JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A STUDY OF SECURITY IN BLOCKCHAIN TECHNOLOGY

Shraddha Yogesh Garg

Assistant Professor, Department of Computer Science, Sabarmati University, Ahmedabad, Gujarat, India

ABSTARCT

Every completed transaction or digital event that has been shared by involved parties is recorded in the blockchain, a distributed database. Most users of the system confirm each transaction. It contains all of the transaction records. The most popular cryptocurrency and blockchain example is called Bitcoin. When "Satoshi Nakamoto" or a group of people going by that name released a white paper titled "BitCoin: A peer-to-peer electronic cash system" in 2008, blockchain technology first came to be known. Blockchain technology makes transactions incorruptible by storing them in a distributed digital ledger. A transaction involving anything of value, such as real estate, cars, and other goods, can be recorded on Blockchain. Blockchain could be a data structure composed of a growing collection of block data representations. The knowledge blocks cannot be taken out or changed because they are interconnected. One cryptocurrency that utilizes blockchain technology is called BitCoin. Transparent information can be transferred throughout a firm network thanks to a sophisticated database technique called blockchain technology. In a blockchain database, information is kept in blocks that are connected to one another in a chain. The data is constant in terms of time since it requires network consensus to remove or modify the chain. Thus, you can use blockchain technology to establish an unchangeable or immutable ledger to record orders, payments, accounts, and other transactions. The system has built-in safeguards that guard against unauthorised transaction submissions and maintain consistency in the shared view of these transactions.

Keywords: Blockchain, Cryptocurrancy, Bitcoin, Distributed database, Network.

1. Introduction

on blockchain, data is stored on a distributed ledger. The blockchain technology provides integrity and availability by allowing participants in the network to create, read, and verify transactions recorded in a distributed ledger. However, it does not support the deletion and change of transactions and other information kept on its ledger. Cryptographic primitives and protocols, such as digital signatures and hash functions, provide support and security for the blockchain system. These primitives ensure transactions in the ledger are integrity-protected, authenticated, and non-repudiated. Blockchain technology requires a consensus protocol, a set of rules that allow all participants to agree on a single record. In a trustless environment, blockchain provides users with desirable properties of decentralisation, autonomy, integrity, immutability, verification, fault-tolerance, which has garnered significant academic and industrial attention in recent years, anonymity, auditability, and transparency. Blockchain technology has gained popularity in academia and industry due to its sophisticated characteristics. We conducted a comprehensive survey and analysis to help users and researchers understand blockchain technology and security issues. We use terms such as blockchain, survey, consensus algorithm, smart contract, risk, and blockchain security to search for relevant articles and material on the internet. Second, we review blockchain-related articles published in prominent security conferences and journals, such as the USENIX Security Symposium, IEEE Symposium on Security and Privacy, and IEEE Transactions magazines. In this method, we assessed as many papers as feasible to eliminate research and result biases. Our survey article includes complete findings from previous studies.

2. Blockchain Technology

2.1 Consensus Algorithms in Blockchain

Blockchain is a distributed, decentralised network that ensures immutability, privacy, security, and transparency. There is no central authority present to approve and verify transactions, however every transaction on the Blockchain is deemed entirely secure and confirmed. This is only feasible because to the presence of the consensus protocol, which is an essential component of any Blockchain network. A consensus algorithm is a technique that allows all peers in the Blockchain network to agree on the current state of the distributed ledger. Consensus algorithms create reliability in the Blockchain network by establishing confidence among unknown peers in a distributed computing environment. Blockchain is a distributed, decentralised network that ensures immutability, privacy, security, and transparency. There is no central authority present to approve and verify transactions, however every transaction on the Blockchain is deemed entirely secure and confirmed. This is only feasible because to the presence of the consensus protocol, which is an essential component of any Blockchain network. A consensus algorithm is a technique that allows all peers in the Blockchain network to agree on the current state of the distributed ledger. Consensus algorithms create reliability in the Blockchain network by establishing confidence among unknown peers in a distributed computing environment.

2.1.1. Proof of Work (PoW): The miner for the subsequent block creation is selected by this consensus algorithm. PoW consensus is utilized by Bitcoin. This algorithm's main goal is to swiftly and efficiently solve a challenging mathematical puzzle. The node that solves this mathematical puzzle the fastest gets to mine the next block because it requires a lot of processing power.

2.1.2. Proof of Stake (PoS): the most widely used substitute for PoW. PoS consensus has replaced PoW consensus on Ethereum. With this kind of consensus approach, validators stake some of the system's coins as an investment in the system rather than spending money on pricey equipment to solve a challenging challenge. All of the validators will then start confirming the blocks after that. Validators will wager on a block that they discover and think has the potential to be added to the chain. Every validator is paid off according to how much they wagered, and their stake rises in proportion to the actual blocks that are added to the Blockchain.

2.1.4. Delegated Proof of Stake (DPoS) is an additional Proof of Stake consensus method. The delegation of votes is the foundation of this type of consensus-building process. Votes are assigned by users to other users. The advantages will be distributed to the people who delegated to that particular vote by the next person who mines the block. See the article Delegated Proof of Stake for further information.

2.1.5. Proof of Elapsed Time (PoET) is one of the most fair consensus algorithms, selecting the next block only based on fairness. It is commonly utilised in permission-based Blockchain networks. In this algorithm, any validator on the network has an equal opportunity to construct their own block. All nodes achieve this by waiting for a random amount of time and then adding proof of their wait to the block. The produced blocks are broadcast to the network for others to consider. The validator with the lowest timer value in the proof portion wins. The block from the winning validator node is appended to the Blockchain.

	PoW	PoS	DPoS	PoET	PBFT
Setup	Public permissionless/ Private Blockchain	Public permissionless/ Private Blockchain	Public/ Private Blockchain	Private permissioned/ permissionless blockchain	Private permissioned non-blockchain
Cost of Entry and Return	Relatively high cost of entry, but high return	Low cost of entry, but low return	Lower cost and lower return than PoS	Very low cost of entry, but low returns	All participate with no return
Scalability in Network	Probabilistic high	Probabilistic medium	Probabilistic medium	Probabilistic medium	Immediate Low
Energy Efficiency	Very low	High	High	High	Medium
Majority or 51% attack	Reduced 25% attack probably	Reduced 51% attack probably	Easier to organize a 51% attack if delegates combine	Reduced 51% attack probably	The number of malicious nodes> one third of all nodes for

			their power		attack
Transactions per Seconds	Bitcoin 7 and max 27	Ethereum 15	EOS 3996 Bitshares 3300	Hyperledger Fabric approx. 3500	IOTA 250

Table 1 Comparison of consensus algorithms

2.2 Smart Contact

A Smart Contract (or cryptocontract) is a computer programme that directly and automatically manages the transfer of digital assets between parties under specific conditions. A smart contract performs the same functions as a standard contract while additionally automatically enforcing it. Smart contracts are programmes that run exactly as they are programmed by their developers. Smart contracts are enforceable through code, just as regular contracts are by law.

- The Bitcoin network was the first to employ smart contracts to transfer value from one person to another.
- The smart contract in question applies fundamental constraints such as verifying that the amount of value to be transferred is truly available in the sender's account.
- Later, the Ethereum platform emerged as a more powerful option since developers/programmers could create custom contracts in a Turing-complete language.
- It should be emphasised that the contracts designed for the bitcoin network were written in a Turing-incomplete language, which limits the possibility of smart contract implementation in the bitcoin network.
- Some popular smart contract platforms are Ethereum, Solana, Polkadot, Hyperledger Fabric, and others.

2.3 Cryptography for Blockchain Technology

Cryptography is a means of protecting data against unauthorised access. Cryptography is used to safeguard transactions between two nodes in a blockchain network. As previously explained, there are two basic ideas in a blockchain: encryption and hashing. Cryptography encrypts messages in a peer-to-peer network, while hashing secures block information and link blocks in a blockchain. Cryptography is largely concerned with guaranteeing the security of participants, transactions, and measures against double spending. It helps to secure various transactions on the blockchain network. It assures that the transaction data may only be accessed, read, and processed by the intended recipients.

Role of Cryptography in Blockchain: Blockchain is built utilising a variety of cryptographic ideas. The advancement of cryptographic technology creates constraints for the future development of blockchain. Cryptography is primarily employed on the blockchain to secure user privacy and transaction information, as well as to assure data consistency. Cryptography's main technologies include symmetric and asymmetric encryption. Asymmetric cryptography employs digital signatures for verification purposes; each transaction recorded to the block is verified by the sender using a digital signature, ensuring that the data is not corrupted. Cryptography is critical to keeping the public network secure, ensuring the integrity and security of blockchain.

Cryptography is a system or set of procedures for protecting information from unauthorised third parties during the course of communication. It is also made up of two Greek concepts, Kryptos (meaning "hidden") and Graphein (meaning "to write"). Some terms linked to cryptography: Encryption is the conversion of normal text into a random sequence of bits. Key: A certain quantity of information is necessary to obtain information about the cryptographic algorithm. Decryption is the inverse process of encryption, which converts a random sequence of bits to plaintext. Cypher: A mathematical function, or cryptographic procedure, that converts plaintext to ciphertext (random sequence of bits).

Cryptography Hash Function in Blockchain

One of the most well-known uses of cryptography is cryptographic hashing. Blockchain immutability is made possible by hashing. Hashing cryptographically does not need the use of keys. Following validation, a transaction is added to the block and a new, distinct hash is generated from the original transaction via the hash algorithm. The original footprint can still be accessed even while hashing is still mixing and creating new hashes. The term "root hash" refers to the single combined hash. Any modifications to the block contents cause the blockchain to collapse. The hash function helps to connect blocks and maintains the integrity of the data included in them. MD5 and SH1 are two hashing methods that are frequently utilized.

Cryptographic Hash Properties: The hash function remains constant for a given message. The hash value will fluctuate significantly in response to any small change in the data. The output hash function cannot be used to infer the input value. Due in great part to their reliance on bitwise operations, they are quick and effective.

Utilizing Hash Functions in Cryptography Since the blockchain is also accessible to the general public, it is critical to secure data there and prevent user data from falling into the wrong hands. Thus, cryptography is an easy way to accomplish this. The transaction is added to the blockchain after it has been validated by a hash algorithm. As more transactions are validated, they are added to the network, forming a chain of blocks. By using mathematical codes, cryptography makes sure that the data can only be accessed by the designated users so they may read it and complete the transaction. With a variety of features, numerous new tools pertaining to the use of cryptography in blockchain have surfaced throughout time.

Advantages of Cryptography in Blockchain

Cryptography has numerous benefits in blockchain, some of which are listed below:

In order to prevent unauthorised exposure and access to information, cryptography uses asymmetric encryption in its network interactions. Blockchain relies on immutability, a cryptographic property that guarantees data stored in the blockchain is reliable and enables blocks to be safely connected by other blocks. Furthermore, from prior questions and their matching signatures, it makes sure that an attacker cannot obtain a legitimate signature for an unposed query.

Security: Cryptography facilitates the recording of transactions by encrypting data and allowing access to data via public and private keys. Tampering with data through cryptographic hashing is impossible making blockchain more secure.

Scalability: Cryptography renders the transaction irreversible, ensuring that all users can rely on the accuracy of the digital ledger. It enables unlimited transactions to be safely logged in the network. Non-repudiation: The digital signature includes a non-repudiation service to protect against any denial of a message sent by the sender. This feature is connected with collision resistance, which means that because each input value has a unique hash function, there is no clash between the messages that are transmitted and one message can be clearly distinguished from the others.

Prevent hackers: The digital signature stops hackers from changing the data because if the data changes, the digital signature is rendered invalid. Cryptography protects data from hackers and makes cryptography in blockchain unstoppable.

3.1 Real attack and bugs with Blockchain Technology

3.1.1. 51% Attack

A 51% attack occurs when a single miner or group of miners controls more than 50% of the network's processing power, giving them the upper hand in the consensus method. This attack vector is mainly associated with the Proof of Work method, but it can also be used as a test case for other consensus algorithms if there is a chance that one party will become powerful enough in the network to unreasonably change the chain's state. This may result in new blocks being added, the chain data being rewritten, and double spending, among other harms. The attack's mechanism is depicted in the diagram that follows.

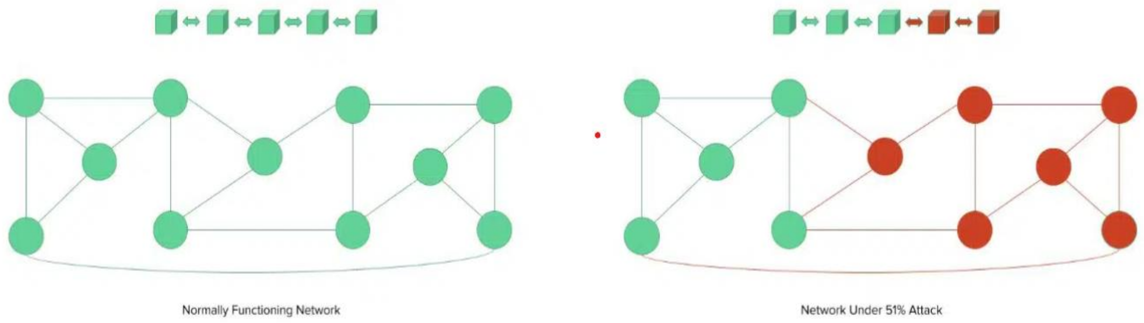

Figure 1 51% Attack

3.1.2. Eclipse Attack

Eclipse Attacks occur in blockchains because of the way the architecture distributes jobs among peers and divides workloads. Each node in a chain, for instance, has view access to only the nodes that are connected to it if the node only has eight outward connections and can sustain a maximum of 128 threads at any one time. If an attacker targets a specific node and takes control of all eight nodes connected to it, the victim node's perception of the chain can be altered. This can result in a wide range of damages, such as assaults on the second layer protocols and double spending of coins by deceiving a victim into believing that a specific transaction has not taken place. By deceiving the victim into thinking a payment channel is available while it is closed, the attacker can force the victim to start a transaction. The diagram that follows shows an Eclipse-attacked node.

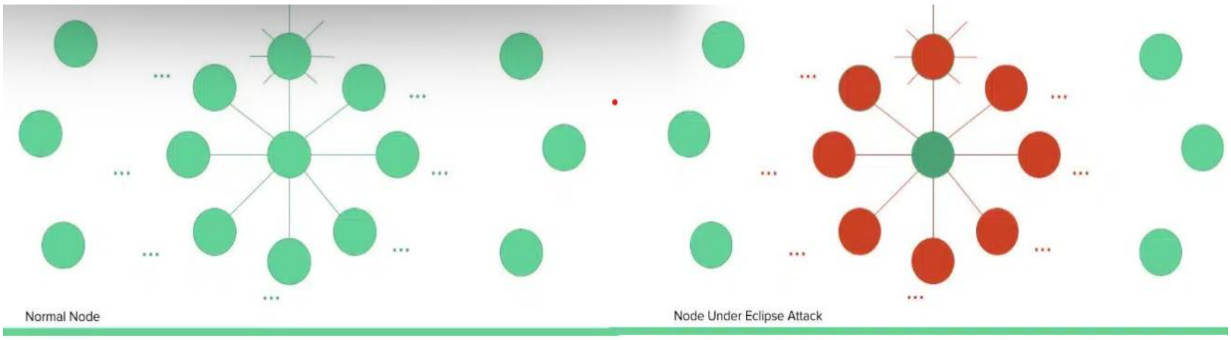

Figure 2 Eclipse Attack

3.1.3. Sybil Attack

The Sybil assault is "a type of attack on a computer network service in which an attacker creates a large number of pseudonymous identities and uses them to gain a disproportionately large influence in order to subvert the service's reputation system." If the victim node doesn't keep track of how many nodes it has in the network, the attacker can completely cut it off. Similar to this, the Sybil attack on the blockchain aims to overwhelm the network with all of the nodes under the attackers' control so that the victim may only connect to those nodes. This might lead to one of three possible actions by the attacker: adding their own blocks to the chain, preventing the addition of legitimate blocks, or confusing nodes, all of which would impair the overall functionality of the blockchain network.

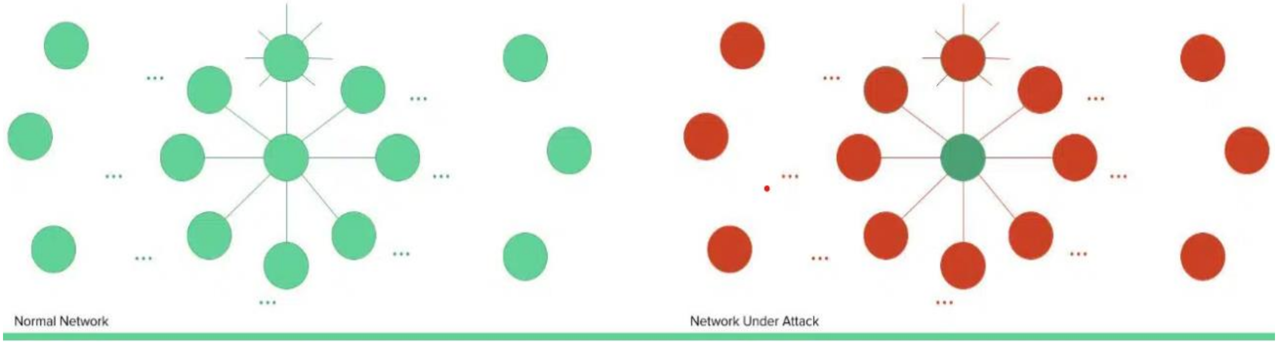

Figure 3 Sybil Attack

3.1.4. Time Jacking Attack

The Sybil assault is also a continuation of the timejacking attack. Every node keeps track of a time counter that is dependent on the peers' median times. If the median times vary by a specific amount from the system times, the node falls back to the system time. A desynchronization can occur when an attacker floods the network with nodes reporting erroneous timestamps, causing it to slow down or speed up.

3.1.5. Fenny Attack

One may see the Finney attack as a continuation of the selfish mining assault. The assailant surreptitiously mines a block and transmits the unverified transaction to the other node, potentially reaching a merchant node. The attacker can quickly add a new block to the chain, reversing the transaction and triggering a double spending attack, if the merchant node approves the transaction. A Finney attack has a very narrow assault window, but if the transaction value is high enough, it can result in significant harm.

3.1.6. Race Attack

In a race attack, the attacker broadcasts two distinct transactions, one to the merchant and one to the network, without pre-mining the transaction. The attacker can broadcast a completely different transaction to the entire network if they are successful in making the merchant node believe that the transaction, they have received is the first one and they accept it.

4.1 Security Measures in Blockchain Technology

Blockchain is an extremely sophisticated system made up of dispersed digital ledgers of blocks of cryptographically signed transactions. The following security features are present in blockchain:

I. A ledger is used by blockchain technology to record every financial transaction. This type of "master" ledger would often be a glaring source of vulnerability. A systemic meltdown might result from a corrupted ledger. For instance, someone may steal an infinite sum of money if they changed a record. Alternatively, they might obtain sensitive personal data if they simply read every transaction. The ledger in the blockchain is decentralized. This implies that no single system or computer is ever in charge of the ledger. To obtain this kind of access to the main ledger, thousands of devices would need to be the target of a highly organized and sophisticated attack at the same time.

II. The chain itself is another security principle. The ledger is made up of a lengthy series of consecutive, cryptographically encrypted blocks. Every link stands for a different component of the whole puzzle. These records go all the way back to the system's inception structurally. This implies that in order to change a transaction, one must first accurately change every transaction that came before it. This adds a great deal of complexity to the imagined tampering procedure. Additionally, it significantly raises the system's overall security.

III. Another security principle is the chain itself. The ledger is composed of an extended sequence of successive blocks that have been encrypted using cryptography. Each connection represents a distinct piece of the overall puzzle. In terms of structure, these records date all the way back to the system's creation. This suggests that in order to modify a transaction, each and every transaction that occurred before it must be precisely modified first. This greatly increases the complexity of the hypothetical tampering process. It also greatly improves the overall security of the system.

IV. In block chain exchanges, the cryptographic keys and two-key mechanism are extremely lengthy, intricate, and challenging to understand unless one is authorized to examine the keys.

5.1 Conclusion

One of the disruptive technologies that has the ability to significantly alter our economy, culture, and society is DLT, or blockchain. Innovative decentralized applications, both financial and non-financial, can be made possible by DLT, doing away with the need for middlemen. This technology is bringing new data management infrastructure that will speed up the services revolution in telecommunications-based businesses like banking and finance, government, healthcare, and super logistics. These provide an important new path for technology development, allowing safe transactions without requiring a centralized authority. Users of telecom services and other businesses will be greatly impacted by this technology, including telecom service providers.

References

1. Zibin Zheng, and et.al. (2017), ”An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.
2. Omar ali, and et.al., (2020), “A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities.”
3. Pankaj datta and et.al. (2020), “Blockchain technology in supply chain operations: Applications, challenges and research opportunities.”
4. Elissar Toufaily, and et.al., (2021), “A framework of blockchain technology adoption: An investigation of challenges and expected value”
5. A Upadhyay, and Et.al., (2021), “Blockchain technology and the circular economy: Implications for sustainability and social responsibility.”