Blockchain Vulnerability and Cybersecurity

[1]Sanjay S, [2]Praveen S Kamath

[1]Undergraduate Student, [2]Associate Professor
Department of Computer Application,
SCMS School of Technology and Management, Cochin, India

***Abstract*: Blockchain technology has earned significant attention due to its different use cases and potential for disruption. One of the most reasons blockchain is so prevalent is its characteristic structure – it uses peer-to-peer networks and registers to store transactions, and is outlined as a computerized log file and stored as a series of connected groups, or blocks. Each and every block is locked cryptographically with the previous block, and once a block has been included, it cannot be changed. It has brought enormous potentials in numerous fields, such as financial services, energy, healthcare and Internet of Things. As often happens with innovative technologies, it has endured from several critical Cybersecurity threats and vulnerabilities.**

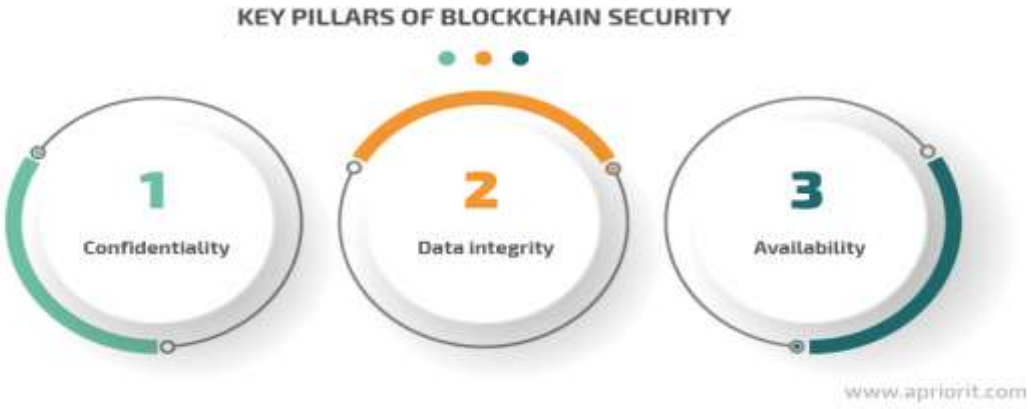
***Index Terms*: Blockchain, Cybersecurity, Trends and stat, Blockchain in Cybersecurity, Blockchain vulnerability, Blockchain for Cybersecurity pros and cons.**

I. INTRODUCTION

Blockchain innovation has ended up a design that move to computerized exchanges. It happens with innovative technologies additionally endured from several critical Cybersecurity threats and vulnerabilities. The connection between Cybersecurity risk management and operational objectives that makes to identify, analyze and control the relevant risk occasions as a major challenge. It uses peer-to-peer networks and registers to store transactions, and is designed as a computerized log file and stored as a series of linked groups, or blocks. Each and every block is locked cryptographically with the previous block, and once a block has been added, it cannot be modified.

THREE ELEMENTS OF BLOCKCHAIN SECURITY:
The technological complexity of blockchain innovation raises a few concerns with respect to its execution and sustainability.

1. **Confidentiality**: The blockchain provides extensive capabilities for guaranteeing a user's secrecy. User keys are the only interface between a user and their information. However, these keys are too simple to anonymize. Some networks utilize non-interactive zero-knowledge proofs to maximize users confidentiality. As a result, while being open and offering rich opportunities for transaction tracking, a blockchain permits users to preserve an exceptional level of secrecy.



2. **Data integrity**: Blockchains are planned as records where every block is connected to adjacent blocks using cryptographic hash functions. In this manner, once a transaction is recorded on the blockchain, it can't be modified or erased. Any changes made to the as of now recorded information are handled as modern exchanges.

3. **Availability**: Having a large number of nodes guarantees blockchain versatility even when some nodes are inaccessible. And as each hub within the network has a duplicate of the distributed record, the correct blockchain remains accessible to other peers even within the case of a compromised node.

II. BENEFITS OF BLOCKCHAIN

- Eliminate the necessity for centralized control and therefore the additional costs
- Trust is distributed among blockchain members.
- Transactions are carefully signed utilizing an asset owner public/private key pair.
- Once recorded, data during a block cannot be altered retroactively.

- Distributed ledgers record transactions between two parties efficiently and during a verifiable and permanent way.
- Transactions don't need to be just data – they can even be code or smart contracts.

III. BLOCKCHAIN USED CASES

1) Cryptocurrency

Risk: encrypted digital currencies distinguish the currency itself, but not its owner. Whoever holds the coin's encryption key claims the currency. this proposes that when a coin is stolen, it's gone—and you have got no way of getting it back.
Solution: storing your encryption keys during a fips-validated root of trust is critical to making sure you own your keys and ultimately your cryptocurrency.

2) Smart contracts

Risk: a smart contract may be a computer program that describes an agreement with the power to self-execute and enforce the terms of a contract. If the blockchain is breached, a smart contract are often altered, breaking the trust of the blockchain and removing the power for 2 parties to conduct business without the necessity for middleman.
Solution: securely self-execute the terms of a contract with anonymous parties through strong authentication and storing your encryption keys during a hardware root of trust, ensuring the parties are properly identified which nobody can access your data.

3) Internet of things (IOT)

Risk: the restrictions imposed by a standard central-authority trust model have helped make the IOT vulnerable. Most notably mirai-style botnets, which recently allowed hackers to simply take over thousands of IOT devices. Only securing the IOT devices with default passwords allowed hackers to launch distributed denial of service (DDoS)attacks.
Solution: Blockchain helps to secure the IOT by providing a distributed trust model. The blockchain removes the single-point-of-failure, successively enabling device networks to guard themselves in other ways, for instance by allowing the nodes within a given network to quarantine any nodes that start behaving unusually.

IV. ADVANTAGE

1. **Process Integrity:** Due to the security reasons, this program is made in such a way that any block or even a transaction that adds to the chain cannot be edited which ultimately provides a maximum range of security.
2. **Traceability:** The format of Blockchain designs is in such a way that it can easily locate any problem and correct if there is any. It also creates an irreversible audit trail.
3. **Security:** Blockchain technology is highly safe because of the reason each and every individual who enters into the Blockchain network is provided with a unique identity which is linked to his account. This make sure that the owner of the account himself is operating the transactions. The block encryption in the chain makes it harder for any hacker to disturb the traditional setup of the chain.
4. **Faster processing:** Before the invention of the blockchain, the normal banking organization take tons of time in processing and initiating the transaction but after the blockchain technology speed of the transaction increased to a really high extent. Before this, the general banking process takes around three days to settle but after the introduction of Blockchain, the time reduced to just about minutes or maybe seconds.

V. DISADVANATAGE

1) Power Use: The consumption of power within the Blockchain is relatively high as during a particular year the power consumption of Bitcoin miners was alone over the per capita. Keeping a real-time ledger is one among the reasons for this consumption because whenever it creates a new node, it communicates with each and every other node at the same-time.

2) Cost: As per the studies as a mean cost of the Bitcoin transaction is $75-$160 and most of this cost cover by the energy consumption. There are very fewer chances that this issue we can resolve by the advancement within the technology. because the other factor that is the storage problem could be covered by the energy issues cannot be resolved.

3) Uncertain regulatory status: In each and every part of world modern money has been created and controlled by the government. It becomes a hurdle for Bitcoin to urge accepted by the pre-existing financial institutions.

VI. CYBERSECURITY

Cybersecurity is a way of protecting computers, mobile devices, servers, data, networks, and electronic systems from malicious attacks. some of you may realize it as electronic information security or Information technology security.

TYPES OF CYBERSECURITY

- **Network Security**: It is mainly the practice of securing any kind of computer or server networks from intruders. Furthermore, they might be opportunistic malware or any kind of targeted attackers.
- **Information Security**: This kind of cybersecurity will secure privacy or data or the integrity of any kind of information in storage or anything that's being transmitted.
- **Application Security**: These are mainly the safety protocols that keep the devices or any program freed from malware. actually, a compromised device or application offers access to the knowledge that it had been meant to guard. Furthermore, a successful security process will begin within the application phase before the appliance can even affect the devices

- **Operational Security**: Mainly this sort of security handles all the choice or processes needed for protecting all the data assets. Furthermore, it's an umbrella term because tons of processes falls under the category. Actually, the permission levels or user access restriction rules fall into here. Furthermore, determining where and the way the knowledge would be stored is additionally a big part of this matter.
- **Business Security**: It's one among the main security procedures. actually, business security would require a mixture of all the cybersecurity categories. However, they may require on an outsized scale. Also, a business has got to maintain the firewall service once they have minimal assets or resources. Thus, many security protocols are made to use less resource but offer more outputs.

Disaster Recovery: It's a necessary a part of every cybersecurity protocol. Any organization or individual would need to possess responsibility for any incident or loss of data. Furthermore, it's more sort of a backup plan, if somehow the safety did not stop the attack.

VII. BLOCKCHAIN IN CYBERSECURITY

- Traditional security solutions are not capable of handling cyber-attacks with an increasing number of complex and cooperating machines. So blockchain security in the mix can really help to be the comprehensive solution for the issues.
- The cybersecurity sector is loaded with issues and more or less a fragile cyber solution isn't capable of handling all the different kinds of threats. Thus, blockchain can be the most promising solution.
- A firewall technology offers a lot of security protocols that they've been gaining a lot of praises from all the industries using it. So, it can easily fend off cyber-attacks. They can use the method to lock out the compromised nodes and saving the whole network. Moreover, you can see that blockchain security actually uses several strength systems to offer the redundancy and tamper proof republication mainly.
- It could mean that hackers may take down a few of the troops, but they can't take down the overall Blockchain security army so with blockchain security on the mix, no industrial operation or information storage is left to depend solely on the single vulnerable system. Here the blockchain and cybersecurity help it to become more scalable and disruptive.
- It means that most security policies, such as flow controls or rotating passwords, would get controlled more diversely. Only authorized persons can get access to specific controls.
- These controls would be used tamper-proofed and by all the nodes on the blockchain and cybersecurity network. Therefore, it forms a self-protecting firewall. Thus, it doesn't have any single point of failure and there would be no unauthorized access to the network or no accidental changes in the blockchain security network.
- If you are confused about whether blockchain security can be the solution, you can surely say that it most certainly can. However, many people do not know what type of blockchain security solution they need as the cybersecurity itself has different types. So, before picking out the solution, the organizations need to know what type of use cases the blockchain security has.

VIII. ATTENTION-CATCHING CYBERSECURITY TRENDS & STATS

- **Bitcoin involved in Almost $76 Billion of Illegal Activities**: Unlike other currencies, Bitcoin offers an incredible sort of quick transactions with anonymity and safety. The cryptocurrency is not regularized by legacy government currency rates. This has quickly transformed it into the foremost preferred mode of anonymous operation in illegal activities just like the cybercrime and drug trade.
- **Ransomware Attack Every 14 Seconds:** It is estimated that in every 14 seconds, an individual or company falls victim to a ransomware attack. this is often consistent with the 2019 Official Annual Cybercrime Report (ACR) that also indicated that the majority of those attacks go unreported. With a replacement person joining social media platforms every 15 seconds, the ransomware vulnerability scope continues to widen.
- **Small Businesses are the first targets of Cyber-attacks:** Most small businesses consider themselves 'unlikely' to suffer from cyber-attacks. according to reports by Cybint, two-thirds of companies have experienced attacks like social engineering incidents, phishing, and DDoS attacks within the last three years. Small businesses continue being the littlest investors in cybersecurity despite making up 13% of the cybercrime market.
- **Cyber threat Costs:** As per the safety Intelligence Report, the common cost of a cyber-attack data breach as of 2019 was $3.92 million. On the contrary, the value of hacking is nearly insignificant, with cyber-attack tools now available on the Dark Web for as low as one dollar, with other complementary services being offered for free of charge. It becomes more alarming that it takes a mean of 5 minutes to hack an IOT device.

IX. BLOCKCHAIN FOR CYBERSECURITY PROS AND CONS

The blockchain has rich potential as a cybersecurity measure, this technology is also related to several risks.

CONS:

- Scalability challenges
- Reliance on private keys
- Adaptability challenges
- Risk of cyberattacks
- High operation and customization costs
- Blockchain literacy
- Lack of governance

PROS:

- Secure data storage and processing
- Safe data transfers
- No single point of failure
- Data transparency and traceability
- User confidentiality
- Increased customer trust

X. BLOCKCHAIN VULNERABILITY

The risk of making vulnerabilities runs high as human developers will naturally make errors, which can, unfortunately, be exploited by appalling parties. Besides human-related vulnerabilities, blockchain itself possesses variety of vulnerabilities and risks. A number of these risk are explained:

- **51% attack**: It may be launched to arbitrarily manipulate and modify blockchain information. For popular blockchains, attempting this type of heist is probably going to be extremely expensive. Renting enough mining power to attack Bitcoin would currently cost over $260,000 per hour. But it gets less expensive quickly as you progress down the list of the over 1,500 cryptocurrencies out there.
- **Private key security**: Once a user's private key is lost, it cannot be recovered. If the private key is stolen by criminals, the user's blockchain account are often tampered by others and since there are not any centralized institutions that manage the blockchain, it's difficult to trace the criminal's behaviours and recover the modified blockchain information.
- **Double spending**: Double spending refers to a consumer who uses an equivalent cryptocurrency multiple times for transactions. An attacker could leverage a race attack to initiate double spending – the attacker just must exploit the intermediate time between two transactions' initiation and confirmation to quickly launch an attack. Before the second transaction is mined to be invalid, the attacker already got the primary transaction's output, leading to double spending.
- **Transaction privacy leakage**: Because user behaviours in blockchain are traceable, blockchain systems got to protect the transaction privacy of users. In practice, users got to assign a private key to every transaction so attackers cannot determine whether the cryptocurrency in several transactions is received by the same user. Unfortunately, privacy protection measures in blockchain aren't very robust, and a few research found that 66% of transactions sampled do not contain any mixins, or chaff coins, that forestalls attackers from inferring the linkage.

Table 2: Taxonomy of blockchain's risks

Number	Risk	Cause	Range of Influence
3.1.1	51% vulnerability	Consensus mechanism	Blockchain1.0, 2.0
3.1.2	Private key security	Public-key encryption scheme	
3.1.3	Criminal activity	Cryptocurrency application	
3.1.4	Double spending	Transaction verification mechanism	
3.1.5	Transaction privacy leakage	Transaction design flaw	
3.2.1	Criminal smart contracts	Smart contract application	Blockchain2.0
3.2.2	Vulnerabilities in smart contract	Program design flaw	
3.2.3	Under-optimized smart contract	Program writing flaw	
3.2.4	Under-priced operations	EVM design flaw	

XI. LITRATURE REVIEW

Blockchain technology has garnered significant attention thanks to its various use cases and potential for disruption. It first manifested because the technology behind the cryptocurrency Bitcoin, which experienced a precipitous rise and subsequent crash at Hollywood-esque proportions, but is now in use by other businesses also. one among the most reasons blockchain is so popular is its inherent structure – it uses peer-to-peer networks and registers to store transactions, and is meant as a digital log file and stored as a series of connected groups, or blocks. Each and every block is locked cryptographically with the previous block, and once a block has been added, it cannot be altered.

Blockchain may be a revolutionary idea. it has directly impacted different industries out there. However, blockchain isn't free from risks. The risks are often associated with technology, implementation, investment, legal, operational, security, finance, and other aspects directly or indirectly associated with blockchain.

Data across the web is not safe. Data is that the most integral and important a part of any system and will be guarded with utmost security. Centralized data storage is an open window for hackers and is extremely susceptible to cyber-crime and illegal usage. Although there are advanced and fool-proof cyber security mechanisms in place to tackle these, they'll not be fully equipped to overcome new and complicated cyber-attack techniques devised by hackers. As a results of which, strengthening cyber security methods is usually a top priority for all of the industries and subsequent organizations.

Blockchain are often duplicated and shared across the entire network of computer systems on the Blockchain. Every participant within the Blockchain has access to the records of all transactions or updates on that. This database is named Distributed Ledger Technology (DLT). The transactions within the Blockchain are stored with a hash, which is an unchangeable cryptographic signature. A hash is nothing but special algorithms. this suggests that it is an immutable ledger with high data security. If one block

within the chain is altered, it becomes quite apparent. it might be very difficult for hackers to be ready to force and entry the system without changing every block within the chain across all distributed versions.

XII. FUTURE WORK

The suggested Blockchain Technology future researches are: Healthcare, public sector, Blockchain as a Service (BaaS), IOT, Energy-aware, large-scale applications, Smart Contracts, Consensus mechanism.

XIII. CONCLUSION

The impact of Blockchain security function as well as other functions that may lead to threats. The paper explores the real attacks on the Blockchain systems. It is crucial to understand the scope, and impact of security and privacy challenges in Blockchain to predict the possible damage. The future Blockchain researches still promising in different applications. One of the important research topics is Bitcoin because it's used on a daily basis in cryptocurrency transaction. Consequently, it will attract the industry and academia to conduct more researches. But there are other domains the researchers can use Blockchain Technology and still has a remaining challenges and open research issues needed to be solved. The blockchain offers rich opportunities for maintaining a high level of knowledge safety because of reliable encoding mechanisms, data integrity, network resilience, and scalability. As a result, switching from a standard system to a blockchain-based system are often beneficial to organizations in almost any industry.

XIV. ACKNOWLEDGMENT

I would like to thank my guide Mr. Praveen S Kamath for his proper guidance and support for helping me to complete this research paper.

REFERENCES

[1] Abdelwahed, Nagy Ramadan, Hesham Ahmed Hefny ,2020," Cybersecurity Risks of Blockchain Technology", Reserachgate
[2] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen,2020," A Survey on the Security of Blockchain Systems", Researchgate
[3] https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons
[4] https://101blockchains.com/blockchain-security/#3
[5] https://cpl.thalesgroup.com/encryption/blockchain
[6] https://101blockchains.com/enterprise-blockchain-risk-assesment/#prettyPhoto
[7] https://101blockchains.com/blockchain-risks/
[8] https://blockchainsimplified.com/blog/is-blockchain-the-answer-to-cyber-security-threats/
[9] https://www.kaspersky.com/blog/secure-futures-magazine/blockchain-business-vulnerabilities/35713/
[10] https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors
[11] https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/
[12] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf
[13] https://onlinedegrees.und.edu/blog/5-blockchain-security-issues/
[14] https://intellipaat.com/blog/future-of-blockchain-technology/#no3
[15] https://www.plugandplaytechcenter.com/resources/hacking-blockchain-blockchain-security-concern/
[16] https://thenextscoop.com/blockchain-technology-impact-cyber-security/
[17] https://medium.com/hackernoon/using-blockchain-technology-to-boost-cyber-security-19b6ef4e6898
[18] https://www.evershedssutherland.com/global/en/what/articles/index.page?ArticleID=en/Diversified-industrials/Blockchain_supply_chain_risk_analysis
[19] https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity
[20] https://ieeexplore.ieee.org/abstract/document/7918009/references#references
[21] https://builtin.com/blockchain/blockchain-cybersecurity-uses
[22] https://ieeexplore.ieee.org/document/8725596
[23] https://101blockchains.com/disadvantages-of-blockchain/