IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 2, Ser.III (Mar. – Apr. 2021), PP 46-48
www.iosrjournals.org

Cyber Security Using Blockchain Technology

Bhavya Ashok k
Dept. of Computer Science
KSSEM, India

Abstract: *The term cyber security is the collection of techniques or method to protect computer, data, coding and networks etc from access or attack by unauthorized source. This attacks is called cybercrimes. The person who performs cybercrimes are called cyber criminals. Cyber criminal who would be expert in hacking a system or a network. Cyber criminal would hack the network or a system of a company or organization for their data, information and intellectual property. For preventing this cyber crime blockchain would be one used. This technology is used in many large company, banks and many other places. Blockchain technology is used in cyber security to prevent the hacking of system and network. Blockchain technology would be more useful in protecting the company network.*

Keywords: *Cyber Security, Blockchain, Cybercrimes*

Date of Submission: 28-04-2021 Date of Acceptance: 12-05-2021

I. Introduction

The term cyber security is the collection of techniques or method to protect computer, data, coding and networks etc from access or attack by unauthorized source. With the increasing amount of people getting connected to internet the security threats that causes massive harm are also increasing. There are many ways to prevent this cyber criminals, one of the technology is blockchain.

Blockchain is a booming technology that boosts every business and industry verticals as the of cyber criminals increases complex and are endlessly trying to steal valuable data. So, blockchain could potentially enhance cyber defense that prevent fraudulent activities through consensus mechanisms and detect data theft depending on utilizing its characteristics such as data encryption. Blockchain technology provides one of the best tools we currently have to protect data from hackers, preventing potential frauds and decreasing the chance of data being stolen or compromised. be accessed from any computer in any part of the world. The complex structure provides blockchain technology with the ability to be the most secure form of storing and sharing information online that we've discovered so far. That's why innovators have begun applying the technology in different sectors to prevent fraud and increase protection of data. Blockchain can be loosely translate as several cryptographically chained block. A block refers to a data structure with three main components; data, the hash of the previous block and the hash of the data and previous hash. Therefore, there is an order of dependency between the blocks that can be used to ensure the integrity of the blockchain. If the data in any block changes, its hash will be changed as well. The block in the blockchain can never be modified since doing so will affect the integrity of all the subsequence blocks. This stringent blockchain architecture implies that caution has to be taken when adding blocks to the chain to ensure that there will not be a need to change it later one. Nowadays protecting technologies could not protect high secret information dates and bank accounts reliably with guarantee. So, technologies based on cryptography are becoming more demanding by companies and organizations as well as scientists and researchers. Thus by using blockchain technologies by companies and organizations will help secure internet data, information, devices and services from cyber attacks.[1]

II. Types of Cybercrimes

The most spread types of cybercrimes around the world, the below figure shows that. Cyber theft of intellectual property is the most dangerous for almost all type of business as cyber crooks works exploit every opportunity they find.[2]

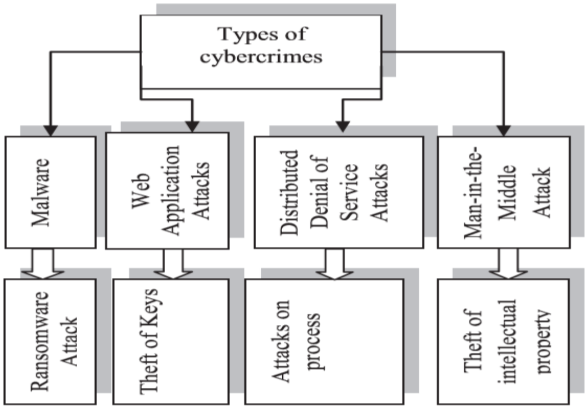

Figure 1 : Types of Cybercrimes

III. Cybercrime Attack

Most cyber crimes are connected through a lack of protection or not effective programs or software. But even with the high protected combination of different software everyone could not be safe totally.

Intellectual property crimes are committed when someone makes such procedures as: manufactures, distribution, or sell the counterfeit or pirated goods – patents, literary, trademarks, industrial designs or artistic works with commercial goals. The main method of cybercrime is committing crimes by targeting the computer networks and devices. With so much attention given to acquiring the newest and most sophisticated types of cyber security software, safeguarding the security of company hardware is often overlook but the loss or theft of device is a real threat to be aware of. There were appeared not only the new types of cybercrime but various tools of their execution.[3]

IV. Blockchain Challenge For Boosting Cyber Security

Blockchain is a powerful innovation that brings substantial positive change to financial services industry. There are two of blockchain: public and permission blockchain. Blockchain implementation are often designed with a specific purpose or function. Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer(P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithm. It is used in decentralized manner and removes the need for intermediaries or “trusted third party”. Thus the company construed a demo blockchain model that protects the companies data, information and intellectual property.

Blockchain is made up of two concepts. One of them is anonymity. Anonymity is the main aspect of blockchain technology. Many people proof that is impossible to break codes steal data from blockchain technologies. Asymmetrical cryptography enables users who do not know each other to exchange encrypted information. The system is based on a public key that can be made available to all, and allows encrypted data to be sent to a third party. The third party accesses the encrypted data via a paired private key. The public key is similar to a bank account number, which can be provided to anyone. The private key, which remains secret, acts as a password. The blockchain is a open-ended and operates in a decentralized, ongoing manner thanks to the activity of its users who can store information and to consensus algorithm- nobly “poof-of-work” and “proof-of-stake”.[4]

The first step in transfer cyber security by blockchain technologies is verifying software that is software that is installed for preventing hacker should be verified first. Then mitigating DDoS attackers. That means when the hacker keeps on sending junk request to a website that increases the traffic until the site is no longer kept with request. Thus this DDoS attacks should be reduces. After that the user should give the private key which the user have. Then the system would automatically prevents some of the hackers. Blockchain would give more secure DNS.

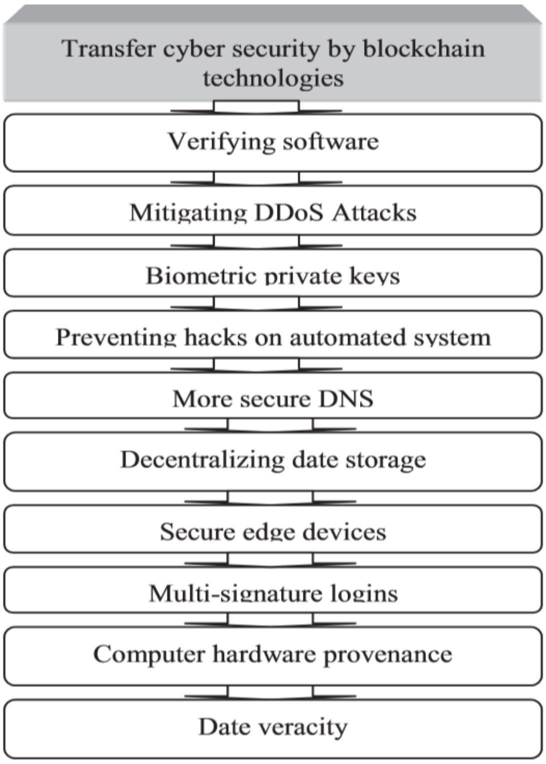
Transfer cyber security by blockchain technologies
Verifying software
Mitigating DDoS Attacks
Biometric private keys
Preventing hacks on automated system
More secure DNS
Decentralizing date storage
Secure edge devices
Multi-signature logins
Computer hardware provenance
Date veracity

Fig 2. Blockchain will transform cyber security

Then the data would be stored by decentralization method. The device should be secure edge. The device would have multiple signature login, that means multiple user can login to the device. After login process the computer hardware are assess. If any fault in the system then cyber security won't be proper. After the assess of computer hardware we would get know how data is accurate, precise and trusted. Thus after all these steps would we secure the data by blockchain. Blockchain technology can be used to prevent any type of data breaches, identity thefts, cyber-attacks or foul play in transaction. This ensure that data remains private and secure.

V. Conclusion

Blockchain technology is a breakthrough in cyber security, as it can ensure the highest level of data confidentiality, availability, and security. Implementing a blockchain-based security system fundamentally changes the game for cyber security, presenting a nearly impossible task for cyber thieves.

It's the reason why nobody has ever hacked Bit coin, the crytocurrency powered by public blockchain technology. Block chain has proven to be a-go-to tech for better security. The technology would be a challenge for cybercriminals where individuals have control of their own data. Its function is endless and it can fit in all industries. The future with this technology might solve a lot of problems.

Blockchain Technology has become a rising trend with regards to cyber security because it is impossible to break codes and keys as it combines many users and computers.

Acknowledgment

This Technical paper could not have been written without my parents Ashok Kumar K R and Sumithra, who encouraged and challenged me through my academic program. And giving me the strength to reach for the stars and chase my dreams, and authors mentioned in the reference.

References

[1]. Antonina Farion Economic Security, IEEE - "Using Blockchain Technology for Boost Cyber Security" (2019).

[2]. Jonathan White, Dept. of Engineering Management and System Engineering Old Dominion University Norfolk, IEEE – " Continuous Cybersecurity Management Through Blockchanin Technology" (2019).

[3]. Zibin Zheng, Shaoan Xie, Hongning Dai, IEEE – "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends" (2017)

[4]. D.Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview". NIST, U.S. Department of Commerce, October 2018. Victor Chang, Muthu Ramachandran, Member, IEEE "Towards achieving Data Security with the Cloud Computing Adoption Framework", 2015,IEEE.