e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

BLOCKCHAIN CYBER SECURITY VULNERABILITIES AND POTENTIAL COUNTER MEASURES

Loganathan R[*1], Hariharan SB[*2], Hariharan R[*3], Haridharan A[*4], Kubendiran E[*5], Vignesh K[*6]

[*1]Assistant Professor, Department Of Cybersecurity, Paavai Engineering College, Namakkal, Tamil Nadu, India.

[*2,3,4,5,6]Student, Department Of Cybersecurity, Paavai Engineering College, Namakkal, Tamil Nadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS45781

ABSTRACT

Blockchain technology has garnered significant attention due to its wide array of potential applications, initially emerging as the foundation for the cryptocurrency Bitcoin. However, it has since found utility across various industries and non-commercial domains. Unlike most prevailing systems based on centralized architectures, this innovative approach employs peer-to-peer networks and a distributed system utilizing a blockchain ledger to establish connections. Its framework functions as a digital log, organized into a series of interconnected units known as blocks. Each block is cryptographically secured to its preceding block, rendering it immutable once added. Many experts believe that the inherent cryptographic nature of blockchain systems makes them resilient against constant hacking attempts and security threats. Nonetheless, prior research on the security and confidentiality of blockchain technology has revealed instances where applications have succumbed to sophisticated cyber-attacks. With the increasing demand for cryptocurrencies and the existing security challenges, earlier studies did not extensively focus on the cybersecurity vulnerabilities of blockchain technology. Consequently, our research endeavors to shed light on potential attacks targeting the weaknesses in blockchain technology's cybersecurity.

Keywords: Block Chain, Cloud Computing, Cyber Security, Ledger, Smart Contracts, Cryptocurrency, Attacks, Consensus Algorithms, Distributed Ledger Technologies, Security.

I. INTRODUCTION

The cybersecurity framework encompasses various elements involved in safeguarding networked computers and data from digital threats. Its objective is to prevent, detect, recover from, and respond to internet-based threats, which come in diverse forms such as unauthorized access or use of information resources and network attacks that disrupt, deny, degrade, or destroy information and network resources. These threats encompass information theft, computer viruses, website tampering, denial-of-service attacks, network intrusions, and data manipulation or creation. The security infrastructure is designed to protect against these risks, ensuring the confidentiality, authenticity, integrity, and availability of data.

Blockchain serves as a transaction database containing records of all previously executed transactions, operating on the Bitcoin protocol. It creates a digital ledger of transactions, allowing all network participants to modify the record securely, shared across a distributed network of computers. To modify existing data blocks, all nodes in the network execute algorithms to evaluate, verify, and match transaction information with the Blockchain history. If the majority of nodes agree on the transaction, it is confirmed, and a new block is added to the existing chain.

The Blockchain metadata is stored in Google's Level DB by the Bitcoin Core client. Conceptually, Blockchain can be visualized as a vertical stack of blocks placed on top of each other, with the bottommost block acting as the foundation. Each block is linked to the previous one and refers to the preceding block in the chain. Blocks are identified by a hash generated using the secure hash algorithm (SHA-256) cryptographic hash function on the block header. A block has one parent but can have multiple children, each referring to the same parent block, thus containing the same hash in the previous block hash field. Each block contains the hash of the parent block in its own header, and the series of hashes linking individual blocks with their parent blocks form a significant chain pointing to the initial block, known as the Genesis block. Blockchain technology (BT) is a decentralized transaction and data management technology that provides security, confidentiality, and data integrity without involving any third-party organization responsible for the transactions. BT includes value management capabilities by utilizing electronic receipt records for transactions performed over the internet. Blockchain technology is also applicable in finance, gaming, gambling, supply chain, manufacturing, trade, and e-commerce sectors. The BT system is a permanent database of all historical transactions stored as a digital record. In the decentralized blockchain network, every user node has the authority to oversee the communal ledger. These blocks are systematically connected, forming chains where the initial block acts as the foundation. Each block is intricately linked to its predecessor within the chain. Utilizing advanced cryptographic hash algorithms, each block is distinctly identified by a unique hash. A block in the chain can have only one immediate parent block but multiple child blocks. A block contains a header, consisting of a unique hash of its parent blocks that links it to its parent blocks, forming a chain. The blockchain technology system acts as a digital proof of ownership, functioning as a decentralized database system, maintaining a continuously growing list of transaction records, which differs from traditional centralized record systems.

II. METHODOLOGY

The adoption of Blockchain Technology in Bitcoin, introduced in November 2008, has significantly fueled the growing interest in BT. Bitcoin, functioning as a decentralized peer-to-peer digital currency, meticulously records all digital transactions on a public ledger. These transactions, shared among participating parties, are verified by a consensus of members within the collaborative network. Once data is recorded during a digital event, it becomes immutable, providing Bitcoin with a real-time and transparent record of every transaction. However, Bitcoin's security remains a contentious issue within the digital currency market.

Nevertheless, Blockchain Technology has found diverse applications in both financial and non-financial sectors. A Blockchain establishes a distributed consensus in the digital realm, offering entities a secure platform that maintains historical records of digital events by creating an immutable ledger in a public domain. Activities associated with Blockchain Technology are categorized into three groups concerning organization and functionality:

(a) First-Generation Public (Blockchain 1.0): Involves cryptocurrencies in financial applications like money transfers, cash settlements, and digital payments.

(b) Second-Generation Public (Blockchain 2.0): Incorporates smart contracts for financial markets and applications, adding complexity to straightforward monetary transactions. This category encompasses stocks, bonds, loans, contracts, titles, smart properties, and smart contracts.

(c) Third-Generation Private (Blockchain 3.0): Extends to applications beyond currencies, money, and markets. This includes sectors such as government, healthcare, science, education, culture, and arts. Blockchain within this category is considered private.

Blockchain technology is a promising innovation that could mitigate the risk of cyber-attacks directed at a single point, potentially minimizing the impact on the entire system. However, a coded intrusion or system vulnerability could lead to severe consequences for the system's security. For example, a successful attacker could gain access not only to the information stored at the point of attack but also to all data recorded in the ledger. Therefore, security concerns related to blockchain are critical in terms of cybersecurity. Security experts need to thoroughly comprehend the scope and impact of security measures related to Blockchain before predicting the potential damage from an attack. They must verify whether current technology can withstand persistent hacking attempts.

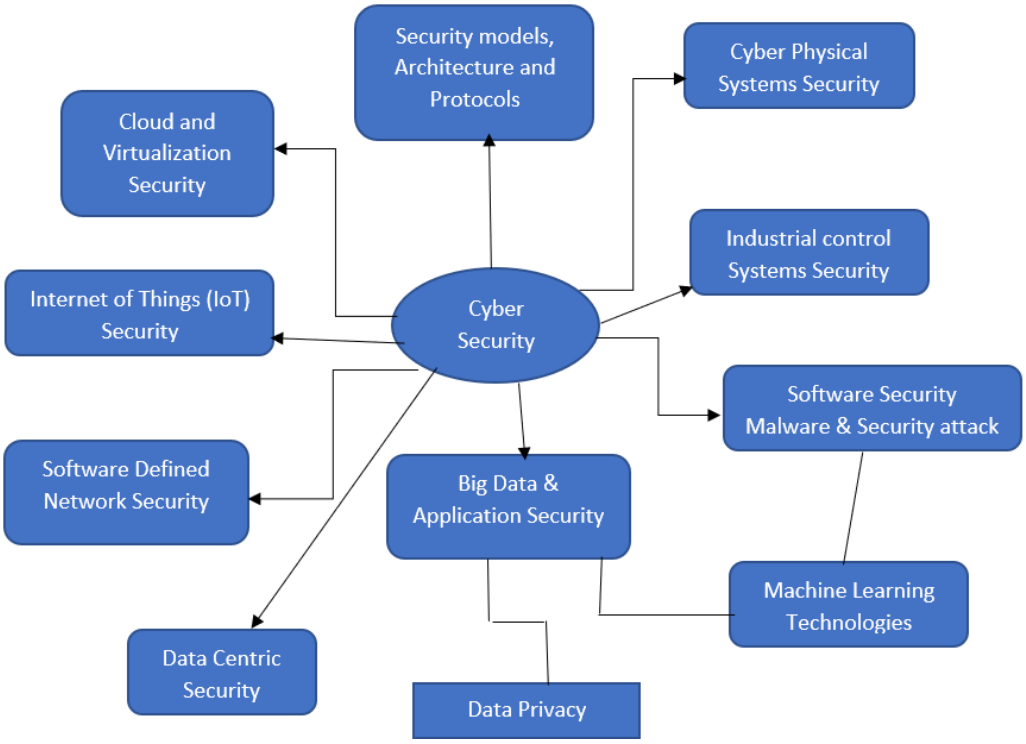
Security models, Architecture and Protocols
Cyber Physical Systems Security
Cloud and Virtualization Security
Industrial control Systems Security
Internet of Things (IoT) Security
Cyber Security
Software Security Malware & Security attack
Software Defined Network Security
Big Data & Application Security
Machine Learning Technologies
Data Centric Security
Data Privacy

Figure 1: Cyber Security approach related technological branches

Previous studies have delved into the technical architecture of Blockchain Technology (BT) concerning cryptocurrencies. While some research has focused on the security aspects of BT, given the rising demand for cryptocurrency and its existing security challenges, these studies have paid limited attention to BT cybersecurity vulnerabilities. Given these circumstances, our research presents a comprehensive review of Blockchain Technology security attacks by exploring attack vectors that specifically target user security and its vulnerabilities.

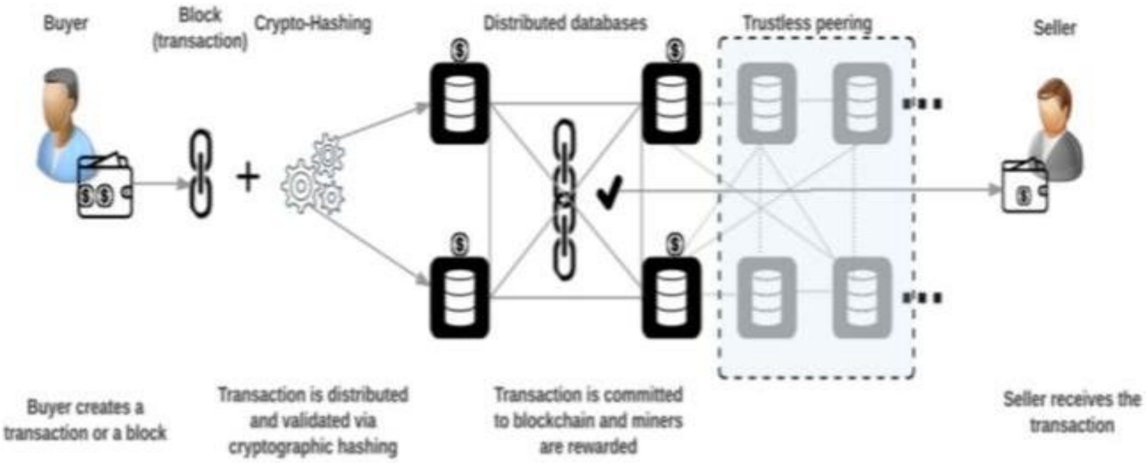
Buyer
Block (transaction)
Crypto-Hashing
Distributed databases
Trustless peering
Seller
Buyer creates a transaction or a block
Transaction is distributed and validated via cryptographic hashing
Transaction is committed to blockchain and miners are rewarded
Seller receives the transaction

Figure 2: Block diagram of Public Blockchain

Firstly, our analysis scrutinizes the challenges and issues related to existing cryptocurrencies, encompassing potential attacks, with a primary focus on matters of user privacy and transaction anonymity. Unlike previous research efforts that merely outlined these challenges and risks without addressing them, our study delves into blockchain security, assessing its vulnerabilities, and discussing potential countermeasures.

Bitcoin fundamental principles :

Authentication: Bitcoin employs a decentralized validation protocol, enabling users to connect to the Bitcoin network. BitID utilizes Bitcoin wallets and QR codes to provide service or platform access, ensuring secure interactions between users and the network.

Integrity: Bitcoin ensures transactional integrity through the use of digital signatures. These signatures verify the authenticity of transactions and prevent them from being altered after they have been confirmed. This feature guarantees the integrity of the transactional data and provides a secure way to conduct transactions on the network.

Non-Repudiation: Bitcoin transactions enforce non-repudiation, meaning that the sender of a message or transaction cannot deny their involvement. To send Bitcoins, the individual must possess the private key associated with the sending address. The sender signs the previous transaction hash and the recipient's public key, providing cryptographic proof of ownership and ensuring that the sender cannot deny their participation in the transaction. This mechanism adds a layer of security and accountability to Bitcoin transactions, preventing disputes and ensuring the authenticity of each transaction on the network.

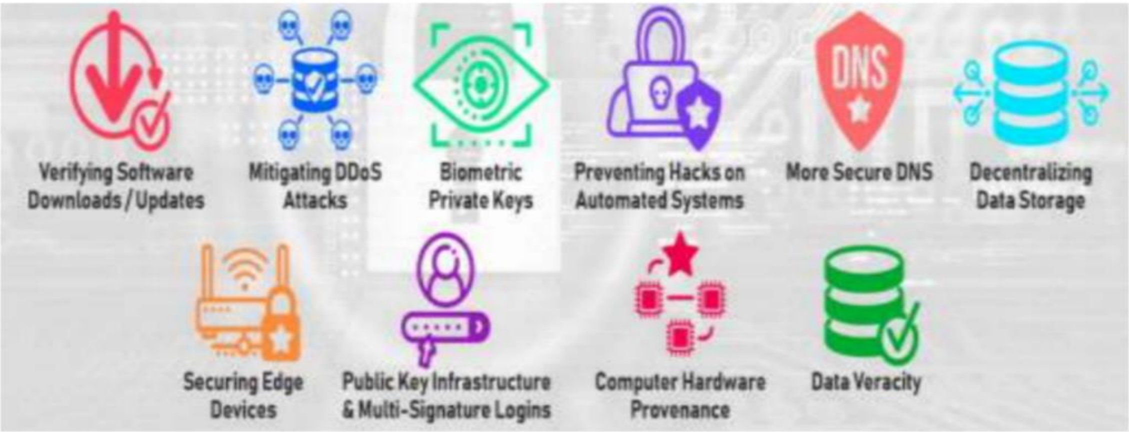
Verifying Software Downloads / Updates
Mitigating DDoS Attacks
Biometric Private Keys
Preventing Hacks on Automated Systems
More Secure DNS
DNS
Decentralizing Data Storage
Securing Edge Devices
Public Key Infrastructure & Multi-Signature Logins
Computer Hardware Provenance
Data Veracity

Figure 3:

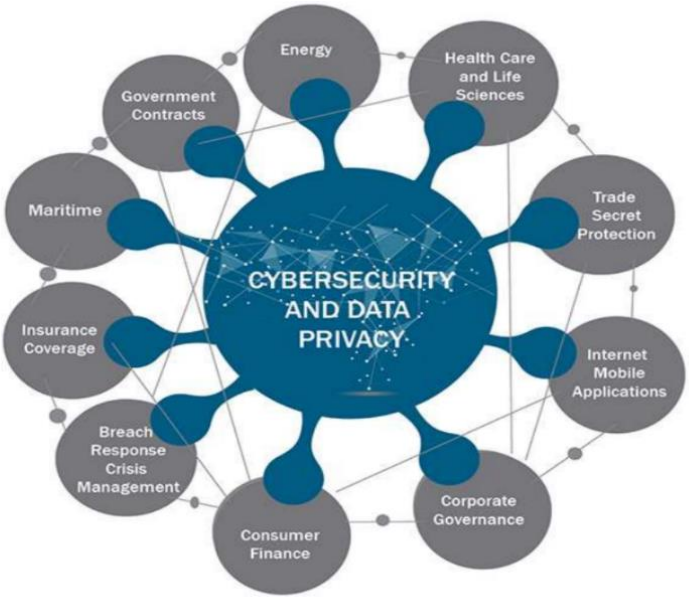
Energy
Health Care and Life Sciences
Government Contracts
Maritime
Trade Secret Protection
CYBERSECURITY AND DATA PRIVACY
Insurance Coverage
Internet Mobile Applications
Breach Response Crisis Management
Corporate Governance
Consumer Finance

Figure 4: Block diagram of Applications of Block Chain

Benefits of Bitcoin

1. Fast and Cost-Effective Transactions: Bitcoin transactions conducted through digital wallets are swift, and the associated transaction fees are minimal, making it an efficient means of exchanging value.

2. Decentralized Registry: Bitcoin operates on a decentralized network, meaning no central authority or government has complete control. This decentralized nature ensures that governments or banks cannot seize your Bitcoin, and there are no chargebacks, providing users with financial independence and security.

3. Secure Payment Information: Bitcoin transactions utilize a combination of public and private keys. When a Bitcoin is sent, the transaction is authenticated by both public and private keys, creating a cryptographic

certificate. This method ensures the security and authenticity of payment information, protecting users from unauthorized access or tampering.

4. Bitcoin Mining: Bitcoin mining offers the opportunity for individuals to create their own currency by setting up a Bitcoin Miner. This process involves validating and securing transactions on the Bitcoin network while earning newly minted Bitcoins as a reward for the mining efforts.

Network-Level Attacks in Blockchain Systems: Addressing Challenges

In the realm of network security, blockchain network safety concerns have become a prominent research area. However, there are lingering concerns about its scalability, security, availability, and sustainability. The rise of digital currency markets has led to an increase in cyber-attacks targeting marketing and business-oriented services. Among these attacks, Distributed Denial of Service (DDoS) attacks, which disrupt services by overwhelming network bandwidth, are particularly common. In blockchain-based platforms, DDoS attacks pose unique challenges, especially in decentralized and peer-to-peer technologies. Unlike traditional distributed application architecture, it is more difficult and costly to suppress the network using a large volume of small transactions in these platforms.

In cryptocurrency environments, currency exchanges play a crucial role, but they often face DDoS attacks. Several exchanges, including major ones like Mt. Gox, have experienced significant disruptions due to DDoS attacks. Research studies have documented numerous DDoS attacks on Bitcoin services, indicating vulnerabilities in various sectors such as exchanges, mining pools, gambling operators, wallets, and financial services. Reports suggest that mining pools, especially smaller ones, are highly susceptible to DDoS attacks.

Two contrasting methods have been observed: a legitimate approach and an unethical one. In the legitimate paradigm, alliance members invest in additional computing resources to enhance their chances of winning future races. Unethical actor alliances, however, focus on attacking mining pools through costly DDoS attacks to reduce the success rate of competing mining pools.

Challenges in Blockchain Systems: Strategies and Vulnerabilities

Block Producers Plan: In certain blockchain systems, the risk of Block Producers' (miners, validators) collusion is imminent. Based on Delegated Proof of Stake (DPoS) consensus, collusion among these producers can occur. According to experts, significant attacks may arise within these colluding Block Producers, including censorship attacks, changes in system parameters, and double-spending attacks.

Censorship Attack: Although the system is designed to encourage competition and consensus among Block Producers, there's no guarantee for developers and users that their applications and transactions won't be censored. In a censorship attack in DPoS, Block Producers may refuse to process legitimate transactions. If even a single Block Producer or a small group censors an entity, it may not pose a significant issue for the network, but it remains a potential threat.

Changing System Parameters: In DPoS, all changes must be approved through active stakeholder consensus. Colluding Block Producers can potentially modify protocol parameters unilaterally. If such an attack succeeds, the attackers may alter block rewards, allocate funds to specific stakeholders, and make other protocol-related changes. The threshold for changing these rules is equivalent to replacing 51% of the selected witnesses. The more stakeholder participation in selecting witnesses, the harder it becomes to modify the rules.

DPoS is structured in a way that makes these attacks improbable without explicit voter approval. In cases like EOS, protocol parameter changes involve time delays before implementation. Also, approval by 17 out of 21 Block Producers is required to alter the constitution, and this approval must be maintained for 30 consecutive days before changes can be implemented. If users don't accept the changes, they have the option to replace those Block Producers over time with ones that do not support the modifications. Ultimately, changing the rules depends on everyone in the network upgrading their software, and no blockchain-level protocol can enforce how networks are altered. This means that hard forking "bug fixes" can be avoided without requiring stakeholder approval, as long as they adhere to the expected behavior of the code. However, only security-critical hard forks should be implemented this way. Developers and witnesses must wait for stakeholder approval, even for minor changes.

Navigating Network-Level Challenges in Blockchain Systems: Insights and Strategies

Within the landscape of network security, blockchain systems have emerged as a critical focal point, raising various concerns such as scalability, security, availability, and sustainability. Particularly with the surge in digital currency markets, cyber-attacks, notably Distributed Denial of Service (DDoS) attacks, have become prevalent, disrupting essential services by inundating network bandwidth. Blockchain platforms, with their decentralized and peer-to-peer structures, present unique challenges in mitigating these DDoS attacks compared to traditional distributed applications.

In cryptocurrency ecosystems, exchanges stand as pivotal entities, often falling victim to disruptive DDoS attacks. Prominent exchanges like Mt. Gox have witnessed significant disruptions due to these assaults. Research studies have highlighted the vulnerability of Bitcoin services, indicating that sectors like exchanges, mining pools, gambling platforms, wallets, and financial services are susceptible. Smaller mining pools, in particular, face a high risk of DDoS attacks.

Two distinct strategies have been observed in these attacks: a legitimate approach and an unethical one. In the legitimate paradigm, alliance members invest in additional computational resources to enhance their competitive advantage. In contrast, unethical alliances focus on attacking mining pools through costly DDoS assaults, reducing the success rates of their competitors.

Challenges and Vulnerabilities in Blockchain Systems: Crafting Strategic Responses

Block Producers' Collaborative Strategies: Certain blockchain systems face the looming threat of collusion among Block Producers (miners, validators). Within the context of Delegated Proof of Stake (DPoS) consensus, these producers can conspire. Noteworthy attacks stemming from such collusion include censorship attacks, alterations in system parameters, and double-spending attacks.

Censorship Attacks: Despite the system's design promoting competition and consensus among Block Producers, developers and users lack assurance that their applications and transactions won't face censorship. In DPoS, a censorship attack could involve Block Producers refusing to process legitimate transactions. While an isolated instance of censorship may not pose a significant threat, ongoing or widespread censorship by even a single Block Producer could compromise the integrity of the network.

Modifying System Parameters: In DPoS, any alterations must secure active stakeholder consensus. Colluding Block Producers possess the potential to unilaterally modify protocol parameters. A successful attack could lead to changes in block rewards, allocation of funds to specific stakeholders, and other protocol adjustments. The threshold for such modifications is akin to replacing 51% of the chosen witnesses. Increased stakeholder participation in witness selection heightens the difficulty of modifying these rules, creating a robust safeguard.

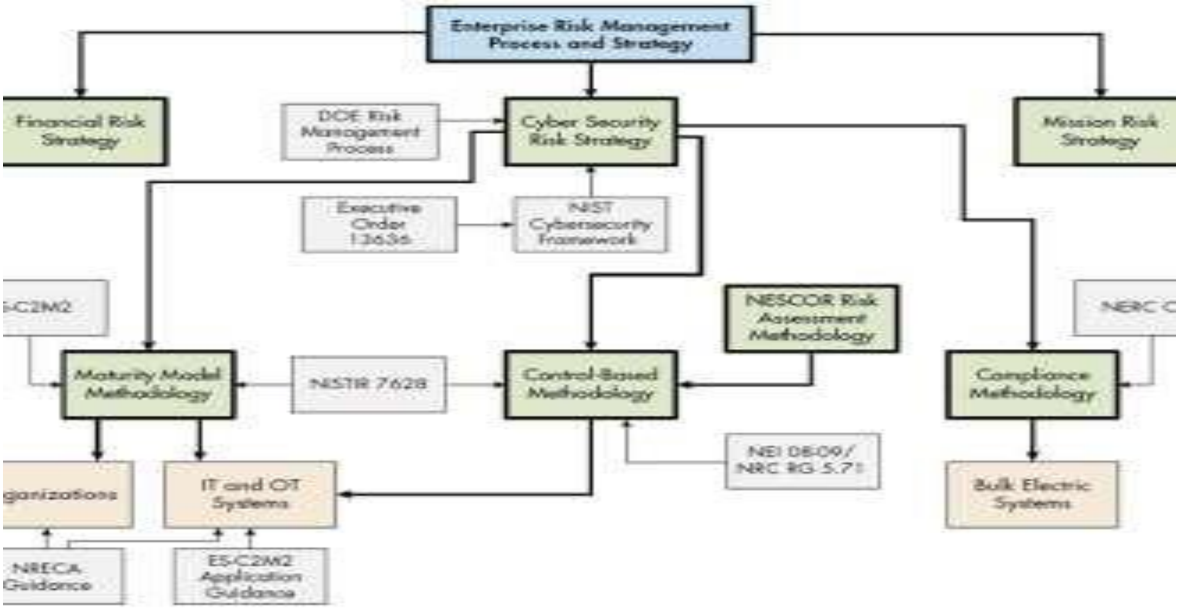
Enterprise Risk Management Process and Strategy
Financial Risk Strategy
DOE Risk Management Process
Cyber Security Risk Strategy
Mission Risk Strategy
Executive Order 13636
NIST Cybersecurity Framework
ES-C2M2
NESCOR Risk Assessment Methodology
NERC C
Maturity Model Methodology
NISTIR 7628
Control-Based Methodology
Compliance Methodology
NEI 08-09/ NRC RG 5.71
ganizations
IT and OT Systems
Bulk Electric Systems
NRECA Guidance
ES-C2M2 Application Guidance

Figure 5: Cyber security monitoring process

DPoS structures inherently deter these attacks without explicit voter approval. In cases like EOS, protocol parameter changes involve time delays before implementation. Additionally, alterations to the constitution require approval by 17 out of 21 Block Producers, sustained for 30 consecutive days. Users opposed to changes can gradually replace supportive Block Producers, ensuring alignment with their preferences. Ultimately, any modifications hinge on network-wide software upgrades. While blockchain-level protocols can't enforce network alterations, stringent approval mechanisms safeguard against unauthorized changes. Critical hard forks should strictly adhere to security concerns, ensuring a delicate balance between progress and stability.

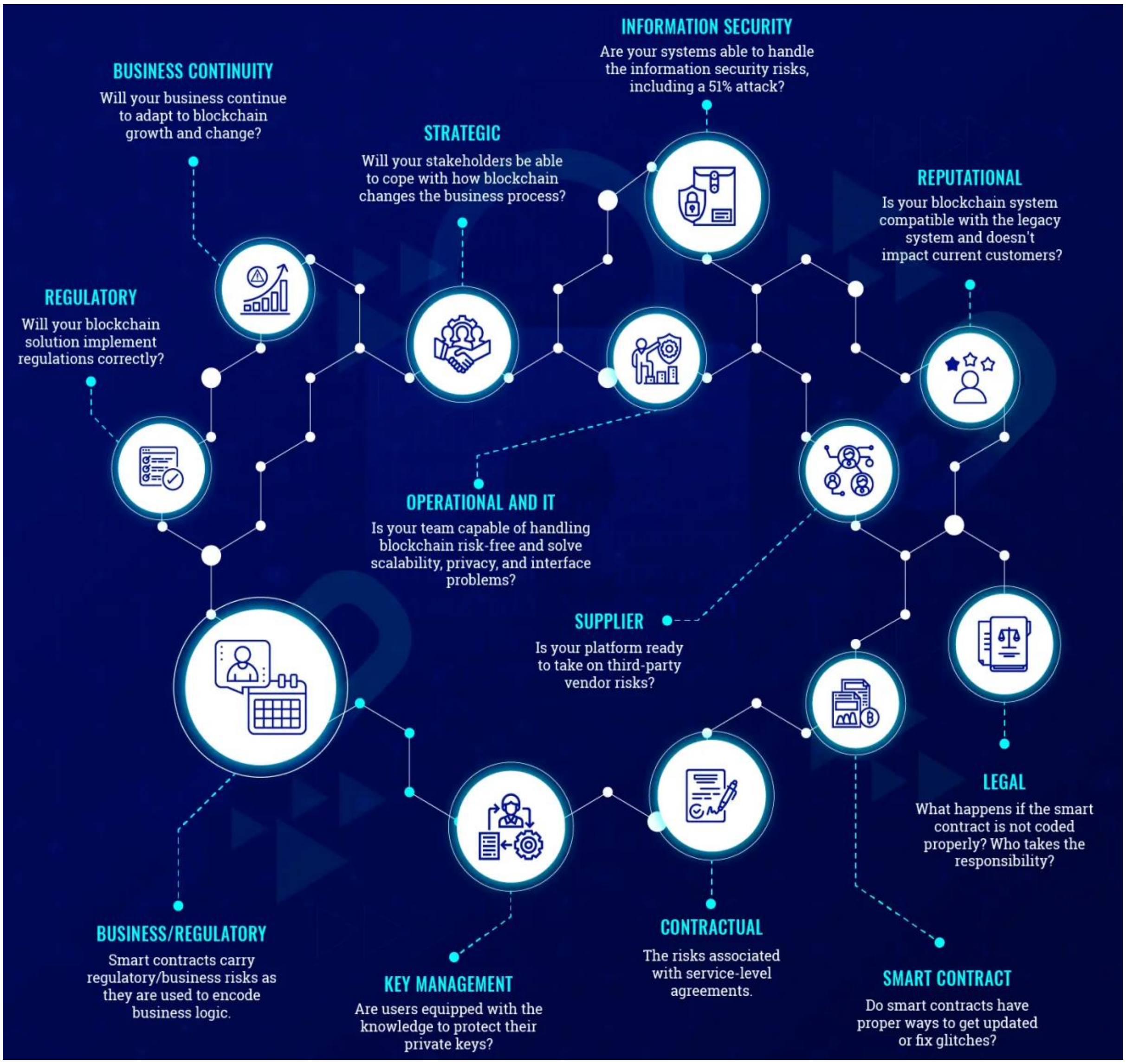
INFORMATION SECURITY
Are your systems able to handle the information security risks, including a 51% attack?
BUSINESS CONTINUITY
Will your business continue to adapt to blockchain growth and change?
STRATEGIC
Will your stakeholders be able to cope with how blockchain changes the business process?
REPUTATIONAL
Is your blockchain system compatible with the legacy system and doesn't impact current customers?
REGULATORY
Will your blockchain solution implement regulations correctly?
OPERATIONAL AND IT
Is your team capable of handling blockchain risk-free and solve scalability, privacy, and interface problems?
SUPPLIER
Is your platform ready to take on third-party vendor risks?
LEGAL
What happens if the smart contract is not coded properly? Who takes the responsibility?
BUSINESS/REGULATORY
Smart contracts carry regulatory/business risks as they are used to encode business logic.
KEY MANAGEMENT
Are users equipped with the knowledge to protect their private keys?
CONTRACTUAL
The risks associated with service-level agreements.
SMART CONTRACT
Do smart contracts have proper ways to get updated or fix glitches?

Figure 6: Block Diagram of Risk Analysis

Scalability Challenges and Governmental Interference: A Glimpse into Potential Threats

Attacks at Scale:

A potential avenue of attack involves assumptions regarding the structure of an industrial-scale Delegated Proof of Stake (DPoS) blockchain. Larimer's vision for EOS suggests a scaling scenario where substantial data centers serve as Block Producers (BPs) to meet the network's bandwidth and speed requirements. Although this scenario hasn't been realized yet, its implications are significant. If BPs are compelled to operate within dedicated data centers, it restricts the pool of potential BPs and severely limits entities that can step in to replace ousted BPs. In case there aren't enough BPs with adequate resources to replace those removed, the network could suffer. Voters would then need to decide on penalizing underperforming BPs, potentially diminishing the overall resources of the network.

Governmental Interference:

Governmental interference presents a similar challenge, resembling a Ponzi scheme within the consensus model. In this scenario, users participate in a contract promising increased returns and a chance to win a jackpot. The contract stores users' addresses in a dynamically sized array, intended to iterate over the addresses to pay out when a jackpot is hit. However, it fails to limit the array size. Over time, the government attracts enough users, exceeding the gas allocation's coverage of the entire array. Consequently, the contract perpetually fails to reset the game and award the jackpot, effectively freezing the contract's state.

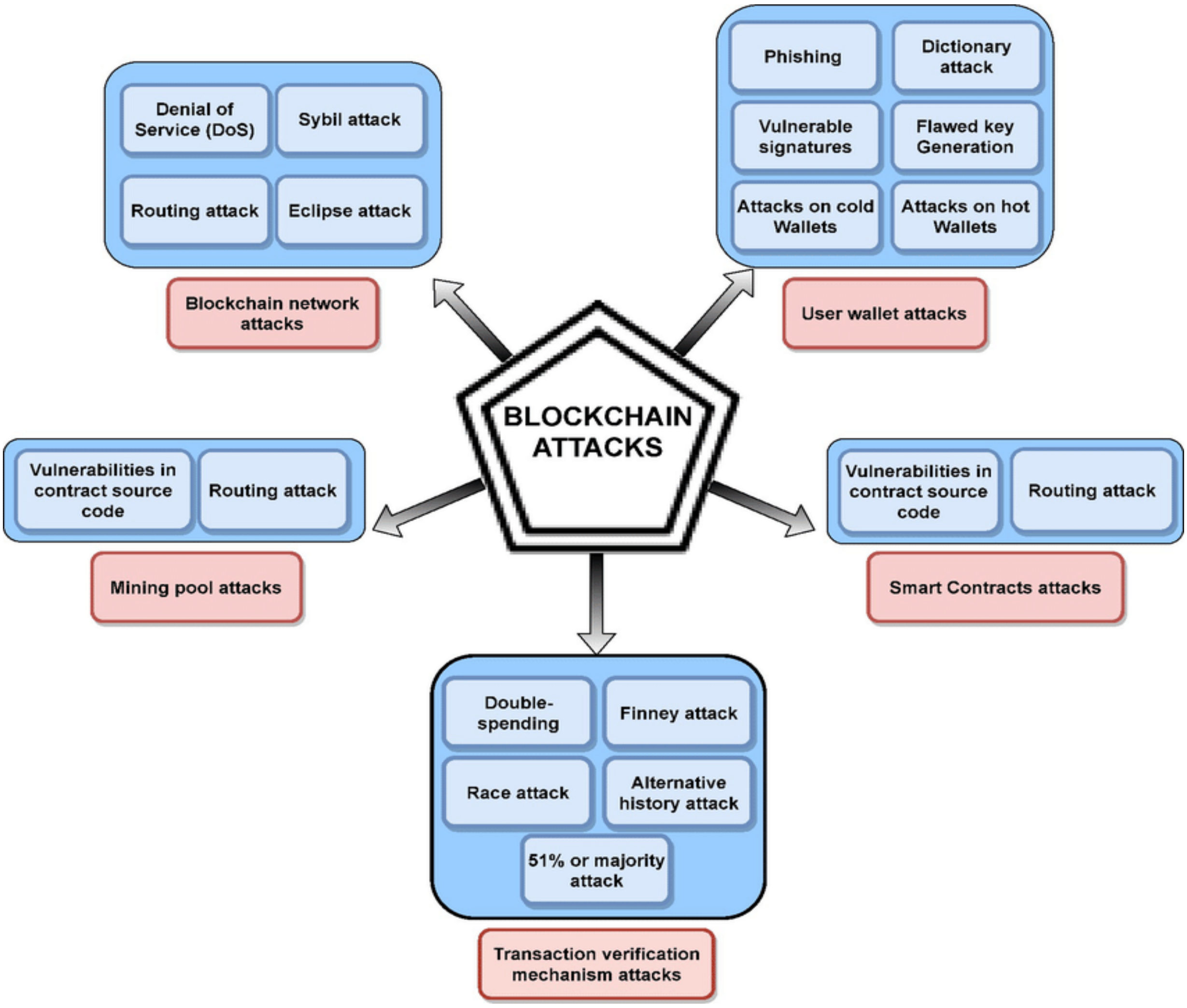

Figure 7:

Enhancing Wallet Security: Safeguarding Private Keys in Cryptocurrency

In the realm of cryptocurrencies, the core of one's holdings lies within a digital safe haven known as a wallet. In this space, each user possesses a unique set of private and public keys to access their funds. However, the vulnerability of wallets, akin to physical assets, is a significant concern. Wallets can be lost, forgotten, or fall into the wrong hands, rendering users unable to access their funds. Ransom attacks compound this issue further, utilizing tactics like phishing, system hacking, installation of flawed software, and mishandling of wallets.

One potential breach point is the private key, the cornerstone of wallet security. Theoretically, a crypto attacker should not be able to decipher the original plaintext, given that it's encrypted. However, the structure of blockchain systems, with consistent patterns in blocks, provides attackers an opportunity. Patterns, albeit obscured, often emerge within each encrypted block, allowing attackers to attempt partial reconstruction of the plaintext. This threat highlights the need for robust encryption methods to safeguard private keys.

In the cryptocurrency landscape, Bitcoin commands the largest market share, with public keys generated securely from private keys using the Elliptic Curve Digital Signature Algorithm (ECDSA). However, experts like

Vedral and Morikoshi raise concerns about ECDSA's vulnerability to quantum computers. Quantum computers possess capabilities that traditional computers lack, exploiting quantum phenomena for computations impossible in classical computing. Notably, a quantum computer can execute Shor's algorithm, rapidly factorizing large numbers, potentially compromising public key encryption. Despite this, Bitcoin protocol's use of the SHA-256 function for public keys, coupled with the RIPEMD-160 hash function and error correction checksum, remains robust. While SHA-256 has theoretical vulnerabilities, no actual breaches have occurred, ensuring its enduring reliability.

III. RESULTS

Results Analysis: Evaluating AES and Other Encryption Algorithms

The study conducted a comprehensive analysis of encryption algorithms, including AES, DES, TDES, RC2, and Rijndael, focusing on the time required for encryption and decryption processes across various content file sizes (25 kb, 45 kb, 70 kb, 2 mb, 4 mb, 7 mb). The primary objective of the statistical analysis was to identify the most suitable algorithm for encoding and decoding content files efficiently based on their sizes. The evaluation considered crucial factors such as resistance against known attacks, speed, code efficiency on diverse platforms, design simplicity, and compatibility with other symmetric encryption methods. Specifically, the study aimed to compare AES with other algorithms and determine the optimal encryption approach for files of different sizes. The analysis involved measuring the time taken by each algorithm to encrypt and decrypt content files, facilitating a detailed comparison between AES, DES, TDES, RC2, and Rijndael. The study aimed to identify the algorithm that strikes a balance between robust security, high speed, and efficient resource utilization, ensuring compatibility across various platforms. Particular attention was paid to the implementation aspects of the Rijndael algorithm, emphasizing its adaptability to a wide range of processors and dedicated hardware. Despite its potential advantages, the research findings highlighted certain challenges and considerations for future implementations. These considerations included the need for encryption methods to withstand known attacks, maintain speed and code compactness across diverse platforms, and exhibit design simplicity. Additionally, ensuring compatibility and differences with other symmetric encryption techniques remained crucial factors in the analysis. In summary, the study's comprehensive evaluation provides valuable insights into the strengths and limitations of various encryption algorithms, emphasizing the importance of balancing security, speed, and implementation efficiency. These findings pave the way for informed decisions in selecting the most appropriate encryption algorithm based on specific use cases and requirements.

IV. CONCLUSION

Blockchain technology, particularly in its most prevalent form, Proof of Work (PoW), has been the backbone of innovations like Bitcoin. The marriage of PoW with secure timestamping services provides a robust security solution. However, even with these advancements, PoW-based systems are susceptible to security risks, including the notorious double-spending attacks. To enhance security and privacy, several blockchain platforms have explored different avenues. Bitcoin, for instance, has adopted technologies like Segwit and Lightning Network, providing increased security and anonymity. ZeroCoin, an extension of Bitcoin, ensures untraceable transactions through the use of zero-knowledge proofs. Ethereum, on the other hand, introduced Proof of Stake (PoS), offering a faster and more efficient alternative to PoW. PoS allows anyone to become a validator, scaling proportionally to the number of blocks a validator can confirm. However, PoS has its challenges, such as the "nothing-at-stake" problem. In response to these issues, BitShares developed a consensus model known as Delegated Proof of Stake (DPoS), which combines blockchain technology with a democratic process. DPoS mitigates centralization by using a voting mechanism to protect the blockchain from malicious use. Despite its advancements, DPoS is not without its vulnerabilities, particularly in terms of centralization control. While blockchain technology has transformed transaction-based industries, it faces persistent security concerns. Although some studies and practical implementations have provided solutions to these risks, robust security measures ensuring the correct functioning of blockchain technology remain challenges and open research problems. Despite these challenges, the rapid growth and development of blockchain technology suggest a future where it becomes a common technology in various business and industrial sectors. Addressing these security concerns effectively will be crucial in realizing the full potential of blockchain technology in diverse applications worldwide.

V. REFERENCES

[1] Stock B., Göbel J., Engelberth M., Freiling F. C., and Holz T. Walowdac-analysis of a peer- to-peer botnet. In Computer Network Defense (EC2ND), 2009 European conference on IEEE; 2009:13–20.

[2] Vedral V, Morikoshi F. Schrödinger's cat meets Einstein's twins: a superposition of different clock times. Int J Theor Phys. 2008;47(8):2126-2129.

[3] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: Big data (BigData congress), 2017 IEEE international congress on. IEEE; 2017:557-564.

[4] ing S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper; 2012.

[5] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, retrieved on 28/04/2018 Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on Blockchain technology?—a systematic review. PLoS ONE. 2016;11(10):e0163477. https://doi.org/10.1371/journal.pone.0163477

[6] Petar T., Andrei D., Drachsler C., Arthur G., Florian B. Securify: Practical Security Analysis of Smart Contracts. arXiv:1806.01143v1 [cs.CR]. 2018

[7] The Finney Attack, Available from https://bitcoincoreacademy.com/the-finney-attack, retrieved on 28/04/2018.

[8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Commun. Surveys & Tut., vol. 18, no. 3, pp. 2084–2123, Mar. 2016.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [8] Decker, Christian, Jochen Seidel, and Roger Wattenhofer., "Bitcoin Meets Strong Consistency".

[10] Cachin C. Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers 2016, 310(1), pp. 4.

[11] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services, 2018, 14.4, pp.352-375.

[12] Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017, 8(1), 297-315.

[13] Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." Computer Science-Research and Development, 2018, 33.1, pp. 207-214.

[14] Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network. 2017; 44:13-6.

[15] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019, 12(5), pp. 1-14.

[16] Sharma PK, Moon SY, Park JH. Block-VN: A distributed blockchain based vehicular network architecture in smart City. JIPS. 2017, 13(1), pp. 184-95.

[17] "How Blockchain Can Fight Fraud Based on Know-Your-Customer Data", Nasdaq.com, 2019. [Online]. Available: https://www.nasdaq.com/articles/how-blockchain-can-fight-fraud-base d-know-your-customer-data-2019-02-11. [Accessed: 19- Sep- 2019].

[18] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017, 50(7), pp. 80-4.

[19] Trautman LJ, Ormerod PC. Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. Am. UL Rev. 2016, 66(1), pp. 1231.

[20] Konstantinos Christidis, and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, vol 4.

[21] T. FitzPatrick (2012), Key Success Factors of eLearning in Education: A Professional Development Model to Evaluate and Support eLearning, US-China Education Review, 2012, A 9, 789-795.