IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 10, October 2020

DOI 10.17148/IJARCCE.2020.91013

Blockchain For Securing Cyber Infrastructure

Riya Suri[1], Nachiket Bhuta[2], Sagar Gada[3], Rahil Vithalani[4]

Student, Information Technology, K.J Somaiya College of Engineering, Mumbai, India[1,2,3]

Student, Computer Engineering, K.J Somaiya College Of Engineering, Mumbai, India[4]

Abstract: Blockchain technology has seen adoption in numerous ventures and most overwhelmingly in money using digital currencies. Be that as it may, the technology is capable of working successfully in cybersecurity. Here we have referred to several blockchain related research papers. It found that most of their researchers are focusing on the appropriation of Blockchain to ensure IoT (Internet of Things) gadgets, systems, and information. The paper inspected the ways featured by past scientists through which Blockchain can manage the cost of security to the three hazardous areas in IT. In conclusion, the paper prescribed that future researchers center around a solitary Blockchain on which to create cyber security applications to take into consideration combination and consistency among arrangements.

Keywords: Cyber, Security, Cybersecurity, Blockchain, Consensus, Hash, Cloud, Cloud computing, Mining, Ledger, Decentralized, E-wallet.

I. INTRODUCTION

Our cash is moved in a flash by means of virtual ledgers, our enlightening sources are huge and careful and even online orders are delivered in a day or two. This amazing digital age comes with an amount and mainly with our privacy of personal information. Many of our records are spread all through the web and ensured distinctly by frequently weak passwords which includes bank accounts, health records and other essential data. The data age blast of online information has carried with it slips by in security conventions that regularly uncover our most sensitive data. Finding a solid cyber security solution, consequently, is a higher priority than any time in recent memory. Our present security conventions essentially can't keep up with new and clever attacks, particularly when they're apparently so basic (i.e., a phishing email to a credentialed user can uncover the information of millions). Blockchain, a Distributed Ledger Technology (DLT), is centered around making trust in an untrusting biological system, making it a possibly solid cybersecurity innovation. The ledger system is decentralized, yet data is straightforwardly accessible to individuals from the particular chain. All individuals (or nodes) can record, go along and see any important transaction data that is being stored on their blockchain.

II. CURRENT CYBER INFRASTRUCTURE

In the current security mechanisms being implemented there are various security threats that exist like unpatched vulnerabilities and software with problem of inconsistent data management, denial of services attack also being on rise with great threat to various aspects of businesses in execution are getting affected.
Attacks like:
1) Phishing
2) Money Extortion
3) Malicious tampering of data
4) Introducing viruses and malware to affect the data and records.
and many more are on the rise today. This can be reduced with better technologies (here blockchain) as discussed below:

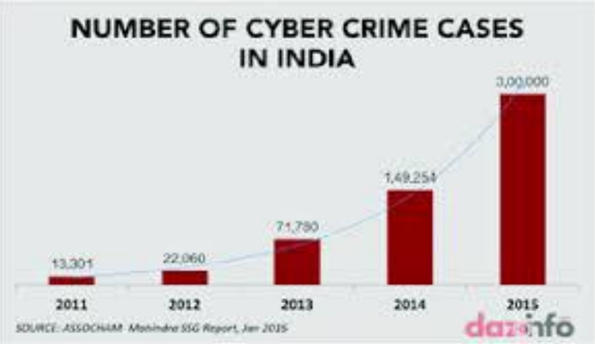

Fig. 1. Cyber Crime Cases in India

DOI 10.17148/IJARCCE.2020.91013

The graph above has statistics about how the crime cyber crime rates have increased in india alone at exponential rate and thus proper measures for controlling it needs to be taken further.

III. HOW BLOCKCHAIN IS USEFUL FOR CYBER SECURITY

A. Immutability And Consensus

What makes blockchain a great choice for cyber security is the fact that the blocks are immutable as we use the previous pointer to the block instead of next; it adds this feature to it. The immutable feature is what sets apart blockchain from rest of the available technologies As can be seen in the diagram below refers to how the basic blockchain structure works.

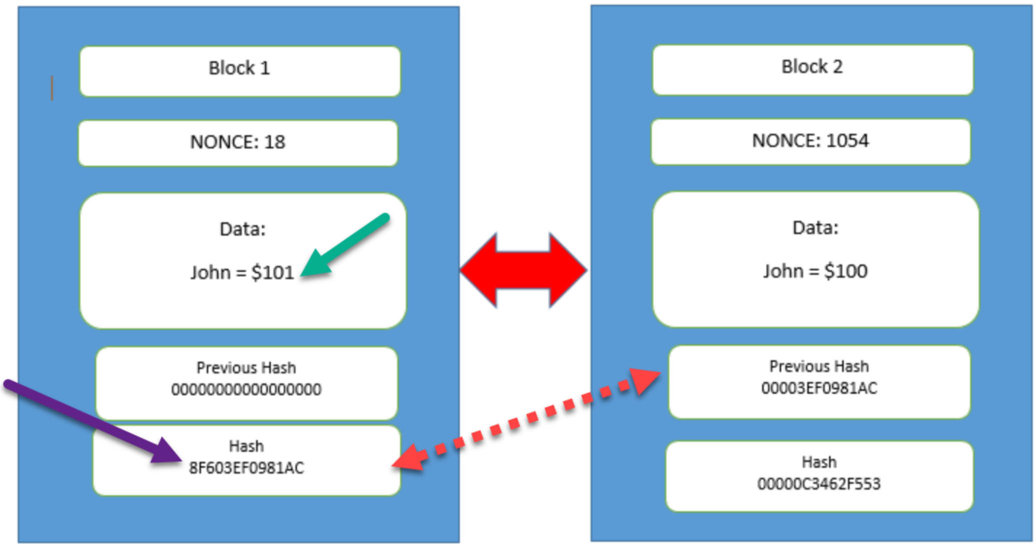

Fig. 2. Basic Structure of Blockchain

One more concept which makes blockchain great choice for security infrastructure is consensus. Consensus is ability of the nodes in distributed blockchain network to Typically, the process of achieving consensus is to agree and there by validate incoming transactions making it difficult for them to tamper the data.

B. Hash Values

What is a great feature about the blockchain security is generation of a hash function. what is even better is the all the input generate a uniform size hash function and every hash value is indeed dependent on the hash value of the previous block. So if a user makes the changes to any block then the next hash changes and transaction will automatically become invalid.

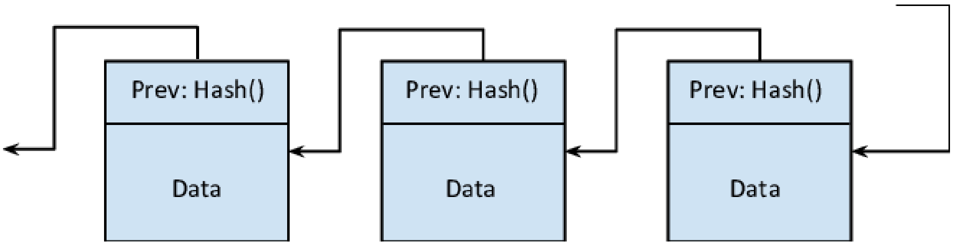

Fig. 3. Use of Previous Block Hash

C. Asymmetric Encryption

The use of public and private key provide non-repudiation to the system means the user if has committed a transaction can not deny from it at any stage and also saves the privacy of user as only the public key is shared in the pool which can be easily understood by the diagram having Bob and Alice as the sender and receiver.

D. Crypto Economics

For the blockchain system great work has to be done either in the form of mining or validation transaction it is evident no miner would do it for free. Blockchain has a great systeof mining reward where for the successful and legitimate transaction you get mining rewards and even credibility as a user in the pool increases.

DOI 10.17148/IJARCCE.2020.91013

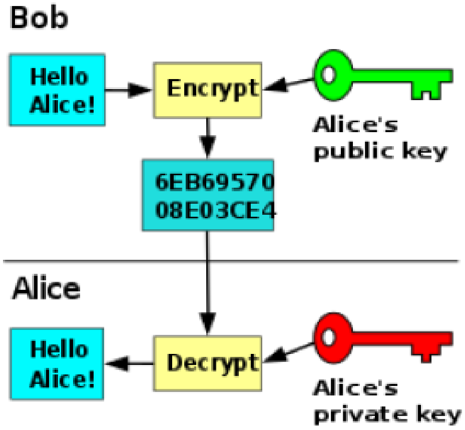

Fig. 4. Asymmetric Encryption

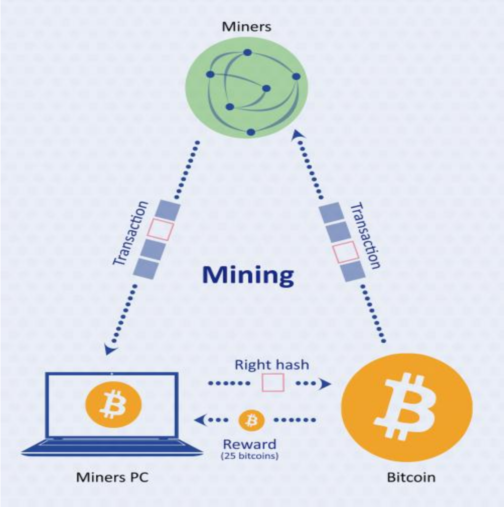

Fig. 5. Crpyto currency Mining

E. Authentication Mechanism

Blockchain can be used for authenticating one's identity by creating key-pair of the user. The key-pair of an user will be generated from the secret private credentials such as biometric information, social security number, aadhar number, etc. The users can register their identity on the blockchain. The recognized party can be the different services such as various government services, airports, banks and other services. The user now can authenticate at the services by verifying the hash values which are registered on the blockchain and this information can be used as the truth on the blockchain.

IV. CLOUD COMPUTING SECURITY USING BLOCKCHAIN

A. Use of Blockchain on Cloud

1) Open Ledger: The storage on the cloud is available and anyone can view the services which are provided by the cloud service provider. The users can also select the services as pay as- per-go policy.

2) Distributed Ledger: The local copies of the users are well synchronized that any user can view the latest version of the ledger.The ledger holds a list of services, policies and service level agreements which are used by individual user.

3) Decentralized Smart Contract: The smart contracts are stored on the blockchain. All the users on the cloud services have a copy of it. When a payment is processed, all the contract transactions which were processed earlier are stored based on the timestamp order on the blockchain along with the events of processing. If any user tries to change the existing contract on the Blockchain, then all the other cloud service users can detect & prevent the changes of the contract.

B. Securing Cloud using Blockchain

The users confidential data is the most sensitive data in cloud computing system. If these information is leaked or disclosed, then there can be psychological and economical losses. The study of the data security for maintaining integrity and privacy is the main focus of the study and blockchain can provide the level of ensuring security in cloud computing environment.

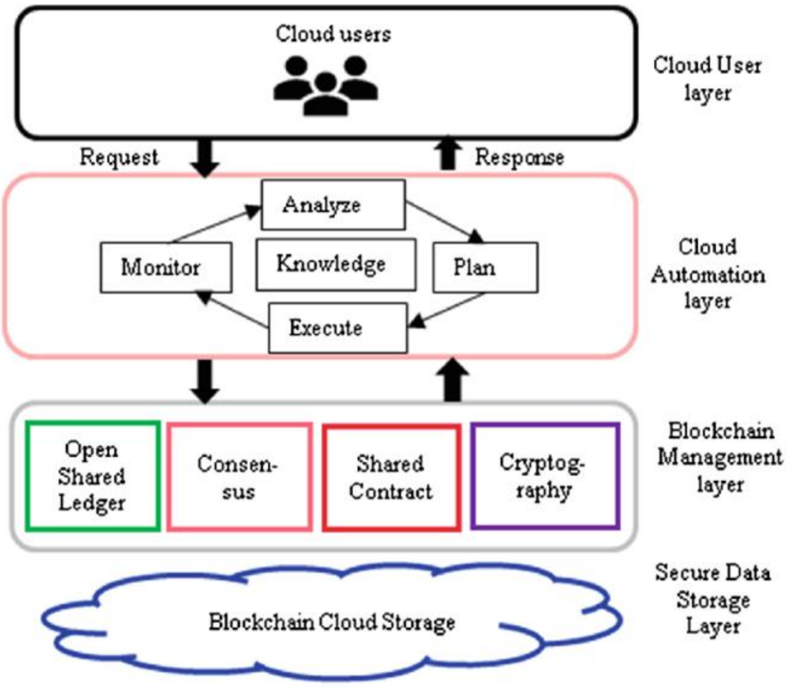

Fig. 6. Blockchain for Cloud Services

A secure e-wallet can be used to store the user information. Eventually the e-wallets were stored on PCs but nowadays the mobile phones are in increasing demand, then the question arises that how to verify the security of e-wallets on the mobile phones. A transaction process should only be completed when the accuracy and integrity of data is maintained and based on the timestamp of the mobile phone which can ensure the security of a transaction. A e-wallet can be created by reducing, verifying and validating problems which can show up at each step of planning infrastructure, the requirements analysis, implementation and testing, and maintenance of the environment.

V. SIGNIFICANT CHALLENGES OF USING BLOCKCHAIN IN CYBER SECURITY

Although block chain is a powerful technology, it still has some flaws. Its powerful rules and concepts like cryptography, distributed consensus, etc can resist many other different kinds of fraud and attacks but it cannot resist 51% attack, account takeover, identity theft, money laundering and hacking.

1) *The 51% attack:* This type of attack occurs when a single user has exceptionally more computing resources than rest of nodes, which helps him in further dominating other nodes and approval of transactions and getting control over the whole chain. As it owns more than half of the computational power of the network, it can include fraud transactions, spend double amount or even steal assets of other people.

2) *Identity Theft:* Although blockchain promises to preserve anonymity and privacy, but the security of user transactions depends on a private key, a digital identity, which is hard to crack. If the private key is stolen the party cannot recover it, but the chances are 0.00001. Thus, all the advantages this owner possesses in the blockchain will evaporate, and it will be almost difficult to distinguish the thief. The result might be wrecking in a world without internet, where outsider foundations (e.g., Mastercard organizations) or focal specialists defend exchanges, control dangers, distinguish suspicious exercises, or help discover guilty parties.

3) *Illegal activities:* Blockchain as a platform can be turned into a illegal activity center. For real life example, there is a website The Silk Road website which is an online market to buy and sell illegal drugs with total anonymity and using bitcoin as a currency. Digital currency that utilizes blockchain innovation may likewise encourage illegal tax avoidance. In spite of the fact that bitcoin isn’t yet treated as a fiat money, it makes it possible to make an ”underground” channel for illegal movement development of assets inside its system.

4) System Hacking: It would be hard to change the records stored in block chain, but not programming codes and frameworks that execute its innovation. Here is a very good real life example, MtGox, once known as the largest Tokyo based bitcoin exchange company, was attacked in March 2014, and bitcoin with estimated value of $700 million were stolen. Inadequately maintained systems and outdated codes permitted criminals to twofold spend (Bitcointalk 2014). A later incident tormented a DAO (Decentralized Autonomous Organization) that holds huge amounts of Ethereum, a cryptographic money like bitcoins (Price 2016). The programmer misused a product defenselessness and took $50 million worth of Ethereum.

VI. FUTURE OF BLOCKCHAIN IN CYBER SECURITY

Due to the above-mentioned challenges blockchain is not mainstream in cybersecurity. Integration of below mentioned features can help in improving the blockchain for security:
1) Developing Public Key Infrastructure: The already existing PKI uses 3rd party certificates to make sure the useris valid or not. Bringing a rule in blockchain where no third-parties are involved to validate the user will be a major win.
2) Developing a mechanism to control the flow of the blocks: DDOS attacks are very easy to be made on blockchains. Developing measures that make sure DDOS is not possible is a major feature needed.
3)Private Blockchains: A lot of companies do not want their data to public. Developing a mechanism that can help companies create a private blockchain path where no data can be made or validated outside the company boundary is a crucial feature.

VII. CONCLUSION

Blockchain is the next big thing in cyber security. With the features such as immutability there is no way data can be manipulated once it is created. Consensus makes sure that no malicious data block is sent over the internet as a majority of the users have to accept that the block is valid and then can be forwarded. Bringing more complexity to this is the hash function where it creates a unique key of the same length for every block using the previous blocks value. Features like asymmetric key cryptography and authentication make sure that user identity is maintained and no one can spoof identity. Further we see how can we implement block chain in cloud-based services and different plans related to the same and in the end we look at the challenges that are faced currently by blockchain limiting the use of blockchain in cybersecurity.

REFERENCES

[1]. Ashok Gupta, Shams Tabrez Siddiqui, Shadab Alam and Mohammed Shuaib "Cloud Computing Security using Blockchain" 2019 JETIR June 2019, Volume 6, Issue 6 .

[2]. Alex. R. Mathew International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019: "Cyber Security through Blockchain Technology".

[3]. Nir Kshetri Bryan School of Business and Economics, The University of North Carolina at Greensboro, Bryan Building, Room: 368, P. O. Box 26165, Greensboro, NC 27402-6165, USA: "Blockchain's roles in strengthening cybersecurity and protecting privacy".

[4]. Zhaoyang DONG, Fengji LUO, Gaoqi LIANG: "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems".

[5]. Taylor, PJ, Dargahi, T, Dehghantanha, A, Parizi, RM and Choo, KKR: "A systematic literature review of blockchain cybersecurity".

[6]. Hai Wang,Yong Wang, Zigang Cao, Zhen Li,Gang Xiong:"An Overview of Blockchain Security Analysis".

[7]. S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 463-467.

[8]. Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye: "From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues", "The 2017 4th International Conference on Systems and Informatics."

[9]. Antonina Farion, Oleksandr Dluhopolskyi, Serhiy Banakh, Nadiia Moskaliuk, Mykhailyna Farion, Yuryi Ivashuk: "Using Blockchain Technology for Boosting Cyber Security", 2019 9th International Conference on Advanced Computer Information Technologies (ACIT).

[10]. Wu J. (2020),"New Approaches to Cyber Defense. In: Cyberspace Mimic Defense. Wireless Networks. Springer, Cham."

[11]. Cheng S., Gao Y., Li X., Du Y., Du Y., Hu S. (2019), "Blockchain Application in Space Information Network Security. In: Yu Q. (eds) Space Information Networks. SINC 2018. Communications in Computer and Information Science, vol 972. Springer, Singapore"