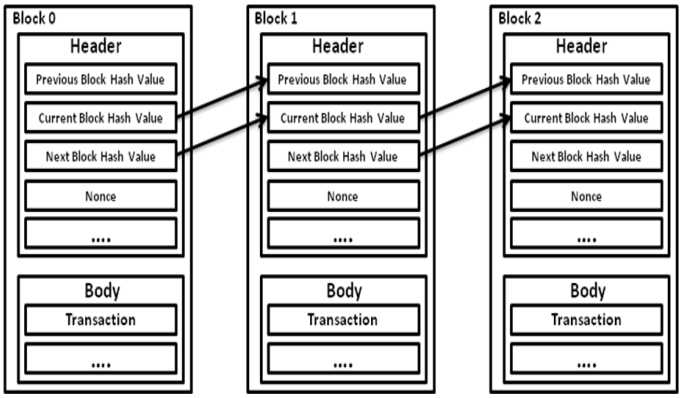

Figure 1: Blockchain Connection structure

Many researchers is going on to strengthening the security characteristics of blockchain and blockchain focus mainly on providing security for public keys of peers which is used during the transaction i.e. during encryption and decryption process. When an attacker uses "reuse attack" in order to get the personal key which is stored in peer's device, that can be used for hacking the bitcoin. Once the personal key is obtained, then the attacker can hack the bitcoin if there is leakage in data.

Bitcoin is vulnerable, since the malware infection can be done because the trade is done on client's personal computer or Smartphones. The applications, emails which are less secure must be detected and well trained in order to stop infection of peer's device, such type of technique can be done in game environments [10]. The biggest strength of blockchain is that it is very difficult to modify the transaction ledgers, since many peers will share the same ledger. If the attacker modifies 51% of all the peers' ledger, then he can access the data block and this problem can be solved by performing intermediate verification that has to be designed to solve this problem.

2.2 Bitcoin

In 2009 Satoshi Nakamoto introduced digital or crypto currency called bitcoin, which allows peers to perform all the transactions without the need of central authority or third party to manage crypto currency. Each transaction in bitcoin is done based on distributed database using public key cryptography technique [11]. This information related to bitcoin is flooded in the network and the peers use this information to verify the crypto currency. Each peer will have the same copy of blockchain who are participating in the blockchain network. In spite of many issues in digital transactions, blockchain implementation is very effective. For example if any user tries to generate false receipt from another users account to his account, this can be blocked by checking the sender's public key.

Bitcoin address is the main component of bitcoin, which specifies the location of the bitcoin and the peers who has confirmed the bitcoin transaction. Each transaction in bitcoin plays a very important role, which takes bitcoin as an input and generates the address as an output. The digital currency used in bitcoin contains chain of digital signatures as shown in figure 2. A central authority is used to check all the transactions, to guarantee, the owner have not used the coins many times [12].

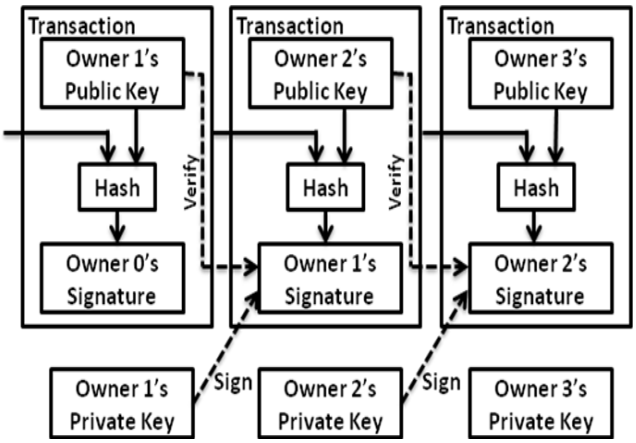

Figure 2: Bitcoin transaction

2.3. Security challenges of Blockchain

2.3.1 Settlement of Blockchain

Even though one to one blockchain exists, which is generated by a block. Consider a scenario where two peers try to generate the block at the same time then the single block will be divided into two blockchain which is generated by two blocks at an instant of time. In this scenario the block which is chosen by majority of peers will be selected and the other will not be selected for mining in bitcoin network. As per the recent study, if the attacker has 25% of mining capability then he can easily falsify the transactions. As the computation cost of bitcoin is very high, getting high mining ability is difficult. But still it can be a risk and because of the basic characteristics of bitcoin, security aspects have affected the economic factors in the market [13, 14].

2.3.2 Security of transaction

Flexible programming language is used to write the scripts for both input and output to create different transactional forms. For authentication and financial services a bitcoin contract [15] is been used and the method for creating a contract includes multiple digital signature technique named multisig. Even though the scripts are written to solve many problems in bitcoin, the possibility of a poor configures transaction increases the script complexity and generally these kinds of transactions are discarded. Much research is going on to check the accuracy of the script which are used to model bitcoin contract type transactions [16].

2.3.3 Security of wallet

The bitcoin address consists of hash value which is encoded using the public key and personal keys, In order to unlock the output a locking script is written for a bitcoin transaction which outputs the address that can be easily unlocked by the unlocking script.

It is clear that if there is a loss of data from digital wallet, which causes loss of bitcoin data and this is a major concern for bitcoin attacks made by the hacker [17]. In order to provide security for the wallet a multisig services care been used for multiple digital signatures and this multisig is used as an redundant security

feature which allows a transaction when there are more than one digital signatures. Here multisig services allow the biometric withdrawal or a two factor authentication is used with other measures [18].

A basic solution to avoid bitcoin wallet attacks is offline storage, such as paper bitcoin or physical bitcoin wallet which is connected to the network or internet. Here the storage unit is used only when there is a signed transaction that is sent using the storage key whenever a bitcoin transaction is required and this leads to another problem such as loss of cold storage or lack of user friendliness to the hardware wallet [19].

2.3.4 Security of software

If there exists a software bug in bitcoin, its critical. Since the bitcoin core structure is very effective as the reference made by Satoshi Nakamoto during software implementation. The core software should be more reliable which should not contain any bug or software malfunctioning. CVE-2010-5139 is one of the most famous bug, occurred during 2010 by integer overflow which is an invalid transaction 0.5 bitcoin, which is referred as 184 trillion bitcoins present in a a block and then the problem was solved 8 hours later. In Bitcoin version 0.7 and 0.8 have different blockchain, which made difficult for the peers to do transactions with peers who have different versions. Hence these two problems clearly show that the security of bitcoin transaction on a block is treated as a software bug [20].

2.34.5 Double transaction

The main problem of bitcoin using bitcoin is it increases the possibility of double transaction. A double transaction is a process in which the bitcoin is sent to two or more peers or accounts for malicious purpose. In order to solve this problem "total currency" and "longest chain wins" mechanisms are adopted for preventing this kind of malicious behavior in the network. As shown in figure 4, the double transaction problem can be addressed using this mechanism, the red blocks represents the chain that loses the competition.

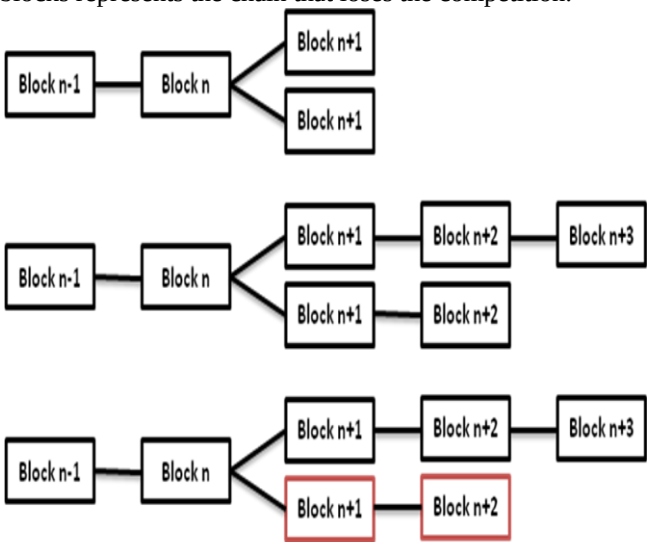

Figure 3: Double Spending Prevention Mechanism

III. SECURE BLOCKCHAIN SOLUTIONS IN CLOUD COMPUTING

In cloud computing the main focus is on how to provide security for the data during transmission and at rest. To provide strong security service, the combination of blockchain and cloud computing can be helpful. Before the user stores his sensitive information on to the cloud, the anonymity can be checked if blockchain technology is adopted and this is done by installing digital wallet.

In this process if the digital wallet is not handled properly, then user's sensitive information can be leaked. In other words the security of blockchain is affected if the sensitive data is leaked in cloud environment, which damages the monetary aspects of blockchain. To solve this problem, a solution has been proposed [21] which installs and deletes the digital wallet safely.

There are few other issues, such as falsifying the transaction ledger or double transaction. Since most of the users use mobile devices, the verification of these devices has to be done. The accuracy and integrity of the timestamp is obtained only when the transaction is guaranteed [21].

The core technology of blockchain must be verified properly, since the vulnerabilities changes from one programming language to another, versions used by peers and also the platform which is used for deployment of digital wallets. The wallet must be implemented securely in order to minimize the verification problems that are occurred during planning, analysis, requirements, quality of service and maintenance. Figure 5 shows the secure bitcoin protocol using digital wallet.

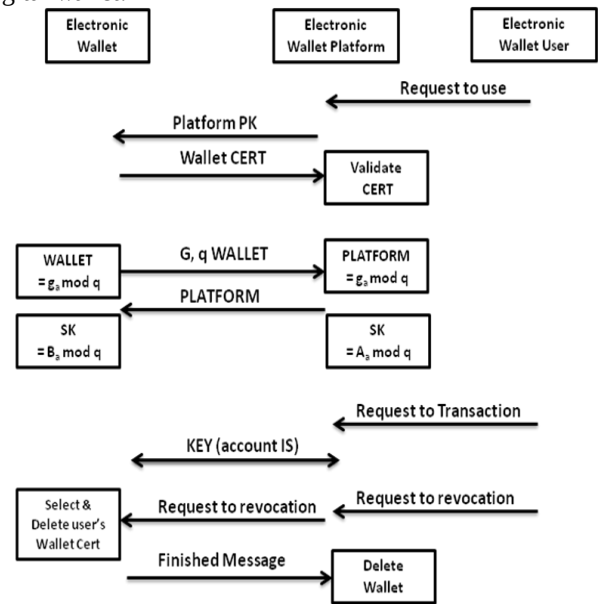

Figure 4: Secure bitcoin protocol

IV. BLOCKCHAIN-AS-A-SERVICE (BAAS)

It is a mechanism of hosting all the features of blockchain in cloud computing environment. BaaS allows the peer to create an application, distributed ledger, platform and also security for the data. Thus BaaS helps to deploy blockchain services and core features on to the cloud computing environment, which can be used by developers and users [22].

The fundamental technique of BaaS is as same as Software-as-a-Service (SaaS) and the functionality of BaaS can be either PaaS explicitly or SaaS implicitly which may vary based on the type of cloud computing environment been used.

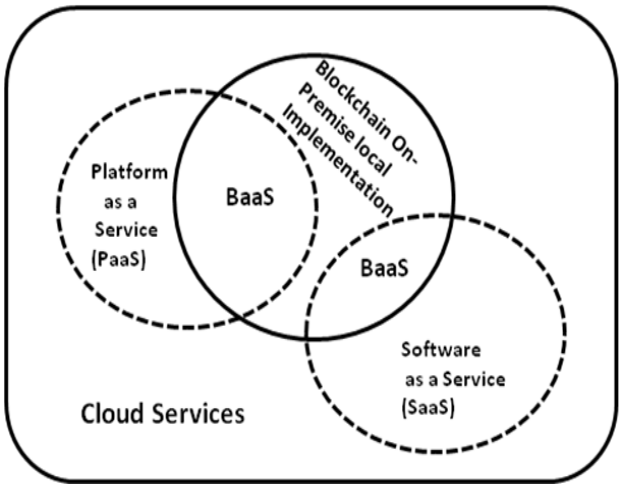

Figure 5: Location of BaaS

Figure 6 represent on premise deployment of BaaS in cloud computing environment. In this scenario BaaS use the support of PaaS and SaaS, BaaS uses software services from SaaS and platform services from PaaS. BaaS provides flexibility for the organizations to focus on functional needs and business logic of blockchain, which helps to deploy all the functionalities on to the cloud computing environment.

Advantages of BaaS

1. Using BaaS based cloud platform, users can receive reliable services with less cost instead of separate on premise blockchain deployment.
2. BaaS takes complete care of peer creation, deletion and transaction verification without any intervention.
3. BaaS provides high interoperability by using the existing services of cloud computing (SaaS, IaaS, and PaaS).
4. BaaS can be managed by users who do not have technical knowledge of enterprise blockchain.
5. The third party authority is not required for managing blockchain technology of BaaS.
6. BaaS provides guaranteed secure transactions.
7. Real time tracking of all the transaction is done with no single point failure in BaaS.

V. CONCLUSION

Blockchain has changed the way how organizations are performing financial transactions. It has eliminated the use of central authority and allows the peer to control all the transactions by himself without any technical knowledge of blockchain. It has a distributed network structure and uses peer network structure for resource computation. Security mechanism is implemented to monitor all the transactions carried out by each peer at real time in the network.

In this paper, the core technologies of blockchain have been studied and various measures should be taken by the peer before implementing blockchain technology in cloud computing environment. Many issues are raised in blockchain even today regarding security for digital wallet, transaction ledger and software. The data uploaded in blockchain network are not controlled by anyone and even if anyone tries to access user data, it can be only partial data which does not provide entire information. All companies that are keen to invest in blockchain technology need to first perform a strategic evaluation to see if it is feasible for their enterprise business model. Thus, it is suggested that companies carry out granular tests on the use-case level to decide which software may be brought on with blockchain technology. A proper strategic technique is needed in order to use blockchain effectively.

REFERENCES

1. Miraz, M.H., Ali, M.: "*Applications of Blockchain Technology beyond Cryptocurrency"*. Ann. Emerg. Technol. Comput. 2, 1–6 2018. https://doi.org/10.33166/AETiC.2018.01.001.
2. Miraz, M.H.: Blockchain: "*Technology Fundamentals of the Trust Machine. Mach. Lawyering"*, Chinese Univ. Hong Kong, 23rd December. 2017. https://doi.org/10.13140/RG.2.2.22541.64480/2.
3. Onik, M.M.H., Ahmed, M.: "*Blockchain in the Era of Industry 4.0. In: Mohiuddin Ahmed, A.-S.K.P. (ed.) Data Analytics: Concepts, Techniques, and Applications. pp.* " 259–298. CRC Press, 2018.
4. Kaskaloglu, K. "*Near zero Bitcoin transaction fees cannot last forever"*. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic, 24–26 June 2014.
5. Aitzhan, N.Z.; Davor, "*Security and Privacy in Decentralized Energy Trading through Multi-signatures,Blockchain and Anonymous Messaging Streams".* IEEE Trans. Dependable Secur. Comput. 2016, 99.
6. Heilman, E.; Foteini, B.; Sharon, G. "*Blindly signed contracts: Anonymous on-blockchain and off-blockchainbitcoin transactions*". In Proceedings of the International Conference on Financial Cryptography and DataSecurity, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Gemany, 2016.
7. Natoli, C.; Gramoli, V. "*The blockchain anomaly*". In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016.
8. Shi, N. *A new proof-of-work mechanism for bitcoin*. Financ. Innov. 2016, 2, 31.
9. Swan, M. "*Blockchain: Blueprint for a New Economy"*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
10. Wressnegger, C.; Freeman, K.; Yamaguchi, F.; Rieck, K. "*Automatically Inferring Malware Signatures for Anti-Virus Assisted Attacks"*. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, 02–06 April 2017.
11. Decker, C.; Roger, W. "*Information propagation in the bitcoin network*". In Proceedings of the 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, 9–11 September 2013.
12. Nakamoto, S. "*Bitcoin: A peer-to-peer electronic cash system*". Available online: https://bitcoin.org/en/bitcoin-paper, 2017.
13. Bozic, N.; Guy, P.; Stefano, S. "*A tutorial on blockchain and applications to secure network control-planes"* SCNS IEEE 2016.
14. Bradbury, D. "*The problem with Bitcoin. Comput. Fraud Secur*". 2013, 11, 5–8. Paul, G.; Sarkar, P.; Mukherjee, S. "*Towards a more democratic mining in bitcoins*". In Proceedings of the International Conference on Information Systems Security, Hyderabad, India, 16–20 December 2014; Springer International Publishing: Cham, Switzerland, 2014.
15. Bamert, T.; Decker, C.; Wattenhofer, R.; Welten, S. "*BlueWallet: The Secure BitcoinWallet. In Security andTrust Management"* Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014;pp. 65–80.
16. Anceaume, E.; Lajoie-Mazenc, T.; Ludinard, R.; Sericola, B. "*Safety analysis of Bitcoin improvement proposals*". In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016.

17. Upadhyaya, R.; Jain, A. "*Cyber ethics and cybercrime: A deep dwelved study into legality, ransomware,underground web and bitcoin wallet*". In Proceedings of the 2016 International Conference on Computing,Communication and Automation (ICCCA), Noida, India, 29–30 April 2016.
18. Haber, S.; Stornetta, W.S. "*How to time-stamp a digital document*". In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Gemany, 1990.
19. Eyal, I.; Emin, G.S. "*Majority is not enough: Bitcoin mining is vulnerable*". In Proceedings of the InternationalConference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Gemany, 2014.
20. Samaniego, M., R.D.I. of T. (iThings), "*undefined*: *Blockchain as a Service for IoT*". ieeexplore.ieee.org, 2016.
21. Rimba, P., Tran, A., Weber, I., … M.S.-2017 I., 2017, "*undefined: Comparing blockchain and cloud services for business process execution*". ieeexplore.ieee.org.
Lahiri, S.K., Chen, S., Wang, Y., Dillig, I.: "*Formal Specification and Verification of Smart Contracts for Azure Blockchain*". 2018.