APPLICATIONS OF BLOCKCHAIN IN CYBER SECURITY

Sourabh Sanjay Abhang

---***---

Abstract - This pandemic has rendered enormous difficulties for the businesses worldwide to remain functional despite of massive shutdowns of their facilities. In a matter of few months the world became far more digitally connected than it was ever before. There has been exponential increase in network traffic which in turn demands more robust IT infrastructure. Most of the employees are working from home which makes them even more vulnerable to attacks. Companies that use secure remote access technology can give remote employees private access (without a VPN) to enterprise applications and systems to mitigate the risks. In this paper we will discuss various methods and techniques we can implement to make ourselves as secure as possible on the internet by the use of new technologies like blockchain which uses distributed decentralized ledger systems which can have great applications in cybersecurity.

Keywords: Blockchain, Cybersecurity, (VPN) Virtual Private Network, block and ledger.

1-Introduction to Blockchain Technology

Blockchain can be called as a revolutionary technology which has the potential to change various industries and their working mechanisms. It is an open and immutable technology which has practical aspects in various fields. A Block is simply a data structure which has three major components data, Hash of the previous block, timestamp and the transaction data. All these blocks are linked together which creates a dependency between these blocks which ensures the integrity of the whole blockchain. If there is a minor change in hash of any blocks the hash data of the next blocks will be changed as well which leads to a spiral effect where data of subsequent block is changed as well thus rendering them invalid. This is one of the reasons transactions on the blockchain are immutable. As we can see from the above this technology can be highly beneficial in the cybersecurity industry due to its robustness and immutability.

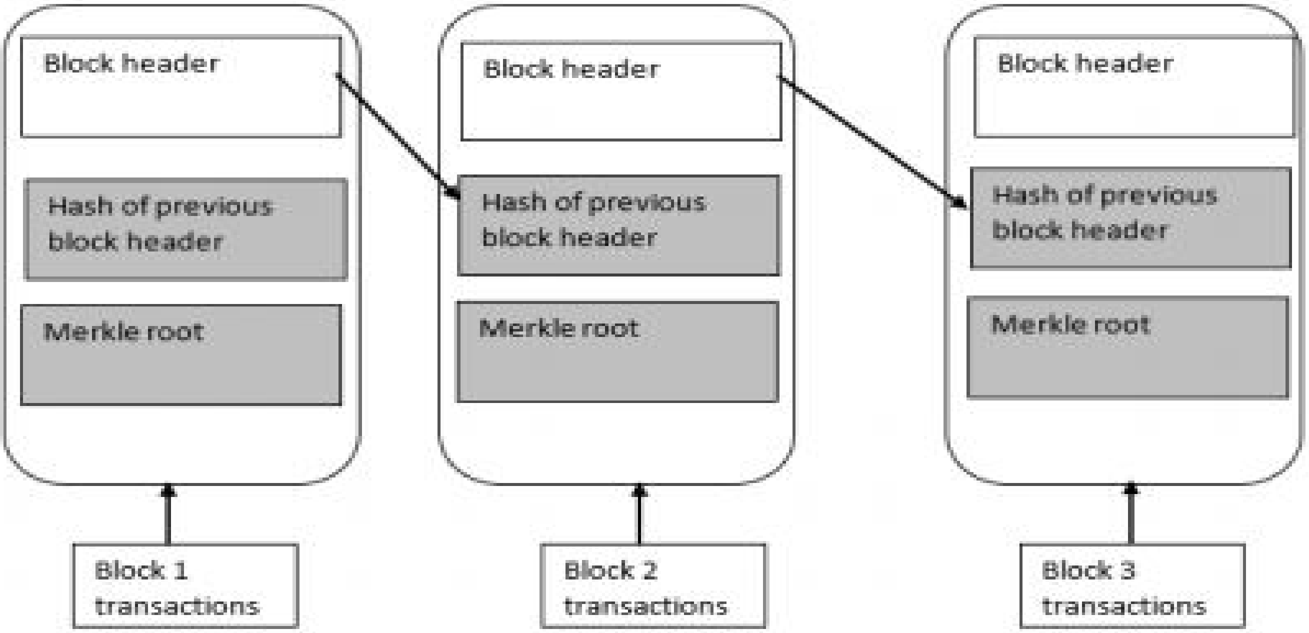


FIG-1 A Block Diagram

2-Some Properties of Blockchain Technology

BlockTransactions are combined into single blocks and in every 10 minutes a new block of about 1MB is formed. Every block consists of 4components, Timestamp, reference to the previous Block, Summary of the included transaction and the Proof of Work that went into creating the secure block.

***Mining*-** Mining means adding transactions records to the blockchain ledger after confirming the validity of transactions. It involves using complicated hardware which performs mathematical calculations which are used to verify transactions. These miners verify the validity of transactions and only then they are put into secure block, miners are also rewarded with certain incentives like Bitcoins and they also get some transaction fees for every transaction that they confirm

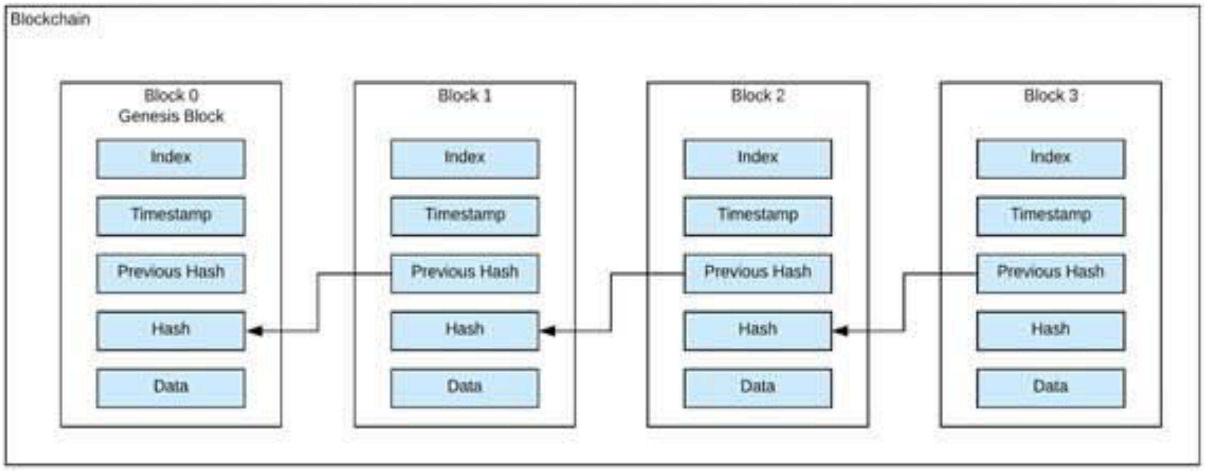
***Proof of work*–** A proof of work is a requirement that expensive computations can be performed in order to facilitate transactions. Proof of work simply exists to enable a trustless consensus. A hash block can be called as proof of work.

***Nodes* —** Nodescan be called as distributed computers in the network that all have a copy of entire blockchain. As soon as new users enter the blockchain network the copies of blockchain and the access to it is distributed. The data is replicable and synchronized and shared all across the nodes across multiple networks. The data does not get controlled by any single authority.

***Smart Contract* —** A smart contract can be called as a digital agreement stored on the blockchain that is unalterable, once signed it dictates some certain logic operations that have to be fulfilled in order to perform tasks such as deposit money or data.

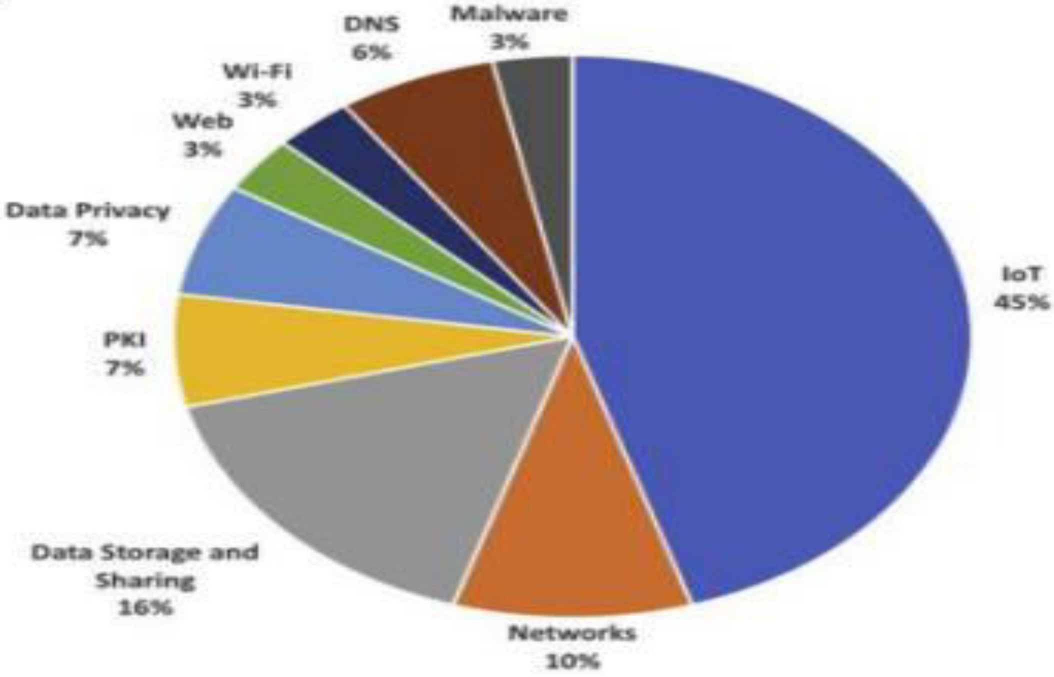
***3-Cybersecurity Context* –**The high level of internet dependency has created new business models and profitable revenue earning sources for organizations but this comes with gaps and opportunities forcybercriminals to exploit. Cyberattacks have become increasingly targeted and advancing everyday due to the sophisticated tools and malwares being built by hackers. These cybercriminals attempt to steal valuable data, confidential information which can be sold to the desired buyers for a high price. In October 2016 one of the biggest domain name service providers experienced a major Denial of Service attack which disrupted the service of several high traffic websites such as Twitter, Netflix, Spotifywhich caused a lot of damage. So how will blockchain help the cybersecurity industry according to ed power's "*Blockchains could potentially help improve cyber defense as the platform can secure fraudulent activities through robust immutable mechanisms*"

***4-Data Access and Disclosure in Blockchain*-**Today, if an attacker gets access to a blockchain network and the data it does not necessarily mean that the attacker can read or retrieve information. Full encryption of the data blocks can be applied to the data being transmitted effectively guaranteeing its confidentiality, considering the latest encryption technologies are followed. Today's cryptographic algorithms, used for public/private key generation, mainly rely on integer factorization problems, which are hard to break with today's computing power. According to Jacky Fox, Deloitte Ireland's Cyber Lead, "Advances in quantum computing will become significant for the security of blockchain due to their impact on current cryptography practice.



***Immutability of Blockchain*-** Blockchain technology may be considered a secure technology, from the purpose of that it permits users to trust that the transactions kept on the tamper proof ledger are valid. the mix of sequent hashing and at the side of its redistributed structure makes it terribly difficult for any party to tamper with it This provides organizations a sense of assurance regarding the integrity and honestness of the information. The accord model protocols related to the technologyconjointly gift organizations with an extra level of assurance over the safety of the information.

***Traceability Factor*-** This issue is one amongst the foremost crucial technology which may be wide employed in cybersecurity business each group action side to a public or personal blockchain is digitally signed and timestamped, which implies that organizations will trace back to a particular fundamental measure for every group action and determine the corresponding party (via their public address) on the blockchain. This feature relates to a very important info security property: non repudiation, that is that the assurance that somebody cannot duplicate the legitimacy of their signature on a file or the authorship a group action that they originated. This out of the box practicality of the blockchain will increase the reliableness of the system (detection of tamper tries or fallacious transactions), since each group action is cryptographically associated to a user.



Most Researched Areas of Application of Blockchain in Security

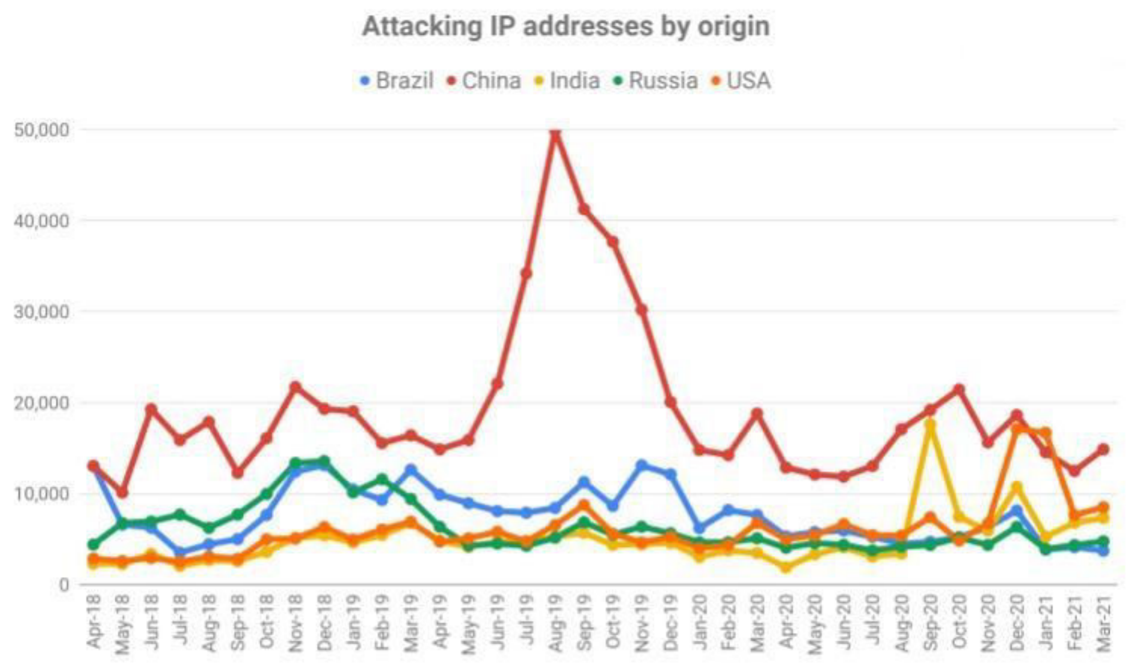
Recently, NASA decided to implement blockchain technology in order to boost cybersecurity, and prevent denial of service and other attacks on air traffic services. They will do this by using the same distributed ledger technology that is often associated with bitcoin and other cryptocurrencies.

5-Blockchain Use-cases in Cybersecurity

***Decentralized Storage Solutions*-** SomeBusinesses are still using centralized storage systems for their data. However, this approach appears to be changing slowly. Blockchain based storage systems are getting popular day by day. This system allows users to archive data on the blockchain and grant permission for accessing third-parties. The Cryptographic access can be revoked anytime, further it reduces the risk of data theft. Thanks to the decentralized storagesystem of blockchain technology, hackers no longer get access to entire repositories of data if they are able to breach the network.

IoT Security- Hackersoften get access to systems by exploiting end devices which includes routers, webcams, smart thermostat, video doorbells etc. Simply put, the security rigorousness is often not applied when ensuring whether these IoT devices are secure. Blockchain can make these Iot devices enough smart to make security decisions without relying on a central authority. Blockchain technology can also protect the data transmission happening between these iot devices. It can be used to attain near real-time secure data transmissions and ensure timely communications flow smoothly between devices located thousands of miles apart.

***Safer Domain Name System (DNS)*-**Dns is a largely centralized technology as a result hackers can break between the name and ip address of website and wreak havoc. They can redirect the users to fraudulent websites to steal confidential information or they can perform DOS attack which can render the website temporarily unusable which causes huge losses to the organization. A blockchain based security system can take one step further mainly because itsdecentralized it would be much more difficult for hackers to find a single point of vulnerability. Your domain information can be stored on an immutable ledger for which the connection can be powered by immutable smart contracts. This can make your DNS extremely safe from attacks.



Attacks on Ip addresses By Origin

Data Integrity In Blockchain

Maintaining Data consistency and guaranteeing its integrity is crucial for information systems. Data encryption and hashing are few methods of maintaining the data integrity regardless of its stage. Blockchain Technology already provides these features which are a means to ensure data integrity. Blockchain technology is regarded a secure technology from the point of users which enable them to trust that the transactions stored on the ledger are valid.

No single Point of Failure-

It can be said that blockchain technology does not have any single point of failure which highly decreases the chances of an DDos attack whichare intended to disrupt the entire operation. If by any chance a node is taken down the data can still be accessible by other nodes within the network since all of nodes contain a full copy of ledger all times. Bitcoin to date is the most tested platform on the blockchain which has withstood several Cyber attacks for more than 8 years.

CONCLUSION

In information security no system can be regarded as 100% secure whatsoever. There is always a possibility that we call safe today can be doomed tomorrow given the lucrative nature of cybercriminals and the criminals ingenuity to seek new methods of attack. Although some of blockchain fundamentals provide data confidentiality and security cybersecurity controls and standards need to be adopted for organizations using blockchain within their technical infrastructure to prevent their network from attacks. It is believed that he best approach and defense strategy to tackle cyberattacks is to continuously update ourselves about the new trends used by cybercriminals so that we can keep our organizations safe as possible.

References

https://builtin.com/blockchain

https://en.wikipedia.org/wiki/Blockchain

https://en.wikipedia.org/wiki/Computer_security

https://www.blockchain-council.org/blockchain/what-is-blockchain-technology-and-how-does-it-work/