Journal For Re Attach Therapy And Developmental Diversities
EISSN: 2589-7799
2023 September; 6(8s): 941-949

Enhancing Security In Blockchain Technology: A Comprehensive Study

Sudhanshu Verma[1], Mayur Srivastava[2], Shan-e-Fatima[3], Suman Kumar Mishra[4*]

[1,2] Student, M. Tech. CSE (AI & ML)
[3,4*] Assistant Professor, Dept.of Computer Science and Engineering
[1,2,3,4]Khwaja Moinuddin Chishti Language University, Lucknow. E- Mail id: shan.ftm@gmail.com

***Corresponding Author:** Dr. Suman Kumar Mishra

Submitted- 11 June 2023 Revised- 16 July 2023 Accepted- August 2023 Published- September 2023

Abstract

In recent years, concerns about data security have significantly increased, driven by the growing frequency and sophistication of cyberattacks and data breaches. As a result, blockchain technology has emerged as a promising solution for securely storing information. Its inherent characteristics of transparency, immutability, and decentralized trust, facilitated by cryptographic algorithms, make it an attractive option for enhancing data security. However, the question remains: is blockchain completely secure?

This research paper aims to thoroughly analyze and review the security aspects of blockchain technology. We will explore the strengths and weaknesses of blockchain in safeguarding data, examining the various cryptographic techniques it employs, and assessing its resilience against different types of attacks. Additionally, we will investigate real-world applications and case studies to understand how blockchain security is implemented in practice and identify potential vulnerabilities and areas for improvement. By providing a comprehensive overview of blockchain security, this paper seeks to contribute to the ongoing discourse on how to effectively protect data in the digital age.

***Keywords*—** Blockchain, Security, Smart Contract, Ethereum Cryptocurrency

I. INTRODUCTION

Blockchain is a computerized distributed agreement-based technology which ensure proper information repository in a secure way also protect it from tampering in every peered server network. It is a technology that remove intermediaries and create trust through decentralized consensus algorithm. The blockchain technology was introduced in 2008 in a paper called *Bitcoin: A Peer-to-Peer Electronic Cash System*[1]. It is an immutable ledger i.e., once a transaction is recorded then it cannot be tampered by any of the node. If a transaction record has any error, then a reverse transaction would be added to reverse that error and both the transaction would be visible.

Need of de-centralized system: In traditional banking system transaction fee is high. In year 2015 a report provided by CNNMoney and SNL Financial, Bank of America and Wells Fargo make 6 million dollars from overdraft and ATM fees. Every node in the peered server network (a network in which all the computer can act as server for others), has a copy of the blockchain so if anyone anyhow tampers the transaction record then all the nodes will easily detect it. So, to make changes in transaction records you must take control of more than 50% of the majority by redoing the *Proof-of-Work* for each block.

Blockchain uses consensus-based algorithm i.e., group of nodes decides which blockchain transaction is valid and which are not. When a new block gets shared on the peered server, the connected nodes to the network have the right either ignore that transaction to the copy of ledger or to accept it. To achieve consensus, it is compulsion for all the nodes to decide on a single state. Blockchain uses different consensus algorithm such as Proof of Work, Proof of Stake, Proof of Burn and Proof of Elapsed Time.

1. **Proof of Work:** It is the algorithm based on agreement where each node takes part and tries to solve a cryptographic hash algorithm based mathematical problem. Miner gets a tip when they solve the difficult mathematical problem. *For example, Bitcoin miners gets a reward of 12.5 bitcoins when they solve the mathematical problem*.

The node must perform various mathematical operations to prove that transaction involved is valid. After transaction gets verified rest of the clients join the transaction to the digital ledger. In distributed network, when two or more entities obtain suitable nonce then authorized block gets produced. This algorithm wastes the provided resources because the node has to perform various mathematical operations. [2].

2. **Proof of Stake:** It is also a consensus algorithm. In this algorithm the generator of new block is chosen on the basis of its wealth/stake. During designing of the block, the nodes which are taking part are required to offer few assets. The assets get refunded as a bonus when the formed block gets verified. It would be fined if this is not the case.[2].
3. **Proof of Burn:** Proof of Burn is the agreement-based algorithm in which nodes send their coins to an irrecoverable address in order to burn them. It is energy efficient but could consume a large amount of virtual currency or token[3].
4. **Proof of Elapsed Time:** This is the agreement-based algorithm developed by Intel in which a waiting time is given to each node. The timer is different for each node. The first participant to finish waiting time gets the chance to commit the upcoming block to the blockchain network.

II. Comparison of different agreement-based algorithms

Consensus algorithm Parameter	**Proof of Work algorithm**	**Proof of Stake algorithm**	**Proof of Burn algorithm**	**Proof of Elapsed Time algorithm**
Threshold for Attack[2]	33.33%	51%	23%	25%
Energy Consumption[2]	High	Moderate	Moderate	High
Verification speed[3]	>100s	<100s	-	-
Application	Bitcoin	Cardano	Slimcoin	Hyperledger Sawtooth

III. Smart Contracts

Nick Szabo had termed "Smart Contract" in the mid-1990s[4]. Smart Contracts are computerized contracts which gets executed by itself and contain the terms and conditions of a consent between the nodes in the form of program. To write the smart contracts, Solidity and Serpent programming languages are used.
Clack et al. has put forward a definition of smart contract in which smart contract has been described as "an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code."[5]
The example of Ethereum Smart Contract is *AXA* (is an insurance company) flight delay insurance.
For the evaluation of Smart Contract, they are acknowledged to the nodes on EVM. EVM (Ethereum Virtual Machine) is a compiler which is used to execute smart contract's code.
Basically, Smart Contracts are immutable contracts which are more secure and efficient than traditional contracts.

A. Comparison of Smart Contract v/s Traditional Contract

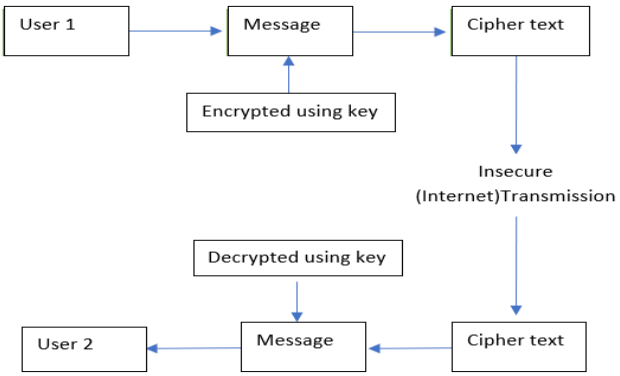
	TRADITIONAL CONTRACT	**SMART CONTRACT**
MEDIATOR	ADMINISTRATION, ATTORNEY…	NO THIRD PARTY
IMPLEMENTATION TIME	SOME DAYS	FEW SECONDS
PAYMENT	NOT AUTOMATIC PROCESS	COMPUTERIZED
TRANSPARENCY	NOT AVAILABLE	FEASIBLE
MAINTAINING RECORD	CHALLENGING	SIMPLE
SAFETY	LITTLE (CAN BE COMPROMISED)	SECURE
COST	HIGH COST	INEXPENSIVE
SIGNATURES	NON-AUTOMATIC PROCESS	COMPUTERIZED SIGNATURES

IV. Cryptography

While transferring data between two nodes it is necessary to maintain:
1. Privacy
2. Incorruptibility
3. Acknowledgement
4. Verification

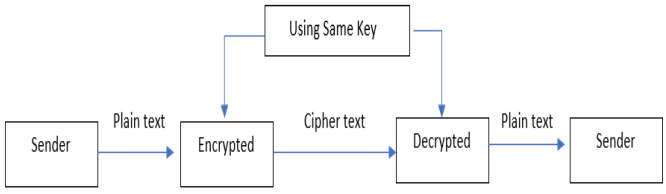
To maintain Privacy, Incorruptibility, Acknowledgement, and Verification we use cryptography.

'Crypt' means 'secret or hidden.' Cryptography is a method of securing the transaction, from unauthorized access, taking place between two nodes in the blockchain network. In cryptography the message is encrypted in to cipher text by sender node using key and then can be decrypted using another key by the receiving node. Cryptography is the key to the security in blockchain.



Cryptography can be categorized as:
1. Symmetric or Private key Cryptography
2. Asymmetric or Public key Cryptography

Symmetric key Cryptography: In this cryptography, nodes share the identical key to encode or decode the messages. It depends on a single key to encode and decode data. The key must be kept confidential and made accessible to both the sender and the receiver. The power of encryption depends on the key size used. Do not send the key to the recipient a long with the cipher text because it defeats the whole purpose of using encryption. Key exchange can be done in advance using other algorithms such as the Diffie-Hellman key exchange protocol.



Types of encryptions used in Symmetric key Cryptography:
1. Stream Ciphers
2. Block Ciphers

Overview of Stream Cipher and Block Cipher

Stream Cipher	**Block cipher**
Encrypt information one bit at a time.	Information broken down to blocks of fixed size.
Quicker format of encryption and decryption.	Size of blocks depend on key size.

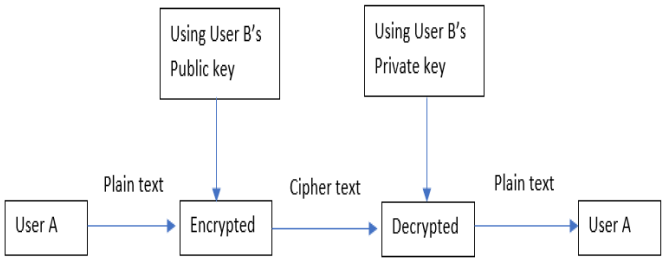
Data is converted to binary digits and encrypted sequentially.	The blocks are encrypted and later chained together.
Popular algorithms are: RC4, SALSA20	Popular algorithms are AES, DES, 3DES
Faster as they work on single byte.	Slower but tamper-proof.

Advantages of Symmetric-key Cryptography:
1. Faster than asymmetric-key cryptography.
2. Better performance metrics.
3. Optimized for bulk amount of data.
4. Easier to set up and implement.

Disadvantages of Symmetric-key Cryptography:
1. Same key for encryption and decryption means single point of failure.
2. Key always need to be always kept secret.
3. Receiver can also generate message with the same key, so authentication issue will arise.

Applications of Symmetric-key Cryptography:
1. Banks uses Symmetric-key Cryptography to authenticate ID and transactions.
2. It can also be used at Server/Data Centre to encrypt information at REST.

Asymmetric key Cryptography: In this Cryptography two non-identical keys are used to encode and decode the messages. In asymmetric key cryptography the data is encrypted using public key and decrypted using private key. The public key is shared with everyone, and it cannot be used to decode the information and the private key can decode the information, but it need not shared with anyone. Public keys and Private keys are mathematically linked to each other. Since this encryption is highly secured therefore it can be used where we need high confidentiality.



Since the key needed to send a message is publicly available therefore asymmetric key cryptography is also called as public key Cryptography.
Applications of asymmetric key cryptography:
1. Computerized signatures to maintain originality of documents.
2. It manages secure crypto-currency transactions.
3. It protects from hackers by encrypting browsing sessions.

Advantages over Symmetric key cryptography:
1. No need of sharing secret key.
2. Longer key length means stronger encryption.
3. Proof of owner's authenticity.
4. Data cannot be modified in transit.

V. Architecture of Blockchain
Blockchain consists of following components:

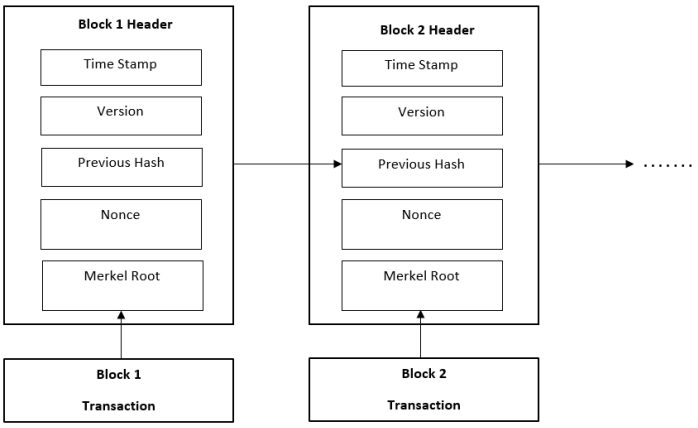
1. Nodes
2. Block
3. Transactions

4. Miners
5. Consensus

Nodes – Nodes are the systems connected in the p2p network in blockchain

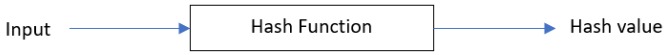
Blocks – Block can be called as container or data structure which contains a set of confirmed transactions. Transactions are stored on hard drives of nodes.

Structure of Block:
A block mainly consists of two parts-
1. Block Header – It contains details such as Time stamp, Version of blockchain, Merkel Root, Nonce, Previous Hash.
2. Transactions – It is the record of data in chronological order. Transactions are stored in a Merkel tree inside the block. The transactions when submitted are chosen up by the blockchain network and is inserted into 'Pool of unconfirmed transactions. The transactions on blockchain network that has not been confirmed yet are collected in transaction pool.



Architecture of Blockchain

VI. Hashing
It is the mechanism of converting input of arbitrary length in to output of fixed length called Hash value. Hashing is done with the help of **Hash functions**. It is different from encryption because encrypted data can be decrypted to get the original data, but hashing cannot be reversed.

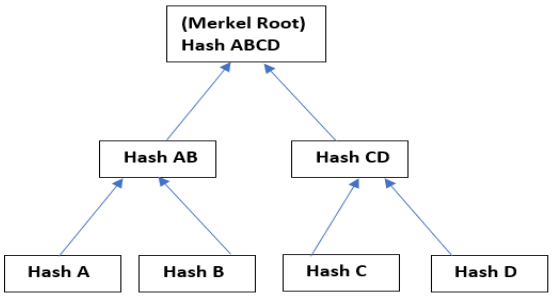


Based on different types of algorithms used in Hash function we get different length of output, but input can be of any length (from 1 bit to millions of bit).
The most popular algorithm used in Hash function is SHA (Secure Hash algorithm) built by NSA (National Security agency).
The Hash function must have the following properties:
1. **Deterministic –** Hash function should give some hash value for some input.
2. **Fast Calculation –** The hash of input has to be returned quickly by hash function.
3. **Pre-Image Resistance –** It means that it is not possible to control input data based on output hash.
4. **If input changes then output will also be changed.**
5. **Impervious to collision**– Two different inputs cannot have same hash value.
6. **Puzzle friendly**

VII. Merkel Tree

Computerized fingerprint of the entire set of operations can be generated using Merkel tree which allow the user to authenticate whether a transaction is included in the block. A Merkel tree also totals all transactions in a block. It acts as summary of all transactions. Merkel tree also helps to verify the consistency and content of the data.

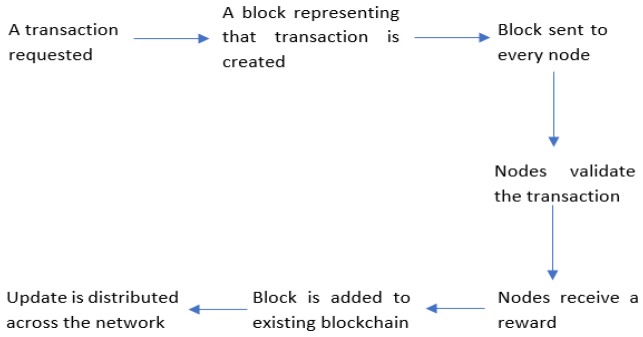
Merkel tree are formed up by hashing pairs of nodes again and again until only one hash remains. This hash is called as Merkel root.



VIII. Working blockchain transaction

Step 1. A user creates a transaction from their wallet, attempting to send currency or data to someone else.
Step 2. The transaction is put across a 'a pool of unconfirmed transactions.
Step 3. Miners on the blockchain select transactions from these pools and form them into a 'block'.

Step 4. Once the block is created, miners generate a block signature. This signature is created by solving a complex mathematical problem. Each block has a different mathematical problem as per the transactions.
Step 5. The miner that finds a target signature for its block first, broadcasts this block and the signature to all other miners.
Step 6. Other miners verify the signature if it is valid, the other miners will confirm its validity and agree that the block can be added to the blockchain. This process is also termed as consensus



IX. Blockchain examples

1. Walmart Food Tracking – It may take days or weeks to find the source of food poisoning. That's why Walmart has developed a food traceability system based on his Hyperledger Fabric. Walmart conducted two of his POCs with IBM to test the system. Mangoes sold in US Walmart stores were the first to be tracked, and pork sold in stores in China was another. Tracking improved from his 7 days to his 2.2 seconds.

2. Honeywell Marketplace - To cut purchasing time for aerospace products from days or weeks down to seconds and to connect each physical part to its digital equivalent So, Honeywell created an online marketplace system based on Hyperledger Fabric. Tracking of new and old parts for aircrafts is done with the same. Also, it created a trust system due to cryptography as most purchases happened using bonds. Any seller can launch his/her own selling system for aircraft parts using Honeywell solution known as Go Direct.

X. Security

Security of blockchain can be summarized by studying recent incidents:

1. Exploited Code: The DAO which was deployed on 28th May of 2016 is a smart contract which carry out a crowd-funding platform. It was attacked only after 20 days it has been established[7]. This event showcased privacy and security issues of Decentralized autonomous organization (DAO) blockchain wherein engineers were fixing a problem with

regards to program malfunctioning. During this hour an anonymous hacker started depleting the DAO of ether collected from the sale of its tokens. The hacker managed to deplete 3.6 million ethers by Saturday, 18th June.

2. Missing Keys: There have been cases wherein Bitcoins have been stolen. A prominent one happened from Hong-Kong based Cryptocurrency exchange Bitfinex. The amount stolen was close to $72 million and it proved out that the most probable cause for the event was private keys which was stolen.

3. Hacking Employee System: Bitthumb is another example of security issues in blockchain. It is one of the biggest cryptocurrency exchanges for Bitcoin based out in South Korea. The attackers were capable to dig into information of around 30,000 customers alongside stealing Bitcoin which cost around $35 million in this incident.

4. In November of 2014, Mt. Gox was handling over 70% of all Bitcoin transaction when it fell victim to an attack that cost 850,000 bitcoins, valued at 450 million at the time and 7.9 billion at the time of this writing. This attack has been running for years and was largely due to poor management and poor security practices.[6]

XI. Things which raises question about security of blockchain

Sybil Attack: In Sybil attack a single rogue identity (a hacker) creates fake identities (also known as Sybil identities) to overwrite honest nodes in the network. The attacker's goal is to separate the target node from the other honest nodes on the blockchain network. Attackers can carry out various forms of double-spend attacks against a target by refusing to transfer transactions and only transferring blocks that the target has created, allowing the target to confirm. Specific transactions can be filtered for double spending if the destination accepts 0 transactions or disables anonymization protocols such as Tor or JAP. [6]

51% Attacks: In 51% attack a group of miners control more than 50% of the network's mining hash rate or processing power. If an attacker accomplishes this, new transactions may fail to receive confirmations, halting payments between some or all network users. You can also undo transactions completed while in control of the network So, you can double spend your coins.
In 2018, his three reputable cryptocurrency platforms faced the problem of his 51% attack. Three prominent platforms are Ethereum Classic, Zen Cash and Verge.
Some companies lost nearly $20 million in 2020 alone to 51% attacks.

Routing attacks: All blockchain networks and applications rely on massive amounts of real-time data transfer, so all an attacker needs to do is interfere with the data being sent to your internet service provider. For example, a hacker can use routing attacks to divide a network into two (or more) separate components. The attacker can force the creation of parallel blockchains by preventing nodes inside the component from communicating with nodes outside the component. Once the attack is over, all blocks mined with small components are destroyed along with all the transactions and miner earnings they contain.
routing attacks can exfiltrate sensitive data or gain financial gain without warning network participants.

Blockchain endpoint vulnerabilities: A point where an individual is accessing any form of data could be an endpoint. Most attackers spend a lot of time attempting to steal an end user's keys because they are aware of that there is no use in pursuing to find end user's keys. On attacking the weakest point in the entire network i.e., personal computer or smartphone, the attacker can obtain keys. Endpoints becomes sensitive while accessing blockchain in order to receive that data.

Vendor Risks: It is common for vendor solutions to have fixed focus on security area while having poor security controls on their systems, improper code and even personnel vulnerabilities which can easily expose their user's blockchain testimonials to uncertified users.

Transaction Privacy leakage: The architecture of public blockchain networks makes every transaction traceable. These transactions are open and transparent. The consensus among distributed nodes can be reached due to the publicity of this data. Transactional privacy leaks can pose significant problems for some blockchain applications such as the Internet of Things and mobile crowdsourcing.
The correlation between different transaction addresses could be exposed by analysing the transaction graph. The user's identity can be revealed from any additional data collected elsewhere using this correlation.

Phishing attacks: Phishing attack is primarily a scamming attempt to get the testimonials of a user. In this attack, attacker send emails to the owners of wallet key by posing as a certified trustworthy source. The attacker request information

about credentials with the help of pirated hyperlinks and after getting these credentials, the user as well as blockchain network are open to successive attacks. In year 2020 there were about 100,100 phishing has been reported.

Eclipse Attack: Ethan Heiman et. al. has presented eclipse attack on blockchain. [8] It is a kind of attack in which a hacker takes over all of the target's arriving and departing connection and tries to separate a target from the remaining nodes of the blockchain[6]. Eclipse attack can lead to performing double spending.Eclipse attack can only be performed on nodes that accept incoming connections.

XII. Previous Works on Security of Blockchain

REFERENCE NO.	YEAR	FOCUS AREA	OUTCOME
[9]	2018	51% ATTACK	The writer applied the 51% attack strategy to simulate the attacker's behavior and obtained the changing trend of the number of states and the number of attacks. After receiving this data, they evaluated the security of each state on the blockchain.
[10]	2020	Risks to blockchain and security enhancements.	The writer conducted a systematic examination on the security risks, its cause and possible consequence.
[2]	2020	Security and Challenges in blockchain	The author summarizes security improvements in the blockchain space.
[11]	2018	Security and attacks in blockchain such as DDOS attack, time jacking attack, etc.	The writer evaluated the security of blockchains, especially Bitcoin, Ethereum and Hyperledger networks.
[12]	2018	Vulnerabilities in Smart Contract and DAO Attack.	Author given a brief explanation of various flaws in Smart Contracts and comparison of vulnerabilities detection capabilities of various tools.
[13]	2019	Brief survey on security in blockchain	Attacks on blockchains and how to mitigate them are detailed in the paper. Provides a comprehensive overview of attacks and solutions against blockchain systems.
[14]	2019	Security and privacy in blockchain	The study found that some work has been done on privacy and security issues, but much needs improvement.
[15]	2020	Security threats in blockchain such as 51% attack, phishing, major bugs, etc.	The main security vulnerabilities covered in this article.
[16]	2019	Types of Attacks on blockchain and defense mechanism.	The authors suggested future research directions to improve blockchain security and privacy.
[6]	2019	Different types of vulnerabilities in blockchain and security issues for different aspects.	The author introduced new research directions in blockchain technology.

XIII. Analysis of Blockchain

Based on the all the study, blockchain can be summarized on the basis of SWOT i.e., Strength, Weakness, Opportunities and Threats.

1. **Strengths:**
- Immutability
- Transparency
- Decentralized
- Creating Trust through Algorithm
- Using Smart Contracts

2. Weakness:
- Wastage of resources
- Storage
- Complex
- Slow Speed
- As blockchain says it will replace the banks but VISA can handle 1000 transaction/sec but Bitcoin can only handle 7-10 transactions/sec.

3. Opportunities

- Can be used in maintaining records of real estate property.
- Can be used in Voting in elections.
- Opportunities in IOT[17]
- Smart Contracts in insurance[17]
- Speedup bank processes[17]

4. Threats

- Disappearance of existing bank jobs[17]
- Privacy and security
- 51% Attack
- Lot of research need to be done

Conclusion

Blockchain is peer-to-peer network which ensures secure storage of information protected from revision and tampering by using different algorithms and removes third parties by using smart contracts. It can bring more benefits than traditional database as it is the most secure way for storing data but it has drawbacks too. In this survey paper we have analyzed the security vulnerabilities of the blockchain on the basis of recent incidents and previous researches. Finally, we summarized the blockchain on the basis of its Strengths, Weakness, Opportunities and threats.

REFERENCES

[1] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system.
[2] Ghosh, Arunima, et al. "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects." Journal of Network and Computer Applications 163 (2020): 102635.
[3] Khan, Fakhri Alam, et al. "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development." Sustainable Cities and Society 55 (2020): 102018..
[4] Szabo, Nick. "Formalizing and securing relationships on public networks." *First monday* (1997).
[5] Clack, Christopher D. "Smart Contract Templates: legal semantics and code validation." *Journal of Digital Banking* 2.4 (2018): 338-352.
[6] Dasgupta, Dipankar, John M. Shrein, and Kishor Datta Gupta. "A survey of blockchain from security perspective." Journal of Banking and Financial Technology 3.1 (2019)
[7] Li, Xiaoqi, et al. "A survey on the security of blockchain systems." Future Generation Computer Systems 107 (2020): 841-853.
[8] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in USENIX Security Symposium, 2015, pp. 129-144.
[9] Ye, Congcong, et al. "Analysis of security in blockchain: Case study in 51%-attack detecting." 2018 5th International conference on dependable systems and their applications (DSA). IEEE, 2018.
[10] Li, Xiaoqi, et al. "A survey on the security of blockchain systems." Future Generation Computer Systems 107 (2020): 841-853.
[11] Moubarak, Joanna, Eric Filiol, and Maroun Chamoun. "On blockchain security and relevant attacks." 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). IEEE, 2018.
[12] Mense, Alexander, and Markus Flatscher. "Security vulnerabilities in ethereum smart contracts." Proceedings of the 20th international conference on information integration and web-based applications & services. 2018.
[13] Anita, N., and M. Vijayalakshmi. "Blockchain security attack: a brief survey." 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2019.
[14] Mohanta, Bhabendu Kumar, et al. "Blockchain technology: A survey on applications and security privacy challenges." Internet of Things 8 (2019): 100107.
[15] Oksiiuk, Oleksandr, and Iryna Dmyrieva. "Security and privacy issues of blockchain technology." 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET).
[16] Huynh, Tam T., Thuc D. Nguyen, and Hanh Tan. "A survey on security and privacy issues of blockchain technology." 2019 international conference on system science and engineering (ICSSE). IEEE, 2019
[17] Niranjanamurthy, M., B. N. Nithya, and S. J. C. C. Jagannatha. "Analysis of Blockchain technology: pros, cons and SWOT." *Cluster Computing* 22.6 (2019): 14743-14757.