Journal of Advanced Research in Business Law and Technology Management
Volume 3, Issue 1 - 2020, Pg. No. 1-4
Peer Reviewed Journal

Article

Blockchain: Sustainability in the Field of Security

Sreeja SS[1], Rashmi Vipat[2]

[1,2]Assistant Professor, Master of Computer Applications, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR), Mumbai, India.

I N F O

Corresponding Author:
Sreeja SS, Assistant Professor, Master of Computer Applications, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR), Mumbai, India.
E-mail Id:
sreeja.s@thakureducation.org
How to cite this article:
Sreeja SS, Vipat R. Blockchain: Sustainability in the Field of Security. *J Adv Res Busi Law Tech Mgmt* 2020; 3(1): 1-4.

Date of Submission: 2020-04-29
Date of Acceptance: 2020-06-05

A B S T R A C T

In today's world, new technology is evolving and existing knowledge is used in different ways. Moreover, people are depending more on technology for sharing information. This leads to evolving nature of security needs. This paper deals with a study on blockchain, the working and types of blockchain, features and numerous uses of blockchain. It also covers advantages of blockchain over traditional system and the security vulnerabilities of blockchain.

Keywords: Sustainability in Security, Blockchain, Cyber Security

Introduction

Cyber security refers to the practices, policies, technologies used to protect data, data and network from illegal access and disclosure. Traditional approach in cyber security was to focus on crucial resources and protect them from attack. Now day's experts are thinking on more proactive and adaptive approaches. To ensure cyber security, we must consider various elements of cyber security also. It includes Application Security, Information Security, Network Security, Business Continuity Planning, Disaster Recovery Planning, Operational Security and End User Education.[3] Sustainable cyber security is an approach in which stakeholder's interaction with ICT systems are clear and deliberate and each participant understood his obligation to preserve and protect the ecosystem for future use.[4] One such approach leads to the introduction of Blockchain Technology. Blockchains can be split into two words: block and chain. Then it can be simply considered as a combination of blocks which are arranged in a sequential order and uses cryptographic methods to create connection between blocks.

Blockchain Technology

According to Wikipedia, a blockchain is a growing list of blocks, cryptography techniques are used to link. Every block includes a cryptographic hash of the earlier block, a transaction data and timestamp. The transactions are verified by network nodes through crypto currency is named Bit coin and recorded in a public Distributed Ledgers Technology (DLT) and decentralized.[1] Blockchain is basically an immutable decentralized, distributed network database which is often known as ledger. Blockchain is about sending and receiving transactions between various users. The process starts when the user launches its transactions using its private key. After that user must find the correct solution for mathematical puzzles using his computational power and then broadcast the transaction. Members start checking and verifying the transaction and if properly propagated towards the main blockchain. this transaction is updated to the main blockchain which updates the state of blockchain and then all nodes will receive the updated blockchain. This process uses a consensus mechanism. Consensus mechanism is a blockchain protocol that is responsible for ensuring that all members of the blockchain are in the same state and all are updated and agree on which transactions are legal and which are not.[2]

Working of Blockchain

Blockchain is a public electronic ledger built around a

P2P system that can be split between users to create an unalterable record of transactions. Each transaction is time stamped and linked to the previous one.[5] Each blockchain comprises of three concepts: blocks, nodes and miners.[6]

Blocks

Multiple blocks are there in each chain and three elements in each block. They are data, nonce and hash. Nonce is a 32 bit whole number which is used only once and generated randomly. A 256 number is linked to the nonce which is considered as hash. When the first block of a chain is created, a nonce creates the cryptographic hash. Every block has its own nonce and hash and reference of hash value of previous block.[6]

Nodes

Nodes can be some sort of device that provides copies of the blockchain and keeps the network functioning. Each node has its own copy of blockchain. Collection of nodes act as network and network has to approve each block added to it . No device in the network can own the chain and this leads to the decentralization concept of blockchain.[6]

Miners

New blocks are designed and added to the existing blocks within a procedure known as mining. Linking blocks is difficult due to the presence of nonce and hash value. Drillers are software utilized to resolve this complexity.

Features of Blockchain

Blockchains have some important features which increases its popularity day by day. They are:

Decentralization

The blockchain network is decentralized. it means the network does not have a person or a governing authority who looks after it. Every node in the network stores the full copy of information. All nodes are the owners of information.[7]

Transparency

All transactions saved in the network are visible to everyone which eliminates the chances of fraud. At the same time the identity of users are protected using cryptography, only public addresses of the users are available.[8]

Increased Capacity

Lots of computers working together offer greater capacity than few of them which are centralized. Large numbers of computers increases the capacity of the network.[9]

Better Security

As networks consist of nodes and transactions are confirmed by nodes, the chance of hacking is reduced. This also reduces the chances of shutting down the network. These factors provide more security.[9] Moreover, the working of blockchain is based on hash function which is irreversible. If someone wants to make changes they have to change in data stored in all nodes.[7]

Persistency

In blockchain transactions once done cannot be deleted. This provides continuity of information in the same state. This feature is achieved by the use of hash function.[8]

Types of Blockchain

Blockchain domain can be divided into 3 different types:

Public Blockchain

It is totally decentralized and everyone can read, send transactions to and share in the agreement process and as its public the numbers of users will be millions.[13]

Private Blockchain

The access is for members only, who can be the co-founder, and number of users can be few thousands. The participants are trusted and known, for example, sub entities companies or business partners.[13]

Consortium Blockchain or Federated Blockchain

As the name is clearly indicated that is controlled by a group of consortium of members. It provides faster or higher scalability, and provide transaction privacy, for example, there is a group of 30 financial institutions, each group of which operates a nod and of which 20 must sign every block for the block to be authorized.[13]

Advantages over Traditional System

There are various advantages of blockchain over traditional systems. Conventional systems are mainly server based systems but blockchain is decentralized, so transactions are end to end. It is also more secure than the traditional system as each transaction in blockchain requires approval from both ends. Once authorization is done, it is encrypted and connection is generated with previous transactions. This also increases security. Another advantage is that the information is not stored on a single computer, it's stored over the network. The next advantage of blockchain is its traceability. In blockchain whenever a transaction occurs its audit trial is generated which contains the full details of that transaction. This facility provides protection from frauds. Another advantage is that blockchain is having more efficiency and speed compared to traditional systems. In blockchain all processes are automated which saves time and requires no human intervention. This increases the speed of transaction and its efficiency.[10]

Security Vulnerabilities of Blockchain

In spite of these advanced features and advantages there are some security loopholes in blockchain which makes it vulnerable. Some of the major loopholes are as follows.

Endpoint Vulnerabilities

Endpoints are the point where people and blockchains meet. It can be considered as a point where an individual or organization meets the technology. The utilization of a blockchain starts with data being stored into the pc and finishes with data being yielded from a PC. This point is most vulnerable.[10]

Social Engineering

Another security issue in blockchain is social engineering. The goal of social engineering is to obtain your private keys, login information or crypto currency. The most common form of social manufacturing is phishing. In phishing, a third party establishes a platform to enter your private credentials and once you enter your specifics they are able to gain access to your account.[11]

Lack of Standards and Regulations

Another major security issue of blockchain is the absence of guidelines and norms. It fails to follow any protocol or organizational decision to provide security.[10]

D Weak Permissioned Network

Ledgers are susceptible to Denial of Service, transaction spamming attacks or control over blocks for creation attacks if not set properly.[12]

E. Weak Application of Pki Based Cryptography and Hashing

Hashing is one of the major features of blockchain. At the same time if the keys used for hashing are not stored properly it can lead to a major security issue. Key distribution should also be done with proper care. This can lead to major issues if not handled properly.[12]

Applications of Blockchain

There are several uses of blockchain. Some of the major applications are as follows.

Healthcare

Personal Health records can be encoded and stored on the blockchain with a private key which would grant access only to certain people. The same approach could be used to ensure that research is conducted via HIPPA Law (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and routinely sent to coverage suppliers a proof of delivery.[14]

Digital Currencies (Decentralized Crypto currencies)

Crypto currencies or digital coins are coins that are passed through an electronic network. You can make transactions by check, wiring or cash. You can also use a type of virtual currency, most famously Bitcoin(BTC) but also Lit coin, Peercoin or Dogecoin among others where you use an electronic coded address to make the transaction. Each block is a digital block that needs to be verified before it's allowed to enter the system. The process not only cuts down on fraud such as double spending or spam, but also transfers funds simply, safely and fast.

Supply Chain Sensors

Sensors give companies end-to-end visibility of their supply chain by providing data on the location and condition of the supplies as they are transported around the globe. 87% of these supply chain companies said they plan to use the technology by 2020. The technology is expected to grow to 1 trillion by 2022 and to 10 trillion sensors by 2030, according to the sme Deloitte and MHI report. The blockchain stores, manages, protect and transfers this smart information.[14]

IoT

Any information object is a thing and it becomes Internet of Things (IoT) when it has an on or off switch that unites it to the internet and to each other. By being linked to a computer network the object, such as a car, develops more than just an object. The analyst firm Gartner says that by 2020 there will be over 26 Billion connected devices. On a large scale, cities and governments can use IoT to develop cleaner environments, more efficient energy use and so called smart cities, to enhance how we live and work.[14]

Insurances

Claims processing can be a disappointing and thankless process. Insurance processors have to wade through fraudulent claims, fragmented data sources or discarded policies for users set state a few and process these forms manually. Room for error is huge. The blockchain requires a perfect system for risk free supervision and transparency. Its encryption properties allow brokers to capture the ownership of assets to be insured.[14]

Conclusion

As the sphere develops progressively connected, the opportunity for attackers is also growing. During 2020 the main goal of cyber security is to safeguard people's privacy, rights and freedom involving bodily safety. All these things are indicating on the issue that data sensitivity will increase in future. Here happens the significance of new technologies like blockchain. The journey of blockchain is still on. New research is required in this field which can surmount the drawbacks of blockchain as it will explode in next years.

References

1. Sahana S. Blockchain Technology-An overview: CSI Communications, Knowledge Digest for IT Community. 2019; 43(6).

2. Singh N, Kaur N, Saini A. Decentralized and Distributed Applications: Future Trends in Industries: CSI Communications, Knowledge Digest for IT Community. 2019; 43(6).
3. https://searchsecurity.techtarget.com/definition/cybersecurity
4. https://www.publicknowledge.org/assets/uploads/documents/Securing_t he_Modern_Economy--Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_ PK.pdf
5. https://www.computerworld.com/article/3191077/what-is-blockchain- the-complete-guide.html
6. https://builtin.com/blockchain
7. https://101blockchains.com/introduction-to-blockchain-features/
8. Kaur D. An overview of blockchain technology: CSI Communications, Knowledge Digest for IT Community. 2019; 43(6).
9. https://data-flair.training/blogs/features-of-blockchain/
10. Sharma A. Blockchain: Security and Concerns and Jatin Arora: CSI Communications, Knowledge Digest for IT Community. 2019; 43(6).
11. https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security- issues-in-2019
12. https://blog.aujas.com/6-security-loopholes-that-threaten-private- blockchains-with-tips-to-secure-yours-against-vulnerabilities
13. Exploratory Analysis of Blockchain Security Vulnerabilities: ISSN: 2200-1872(Print) 2200-1883.
14. https://blockgeeks.com/guides/blockchain-applications/