IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115216

A Systematic Study on Blockchain Security and Privacy

Manjunath R[1], Shruthi S[2], Laxmidevi H M[3], Sumanth V[4]

Professor, Department of CSE, R R Institute of Technology, Bengaluru, Karnataka[1]

Assistant Professor, Department of CSE, R R Institute of Technology, Bengaluru, Karnataka[3,4]

Assistant Professor, Department of CSE, Presidency University, Bengaluru, Karnataka[2]

Abstract: Blockchain is a decentralized ledger that may be used to safely exchange digital currency, make deals, and complete transactions. Each network member has access to the most recent encrypted ledger copy in order to validate a new transaction. The blockchain technology has a number of benefits, including decentralization, trustworthiness, track ability, and immutability. This paper describes the blockchain architecture and explains the concept, characteristics, and importance of blockchain in security, as well as how Bitcoin works and how to improve IoT security. It tries to emphasize the importance of Blockchain in defining the future of cyber security, cryptocurrency, and IoT adoption. This article discusses the importance of blockchain technology in a variety of technological domains, as well as its advantages over traditional systems.

Keywords: Blockchain, Network Security, Bitcoin, Decentralized server, Transactions.

I. INTRODUCTION

The Internet of Things (IoT) is a network that connects various computing units or devices that can send data. IoT expands the capabilities of these devices and the ways in which they can be interacted with. Cloud servers connect the devices, and the data is kept on these servers [1]. Because the data on such servers is trust-based and centralized, it contains numerous loopholes and is prone to security attacks. We need to employ Blockchain technology to make IoT systems secure, trustworthy, decentralized, and even more useful.

Cybersecurity is the protection of any and all systems connected to the internet, including hardware, software, and data, from cyber-attacks. Security encompasses both cybersecurity and physical security in order for businesses to completely protect their systems against illegal access to any data or systems [2]. Cybersecurity refers to the ability to safeguard data integrity, confidentiality, and accessibility.

A cryptocurrency is a marketable digital asset or digital form of money that is exclusively available online and is based on blockchain technology. Cryptocurrencies, as the name implies, rely on cryptography to verify and safeguard transactions. The most fundamental attribute of a cryptocurrency is that it is not controlled by a central authority; the blockchain's decentralized structure allegedly renders cryptocurrencies immune to government control and meddling. Private and public keys can be used to send cryptocurrency directly between two parties. These transactions can be made with cheap processing fees, allowing consumers to avoid the mediator's high expenses.

The major goal of this research paper is to provide guidance in the realm of blockchain technology and to implement it in the areas of cyber security, cryptocurrency, and the Internet of Things.

RELATEDWORK

Jing Li et al. [3] proposed a shared decentralized platform to reduce transaction processing latency caused by difficult math problems and other proof-of-work workloads. Xinle Yang et al. [4] offered a solution to the 51 percent attack on proof of work, which occurs when an attacker has more than half of the total hash power in order to perform double spending.

Shu yin et al. [5] use a Directed Acyclic Graph to improve the linear structure of protocols in standard blockchain systems. Ivan Homoliak et al [6] suggested a security reference architecture based on models of various threat-risks and threats stacked hierarchy using ISO/IEC 15408. S. Pavithra et al. [7] conducted a survey that compared and analyzed key security vulnerabilities in cloud platforms, as well as proposing blockchain technologies as a solution to these difficulties. D. Tanana [8] offered a way for preserving data integrity using the metastable blockchain protocol, as well as discussing the advantages of this method over the standard one in terms of providing better security on various blockchain platforms.

DOI: 10.17148/IJARCCE.2022.115216

II. PROPOSED ALGORITHM

A blockchain is a linked list of blocks connected in a chain. Each block in a blockchain has a hash pointer that ties it to the block before it. A hash pointer contains the hash value of a block at a specific time. This hash value is used to verify that the previous block's contents are accurate.
The genesis block, which is the initial block in the blockchain, has no links to subsequent blocks in the network of chains.

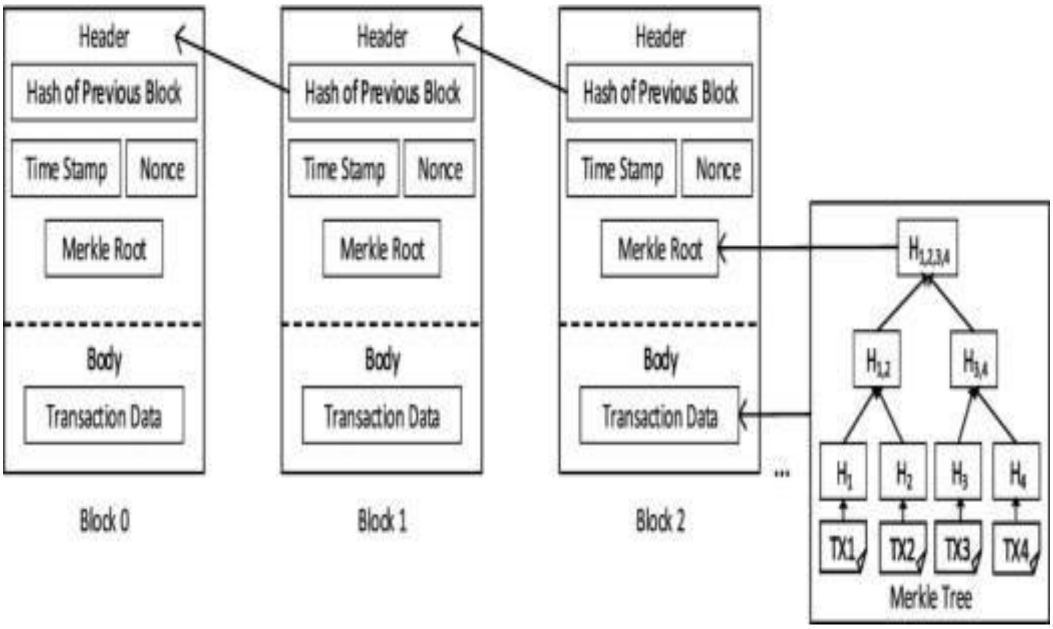

Fig.1. Example of a blockchain

BLOCKSTRUCTURE

Each block, as shown in fig. 1, has a header and a body [10]. The block body contains all of the transactions. A hash value of the previous block connected in the chain, a block created time stamp, a value used only once called Nonce, a hash value of the transactions in a block, and some other related information are listed in the header.
Merkle tree is a tree formed by the root hash value of transactions, as shown in fig.2 with an example of four transactions recorded in the block.

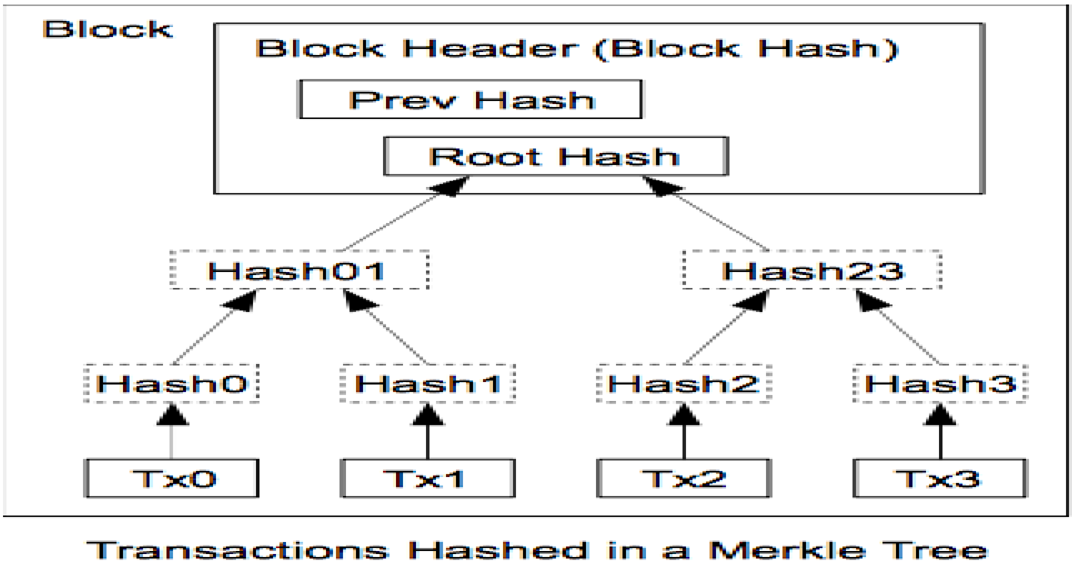

Fig.2. Merkletree.

DOI: 10.17148/IJARCCE.2022.115216

DIGITALSIGNATURE

Digital signatures are employed in blockchain technology to ensure that transactions are valid. Each node has a private secret key that is known to everyone. Every node signs transactions with a secret private key, and other nodes verify the signature with the signer's public key. The usage of a digital signature for document signing and verification is shown in Figure 3.

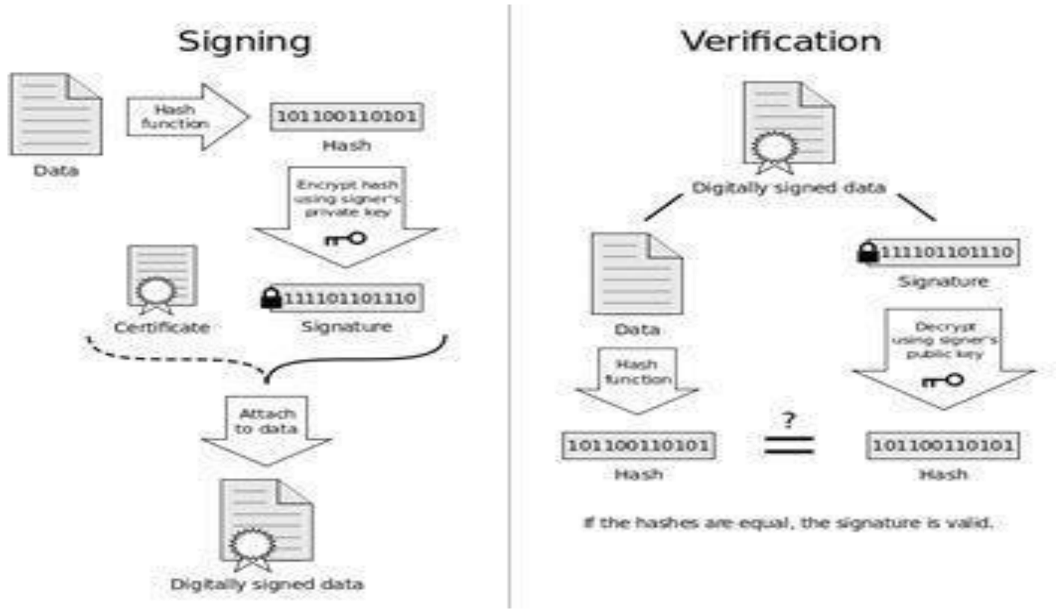

Fig.3. Digital Signature

CONSENSUSPROTOCOL

Before being logged into the ledger, all valid transactions must be validated. The involving nodes utilize a variety of consensus procedures to reach a decision on whether transactions are valid. A user node or a minor node in a blockchain network perform transactions, whereas minor nodes validate transactions, generate new nodes, and maintain the ledger.

The consensus mechanism ensures that the transactions published on the ledger are same to the data on the minor nodes. A set of rules defining consensus is a method that involves all blockchain nodes declaring the same thing in the same post, ensuring that the new block is effectively added to the chain.

Consensus algorithm can be outlined as below:

i. To begin, any new transaction created by any node in the network will be broadcast.

ii. Once the miner nodes have received these transactions, they will generate a new block with the transactional data included.

iii. In each iteration, miner node advertises the newblock created by the node

iv. If a new block contains only legitimate transactions, all other miner nodes in the network agree on that block, and the new block becomes the next block in the chain.

Most used consensus algorithms used are listed below:

1. **Proof of Work [10]:** For producing a block, the mining node must first uncover a nonce, which must then be concatenated with the remainder of the newblock to build a hash for the full contents, with the computed hash value being less than the target hash value.

$$\mathit{Hashfunction}(\mathit{nonc\_value}||\mathit{previoushash\_value}||\mathit{tx1}||\mathit{tx2}||...||\mathit{txn})<\mathit{target}$$

2. **Proof of Stake [10a]:** chosen miner node must keep a stake equal to a percentage of the network's total value. The stake of each miner node is decided by the different apps.

3.

Blockchain functions similarly to a public ledger, except it seeks to ensure the following:

Commitment Protocols: Valid transactions are approved, committed, and incorporated into the blockchain within time limitations.

Consensus: Local copies held by all nodes should be consistent and updated.

DOI: 10.17148/IJARCCE.2022.115216

Security: There's a potential that a few of the nodes will start acting maliciously or that they'll be hacked. It's necessary to have data that can't be tampered with.

Privacy and Authenticity: Data or transactions are generated and held by nodes and that data belongs to those nodes.

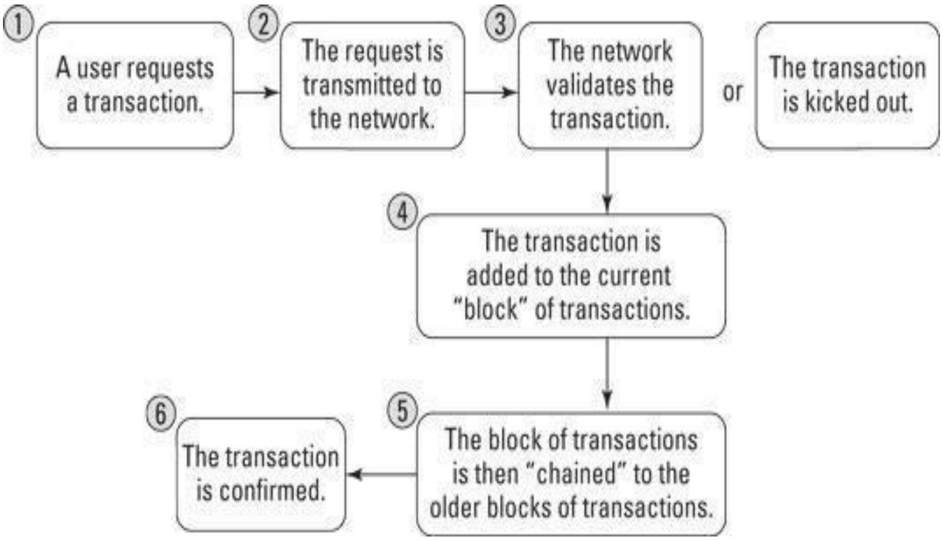
1
A user requests a transaction.
2
The request is transmitted to the network.
3
The network validates the transaction.
or
The transaction is kicked out.
4
The transaction is added to the current "block" of transactions.
5
The block of transactions is then "chained" to the older blocks of transactions.
6
The transaction is confirmed.

Fig.4. How a BlockChain work

III. SIMULATION RESULTS

Blockchain Technology uses a fully decentralized network in order to record and process the information. Ability for optimization and revolutionization of the global infrastructure of the technologies is only present in the blockchain technology. Blockchain technology helps to create a decentralized system that helps to provide interaction among users and the indulgence of central servers will remove. By using blockchain technology a fully transparent and open data base can be created which provides transparency to the users.

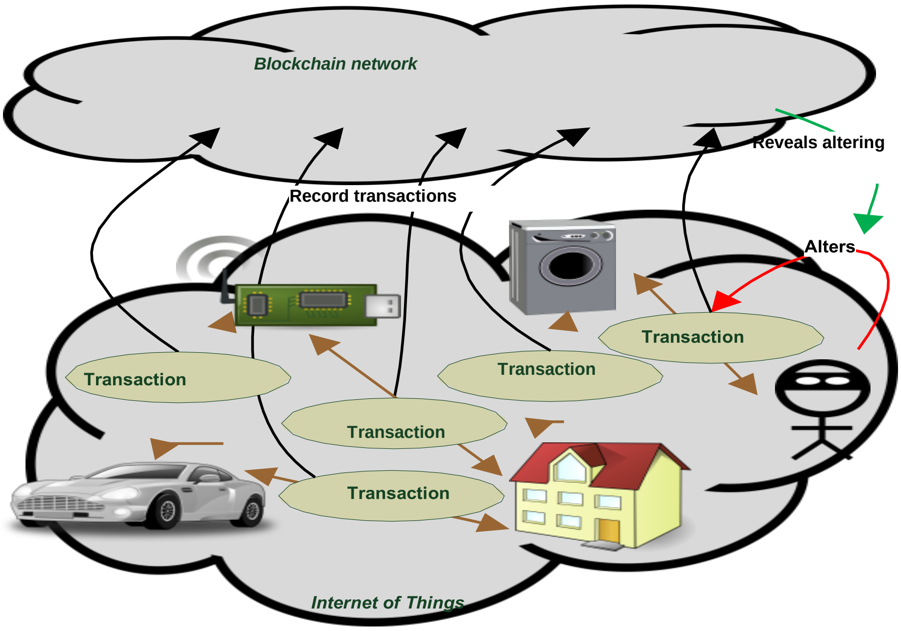

Fig 5: Blockchains For The Internet Of Things – Distributed Tracking Of Transactions Increases Trust By Enabling Detection Of Later Alterations

DOI: 10.17148/IJARCCE.2022.115216

BLOCKCHAIN SECURITY AND PRIVACY

Fifty One Percent attack

A miner with more resources and computational power than other miners in the network will be able to calculate the nonce more quickly using the Proof of Work consensus technique. There is a considerable possibility that a miner with higher computational power will generate a fresh block. A miner on the blockchain network will unquestionably control the entire network if they have 51% more computational power than the other miners [10]. Such a miner can also attack the network with a variety of different forms of assaults, such as selfish mining, repeatedly spending the same coin, commandeering the victim's activities, and blocking important services.

Distributed Denial of Service

Distributed denial of service attack is kind of traffic attack where a dishonest miner node sends plenty of disturbing requests such as invalid blocks, fake transactions to target nodes chosen as victims with help of large number of nodes.
The intention behind this type of attack is to disrupt target node or user system operations. The authors in have proposed Proof of Activity protocol to protect from DDoS attack. The proposed model designed using the aggregation of Proof of Work and Proof of Stake consensus mechanisms. Every miner node makes use Proof of Work consensus approach to create a blank block and transmit its block header to the network. After that, node changes to Proof of Stake consensus approach, a collection of the miner nodes which have transmitted their header to the network decided on to signal the newblock.51percent attack could be defended using the model proposed.

Selfish Mining

In this type of attack, a mischievous or dishonest node, when it finds a new block in the network, hold that block privately and it progress to find extra blocks. Once the dishonest node has a branch, which is kept private to itself, at least two blockslonger in length than the public chain, the dishonest node will broadcast its private chain of blocks to the public. This would be accepted and becomes the new longest valid chain. Problem with this attack is the wastage of the computational power of honest miner nodes.

Injection or Insider attack

Insider attack carried out by an unauthorized user who gains access to some targeted user computer resources and network and manipulates the input to a program processed by interpreter. Unauthorized user who has already gained information of that target system and their administrative privilege manipulates and tampers data. Attacker can modify the system credentials and make it hard for authorized user to access the system.
Following table summarizes the various attacks, threat sand challenges on blockchain.

Security Threats	Definition	Defensive and Preventive Measures
Double Spending	Dishonest node making multiple payments using one body of funds	Increasing the complexity of mining difficulty
51% Attack	Minor node with computation power (51%) more than other nodes to dominate the network for verification and approval of transactions	Detection Techniques; Proof-of-Work Blockchain with History Weighted Information; Delayed proof of work.
Eclipse attack	Isolating and eclipsing the victims' network Connection by flooding them with false data repart.	Peer identification system; Peer selection process; Control connections
Selfish Mining	Dishonest node holding the block privately and adds blocks to generate larger block chain than public blockchain	Freshness Preferred mechanism; Algorithm to detect private blockchains
DDoS	Kindoftrafficattacktodisruptthevictim'sservicesbysendingdisturbingrequests	Peer selection process; Controlling coming and outgoing connections
Identity Theft	Secrete key of an user is stolen	Identify and reputation block chains
Illegal Activities	Parties transact illegal goods or commit money laundering	Detection techniques; laws and regulations

DOI: 10.17148/IJARCCE.2022.115216

IV. CONCLUSION

We conclude that Blockchain technology provides advancement in the field of cyber security, cryptocurrency and IoT. Blockchain Technology is useful for organizations and companies by providing them secure internet data, secure information and provides safety from cyberattacks. The main advantage of blockchain is that it is near impossible to break codes and keys as it combines many devices and computes which are anonymous or decentralized. By using blockchain technology business can easily authenticate users. The device cost is decreasing and computing power is increasing every day therefore Blockchain presents an immense possibility in Internet of Things (IoT) and providing security.

REFERENCES

[1] S. Nakamoto. (2008). Bitcoin: A Peer-to Peer Electronic Cash System. [Online] Available: https: // bitcoin.org / bitcoin.pdf.

[2] BhabenduKumarMohanta,DebasishJena,SoumyashreeS.Panda,SrichandanSobhanayak,"Blockchaintechnology:Asurveyonapplicationsand securityprivacyChallenges",Elsevier,2019.

[3] M. Moser, R. Bohme, D. Breuker ,An inquiry in to money laundering tools in the Bitcoin ecosystem, in: Proceedings of the Crime Researchers Summit (eCRS),2013, IEEE,2013,pp.1–14.

[4] J. A. Dev, Bitcoin mining acceleration and performance quantification, in: Proceedings of the 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering(CCECE), IEEE, 2014, pp.1–6.

[5] Suman Ghimire, Dr. Henry Selvaraj,"A Survey on Bitcoin Cryptocurrency and its Mining", IEEE, 2018.

[6] A. Beikverdi , J. Song , Trend of centralization in Bitcoin's distributed network, in: Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing(SNPD), IEEE, 2015.

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Gold feder," Bitcoin and cryptocurrency technologies: A comprehensive introduction" Princeton University, 2016.

[8] M. Conti, S. Kumar, C. Lal, and S. Ruj, " A survey on security and privacy issues of bitcoin, "IEEE Communications Surveys & Tutorials, 2018.

[9] Anita N, Vijayalakshmi M," Blockchain Security Attack: A Brief Survey ",10th ICCCNT, IEEE, 2019.

[10] Tam T. Huynh, Thuc D. Nguyen, Hanh Tan, " A Survey on Security and Privacy Issues of Blockchain Technology ", 2019 International Conference on System Science and Engineering (ICSSE) ,IEEE, 2019.

[11] Dr. S. Velliangiri, Dr. P. Karthikeyan, "Blockchain Technology: Challenges and Security issues in Consensus algorithm", 2020 International Conference on Computer Communication and Informatics (ICCCI-2020), IEEE, Jan. 22–24, 2020, Coimbatore, INDIA.

[12] Remya Stephen, Aneena Alex "A Review on BlockChain Security ", IOP Conf. Series: Materials Science and Engineering, 2018.

[13] Lu Yanga, "The blockchain: State - of – the –art and research challenges ", Journal of Industrial Information Integration 15 (2019) 80–90.

[14] https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/security-and-privacy-in-blockchain-environments.

[15] M. Rosenfeld ," Analysis of hash rate based double spending, "Available :http://arxiv.org/abs/1402.2009,2014.