International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Blockchain security- security challenges and solutions for decentralized systems and cryptocurrencies

Gaurav Malik [1,*] and Prashasti [2]

[1] *The Goldman Sachs Group, Inc. Dallas, Texas, USA.*
[2] *Application security engineer, The New York Times, Dallas, United States.*

International Journal of Science and Research Archive, 2023, 09(02), 1074-1100

Publication history: Received on 19 May 2023; revised on 08 August 2023; accepted on 11 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0515

Abstract

Blockchain technology is a chain of blocks formed using cryptography on multiple computers. It keeps a list of distributed transactions and ensures it is transparent, immutable, and hard to manipulate. Blockchain's inherent security features would strengthen its build, including cryptographic hashing, consensus algorithms, and immutability. However, it is also highly exposed and vulnerable to several threats. In decentralized systems and cryptocurrencies, blockchain security is a crucial point of security to protect from attacks on systems, data breaches, and financial loss. Challenges in the Security of Blockchain Networks. This paper explores 51% of attacks in blockchain networks, vulnerabilities in smart contracts, and privacy issues faced by blockchain networks. Since blockchain is decentralized, these challenges are among the reasons its nature is inherently more secure than any traditional centralized system, as they cannot allow a single point of failure. A key element for secure blockchain transactions is security mechanisms like cryptography, proof of work, proof of stake, and multi-signature solutions. However, this is somewhat stifled by the fact that blockchain applications have expanded far beyond cryptos, such as healthcare, supply chains, and systems, such as voting, and the requirement for robust security grows. To address these issues, blockchain security must continuously adopt innovation in blockchain security practice, such as developing decentralized security solutions and post-quantum cryptography, up to a comprehensive security framework. Security in the blockchain is the key to securing digital assets, privacy protection, and trust on the decentralized networks mentioned in this paper. To solve the new and evolving threats that will become a menace to blockchain security in the future, we will combine the new technologies of artificial intelligence, quantum-resistant cryptography, and decentralized identity management.

Keywords: Blockchain Security; Cryptography; Decentralized Systems; Smart Contracts; 51% Attack; Interoperability

1 Introduction

Block Chain Technology is a decentralized, distributed ledger system that records transactions securely in several computers to make the data immutable and transparent. In a blockchain, blocks are formed on information and connected in a chain by cryptographic hashes. This structure eliminates the need for the presence of the central authority so that the peer-to-peer transaction can happen without any intermediaries. The blockchain was appreciated thanks to its strong connection to cryptocurrencies like Bitcoin. However, its uses have grown in multiple industries, like healthcare, finance, and supply chain management. Due to its decentralized nature, blockchain due to its decentralized nature, blockchain is resistant to censorship and manipulation and manipulation, which is much better than traditional centralized systems. Nevertheless, blockchain security is paramount since catastrophic outcomes may occur if vulnerabilities in the implementation, design, or use of blockchain are present, leading to data breaches or financial losses.

* Corresponding author: Gaurav Malik

Blockchain security describes practices, technologies, and methodologies used to safeguard blockchain systems and the data they store from different types of security threats. Blockchain, by design, offers some inherent security features, such as cryptographic hashing, consensus algorithms, and immutability. Nonetheless, the technology is not invulnerable to attack or vulnerability. Cryptography is one of the main features of blockchain security. Through public and private keys, transactions are authorized, data integrity is maintained, and the network is secure. The public keys are used to encrypt transactions, and the private keys are required to decrypt them. Furthermore, elements like Proof of Work (PoW) and Proof of Stake (PoS) are used to give consensus to the network, ensuring that only valid transactions are validated in the blockchain. Although these mechanisms are robust for security, the blockchain system is not immune to attack. External threats like cyberattacks are only a few types of security challenges that security officers can experience, as are internal vulnerabilities such as coding errors or poor network management. However, these risks have to be understood and mitigated in order to continue assuring the safety and trust in blockchain technology.

Especially in decentralized systems and cryptocurrencies, blockchain security is the most important aspect. To exist in decentralized networks, control lies in the individual nodes; there is no such thing as a single point of failure. In this way, blockchain technology proves to be more resistant to attacks than the traditionalized built systems. Decentralization also brings new problems to the security of all involved nodes and the avoidance of having a malicious actor take over the network. Security for cryptocurrencies in terms of digital assets is a necessity to ensure that value is not lost. Blockchain is used to secure transactions for cryptocurrencies such as Bitcoin and Ethereum. In case of blockchain security failure, the attack would be financial loss or theft of funds by attackers. For example, a successful 51% attack would allow a malicious entity to persecute most of the network's compressor power, consequently changing transaction records or double-spending coins. This attack damages the currency's trustworthiness, considerably disrupting the cryptocurrency market. In addition, the more blockchain technology goes beyond digital currencies into supply chain tracking, healthcare data management, and voting systems, the more important security is. If there is any vulnerability, a breach of sensitive data, financial fraud, or operational disruptions, it is in everyone's interest.

The weaknesses and assault ability of the systems security challenge scope span adjacent to all systems vulnerabilities, assaults, and misuse. Scalability is one of the primary challenges faced by blockchain systems. As blockchain networks expand, they need more computational power and storage to operate, thus creating more targets for denial of service or network congestion attacks. Such distribution can influence the performance and security of the blockchain. The second important challenge is developing secure smart contracts. Self-executing and cutting contracts with the terms of the agreement are coded into the core tract and are called smart contracts. However, like many things, they have their drawbacks that amplify risk and, through poor coding or insecurity, can be exploited, resulting in loss of finances. In 2016, when a hack on the Ethereum blockchain attacked the DAO (Decentralized Autonomous Organization) as part of a much larger cryptocurrency vendetta, vulnerabilities in smart contract code can unknowingly and detrimentally be exploited.

Privacy is also an issue regarding blockchain security. While blockchain transactions are transparent, there are certain cases when privacy becomes incompatible with transparency. This is a constant struggle for acceptable transparency and privacy, particularly in confidential information cases. Blockchain security is all important. With blockchain technology advancing and finding its way to critical sectors, these challenges must be addressed to achieve such development. Because blockchain systems can be trusted neither by the users nor the organizations who own them, it is necessary to develop effective solutions to protect their integrity, confidentiality, and availability.

2 Understanding Blockchain and Decentralized Systems

Blockchain technology has penetrated the banking sector and generated buzz within the conference room due to its unique security, transparency, and efficiency properties. The basic mechanism of Blockchain as a DLT is a means of storing secure, clear, and immutable data on a network of computers called nodes. To understand the breadth of security related to this technology (and beyond), one must understand how the hell blockchain works, what it is, how Blockchain works, and the roles decentralized consensus and decentralized systems play.

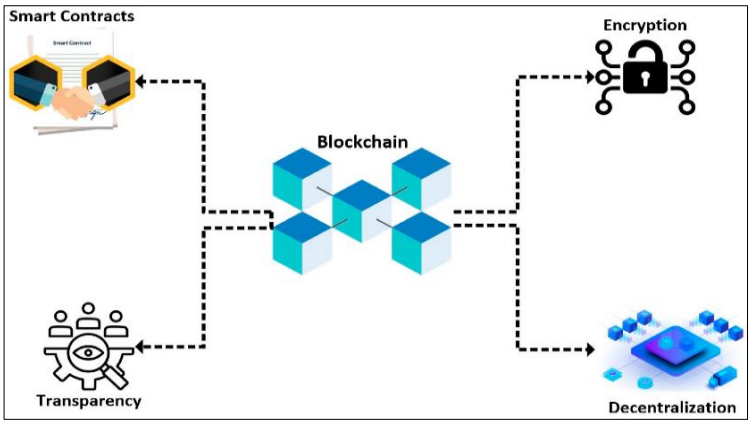

Figure 1 The four main features of blockchain technology.

2.1 How Blockchain Works

Inside Blockchain is a chain of blocks and a list of transactions. Whenever a transaction occurs, it sends it to a network of nodes. These nodes are assigned to verify the transaction's authenticity and add it to the Blockchain. Once a set of transactions is verified and put into one group (known as a block), a new block is created. This makes each block a reference to the previous one, forming a secure and immutable data chain.

Cryptography is the only mechanism to ensure these transactions are accurate and secure. Each block has a unique cryptographic hash, a digital fingerprint that refers to the previous block. A part of this system ensures it is nearly impossible to change data after it is recorded, which is something Blockchain has become known for. In addition, the Blockchain relies on consensus algorithms, that is, Proof of Work (PoW) or Proof of Stake (PoS), to prove that the transactions inserted in the Blockchain are legitimate (Lepore et al., 2021). As opposed to the central authority overseeing the transactions in a blockchain network, the users on that network do this. The network relies on a decentralized set of nodes, each storing a copy of the Blockchain. This decentralized approach eliminates the requirements for intermediaries, reduces the risk of fraud, and provides greater security.

2.2 Structure of Blockchain Networks

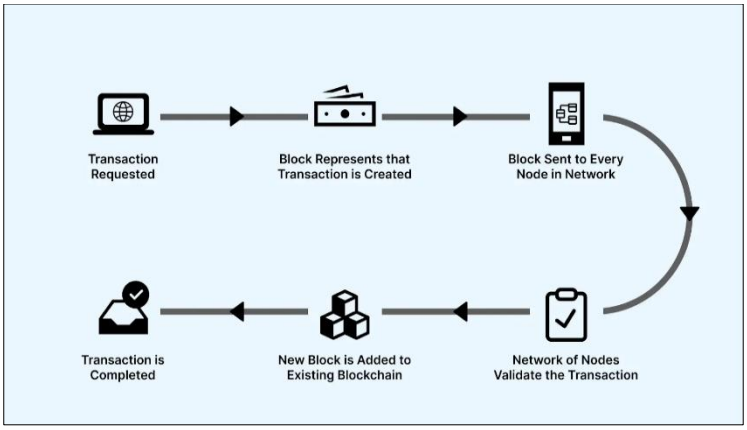

Figure 2 Blockchain Technology

The key components of a network are many interconnected nodes, and most such networks are blockchain networks. However, these nodes can be classified into two kinds: full nodes and lightweight nodes. Full nodes have a fully downloaded and in-memory copy of the entire Blockchain, so they know they can verify and validate all transactions over the network. However, lightweight nodes store a subset of the Blockchain and keep track of the most recent transactions (Liu et al., 2019). It is based on the consensus mechanism used by the blockchain network as it dictates the structure of the blockchain network. In Proof of Work, nodes need to compete by solving difficult math problems to add a new block to the chain, while in Proof of Stake, nodes are crowdsourced to blockchain nodes by the amount of crypto they hold. These nodes communicate among themselves peer to peer and send information so that the Blockchain is updated in real-time. All transactions are validated before they are added to the ledger.

The architecture of a blockchain network influences its scalability and efficiency. While public blockchains like Bitcoin have an open and permissionless setup, whereby anyone can join the network and take part in the consensus process, other blockchains have a closed and permissioned setup. Private blockchains are more controlled and used mostly by enterprises or organizations for confidential data.

2.3 The Role of Decentralized Consensus

Consensus on blockchain technology is vital and is a cornerstone of the technology. A distributed network of nodes is designed to enable a distributed network of nodes to agree on the veracity of transactions without the need for a central authority or intermediary. Consensus mechanisms such as Proof of Work, Proof of Stake, and Delegated Proof of Stake are specially designed to reach consensus among participants on the state of the Blockchain (Yang et al., 2019).

An example of a Proof of Work system is when miners solve a complicated mathematical puzzle to verify transactions and add a new block to the chain. However, because this process takes tens of thousands of steps, it takes much computational power and energy, making it prohibitively expensive and time-consuming to manipulate the Blockchain. However, Proof of Stake allows validators to determine the transactions to handle based on how many tokens they currently own, which is collectively more energy efficient and less resource intensive.

Instead, decentralized consensus implies that no single party controls the network. In this case, all of the network participants follow a protocol that validates the transactions and ensures the integrity of the Blockchain (Kairaldeen et al., 2021). The advantage of this decentralization is that it is more secure, transparent, and more resistant to censorship than centralization: no party can change the Blockchain or reverse transactions once they are confirmed.

2.4 Types of Decentralized Systems (Public vs Private Blockchains)

Public and private blockchains can be classified into two types. Each type has advantages and challenges based on the intended use case. A public blockchain is an open, permissionless network hosted by anyone participating in the consensus and validating the transactions. Bitcoin and Ethereum are amongst the examples of public blockchains. They are highly decentralized public blockchains with a very high level of transparency, as all transactions are visible to anyone on the network. Although public blockchains are open to attack, as can be seen in 51% of attacks where someone has control of most of the network's computing power, they can manipulate the Blockchain.

Private blockchains are permissioned networks in which only a specific group of participants can access and participate. Usually used by businesses or organizations to manage their internal processes, such as supply chain tracking or financial transactions, these blockchains. In the case of private blockchains, participants are not anonymous and cannot access the network before the process of being vetted is completed (Christidis & Devetsikiotis, 2016). Though this is a centralized nature, it can lose the security and transparency advantage in a public blockchain. A combination of public and private blockchains has also resulted in hybrid blockchains. The main property of these blockchains is that they enable a business to run private, internal processes but be protected by public blockchain transparency and security in terms of external transactions.

To understand blockchain technology, it is important to understand how it works, the structure of blockchain technology, and the role of decentralized consensus in this technology, and also to know the difference between public and private blockchains. Blockchain is quite a transformative tool in many industries that rely on a unified distributed system, which generally encompasses several mechanisms for data integrity, privacy, and security (Paik et al., 2019). With Blockchain evolving, these concepts should still be explored as they can improve its security and practicality.

3 Blockchain Security Challenges

Although decentralized and secure, blockchain technology presents major security threats that could disturb its integrity and performance. These challenges include network manipulation, smart contract vulnerabilities, and regulatory concerns that threaten both users and developers. The following are some of the most serious security issues that hit blockchain systems.

Table 1 Overview of Blockchain Security Challenges

Challenge Category	Description	Key Threats	Security Impact
51% Attack and Network Manipulation	Attackers control over 50% of the network's mining power.	Transaction manipulation, Double-spending	High
Smart Contract Vulnerabilities	Flaws in the self-executing contracts can be exploited.	Reentrancy attacks, integer overflow	High
Double Spending Problem	User spending the same cryptocurrency more than once.	Lack of confirmations, 51% attack	High
Security Flaws in Consensus Mechanisms	Flaws in PoW, PoS, or DPoS consensus algorithms.	51% attacks, nothing-at-stake attacks	Moderate
Privacy and Data Leakage	Public transaction data leading to potential privacy breaches.	Identity tracking, personal data exposure	High

3.1 51% Attack and Network Manipulation

The 51% attack is considered one of the most popular threats to the security of the blockchain. A single entity or a group of them takes control of more than 50% of mining power or stake evaporates in a proof of stakes (PoS) system. In such a case, the attacker can reverse transactions, prevent new transactions from being confirmed, or double-spend tokens (Moroz et al., 2020). This is a vulnerability for certain blockchain networks, especially those weak in mining power and the less active participants. Bitcoin's network is generally still considered resistant to this attack, but the high mining power means smaller blockchains or less decentralized networks are much more susceptible.

3.2 Smart Contract Vulnerabilities

Self-executing contracts where the terms of a contract are written into code are called smart contracts. However, these contracts are running based on some blockchain platforms like Ethereum, and while they can carry out security, they are not impervious to vulnerability. Such security flaws may occur with poorly written or untested smart contracts. The 2016 fatal DAO hack was also a vulnerability and an exploit of a smart contract, causing a loss of millions of dollars in Ether (Santos & Kostakis, 2018). The most common vulnerabilities in a smart contract include reentrancy attacks, integer overflow and integer underflow errors, and logic errors, which can be exploited to manipulate how the contract executes. Contract developers must audit 100 percent and test their contracts 90 plus percent before deployment to ensure they are as robust as possible against potential exploits.

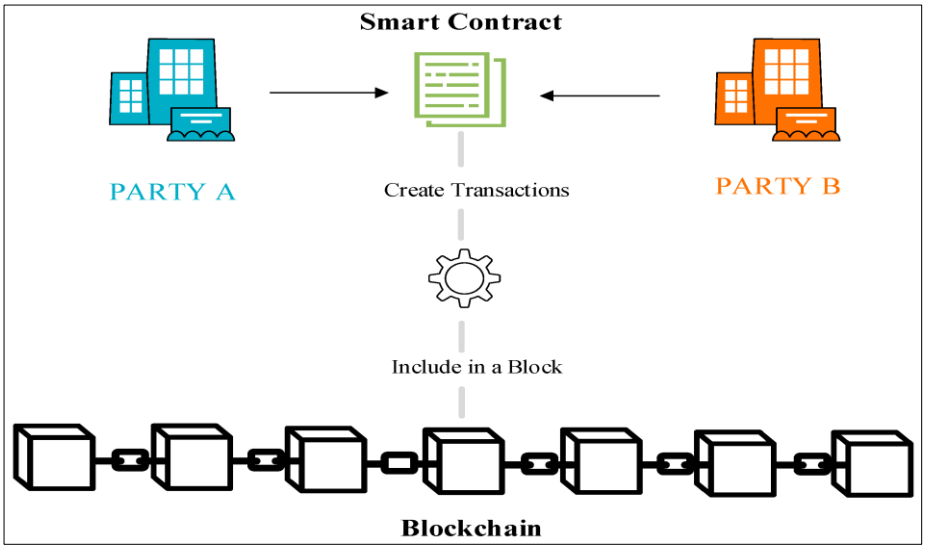

Figure 3 Smart contract execution process

3.3 Double Spending Problem

The act of double spending cryptocurrency is when a given user spends the same cryptocurrency more than once. Although a technology rape within the blockchain, and hence prevent this through the consensus mechanism, there are opportunities for weaknesses, especially with low confirmation transactions or the 51% attack. Double spending is also a major issue in cryptocurrencies because it is a major part of breaking the trust and integrity of the whole system. For example, Bitcoin and the like mitigate the risk by requiring multiple confirmations before a transaction is considered final. In such cases, double spending is still a threat if confirmation times are delayed or the network is attacked.

3.4 Security Flaws in Consensus Mechanisms

The consensus mechanisms of blockchain consensus are vital in the overall functionality of the blockchain network, and that is where the authority of different nodes to validate the transaction lies. Nevertheless, such mechanisms may be insecure. For example, Proof of Work (PoW) is susceptible to 51% attacks, which has been discussed before, and is computationally costly, energy-intensive, and prone to centralization (Saad et al., 2019). However, Proof of Stake (PoS) systems like the ones researchers have seen implemented in the Binance Smart Chain are altogether more energy efficient. However, they are prone to "nothing at stake" attacks as validators simultaneously do not have any real cost associated with voting in many chains. Hybrid models like Delegated Proof of Stake (DPoS) bring the risk of centralization due to such a small number of delegates that may not have been taken to be incorruptible. However, there are trade-offs to each consensus model, and how the blockchain will need to be most secure depends on the specific needs and structure of the blockchain.

3.5 Privacy and Data Leakage

One of the most critical issues related to privacy with blockchain systems is that all the transaction data is on the ledger plain and visible to anyone by design. When it comes to blockchain, its transparency is often a plus point extolled. However, it can result in data leakage, particularly if sensitive personal information is stored on the chain. Moreover, blocks like Monero and Zcash used cryptographic technologies like zero-knowledge proofs to cloak users' privacy. Nevertheless, the larger ecosystem still has some hurdles. In practice, if an address belongs to users, and their identities or transaction histories are linked to them, their activities can be tracked. This is a crucial issue in such regulatory environments as fronted by the GDPR in the European Union, where the laws of how to protect data conflict with the blockchain's inherent transparency.

3.6 Regulatory Compliance and Legal Risks

Blockchain technology is decentralized, which comes with difficulties for regulatory authorities. However, governments and regulators have had trouble designing adequate regulatory frameworks to ensure blockchain systems comply with existing laws and regulations. The adoption of blockchain faces several issues concerning anti-money laundering (AML), Know your customer (KYC), and taxation that render it difficult to turn into reality in finance-related industries such as finance and healthcare. For example, cryptocurrency exchanges must comply with the AML and KYC laws, which prevent money laundering; however, blockchain transactions remain pseudonymous, making it hard to ensure their implementation. Additionally, the lack of legal guidelines that companies must adhere to when using the blockchain to create applications would result in companies likely to find themselves involved in legal disputes or incurring penalties from state regulation. As blockchain technology grows, regulators need to adapt by otherwise ensuring that corresponding legal frameworks are working hand in hand with the decentralized ethos that is the core of blockchain technology and also tackle mafia information technologies.

Understanding these security challenges is also a key aspect of understanding the limitations and risks of blockchain systems. Despite its bountiful possibility, blockchain offers a safe medium of development for Decentralized Apps, yet it is imperative that these vulnerabilities be conversant with strong technical solutions and continued development to guarantee the thrill and soundness of blockchain networks.

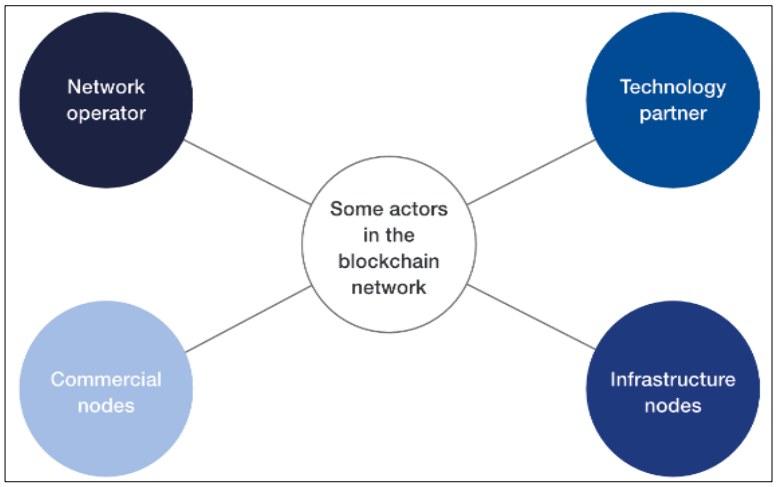

Figure 4 Legal and Regulatory Compliance

4 Threats to Cryptocurrencies

With cryptocurrencies, these systems have been replaced by decentralized alternatives to traditional finance. However, the rise of these digital assets has brought security threats. Cyberattacks and vulnerabilities are not overcoming challenges to the trustworthiness and value of cryptocurrencies.

4.1 Cryptocurrency Exchange Hacks

The huge amounts of money on cryptocurrency exchanges make their target number one for cybercriminals. Many cyber-attacks against these exchanges range from hacking and insider threats to sophisticated malware infections. Millions of cryptocurrencies have been stolen in high-profile exchange hacks in recent years. Hackers exploit weaknesses in the exchange's security architecture, including unpatched software vulnerabilities, weak authentication protocols, and lack of encryption.

For instance, the massive 2014 Mt. Gox hack was responsible for losing almost 850,000 bitcoins (Johnstone, 2019). The stolen funds could not be recovered despite efforts by the event to regain their lost funds, which did not look good to traders who held high confidence in cryptocurrency exchanges. Usually, hackers exploit methods such as SQL injection or cross-site scripting (XSS) to fish around the exchange platform's code to get illegal account and wallet privileges. Once in, the digital assets can be transferred to their addresses, leaving minimal transaction detail.

4.2 Phishing and Social Engineering Attacks

Phishing and social engineering are still among the best methods of stealing cryptocurrency from unwary users. In these attacks, malicious actors trick users into disclosing private keys, recovery phrases, and account credentials by faking websites, emails, or messages almost identical to their intended cryptocurrency services. Phishing attacks have successfully run crypto wallet users and cryptocurrency exchange customers. The users' login details are then tricked into the fraudulent site created by hackers to mimic some common platforms. Moreover, social engineering attacks might also be directed at making users download malicious software pretending to be a wallet or security update (Weber et al., 2020). When a username and password are entered on the malicious site or software, the attacker gains control over the user's private keys and the cryptocurrency safely kept in the wallet.

In another form of phishing, scammers impersonate popular coins or exchange creators to phish the victims into sending funds to a fraudulent address. The attacks, which usually involve attacking public personalities and cryptocurrency influencers, are often launched through a social media platform, where the trust they gain from users is exploited.

4.3 Wallet Theft and Loss of Private Keys

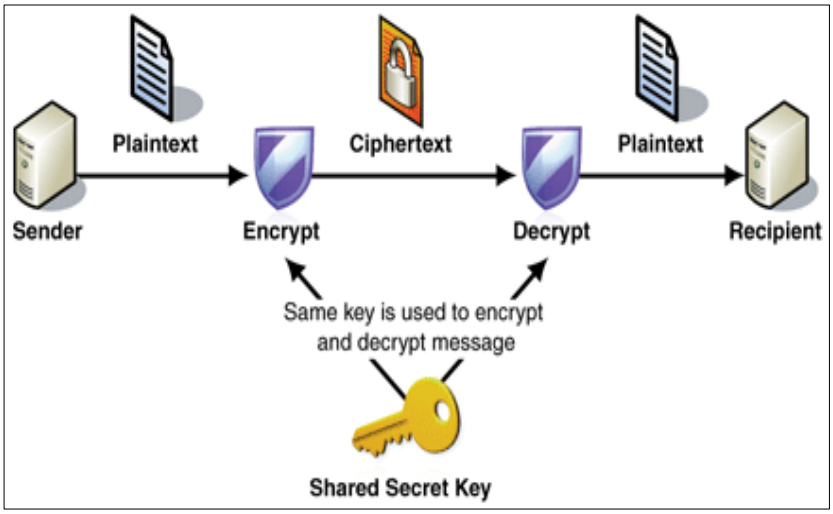

Figure 5 Private Key Cryptosystem

The biggest risk to cryptocurrency's security is losing or stealing someone's private keys. A private key is a cryptographic string that allows a user to access and manage his cryptocurrency holdings. If a user's private key is stolen, the attacker gains full control over the wallet and can transfer assets to any address the attacker would like. Similarly, if a user loses their private key, they also lose access to their funds because no central authority can recover it.

Several currencies are available in hardware, paper, or software wallets. Hardware wallets are considered the safest because they store private keys outside the Internet. However, they are also susceptible to being physically stolen if not tucked away protected. Computer or smartphone-based software wallets are much more vulnerable to malware or hackers. In the case of cloud-based platforms for storing private keys, users would be exposed to even more risks, such as data breaches and hacker intrusions (Akhtar et al., 2012).

Users are asked not to store their wallets using the same password that they use for everyday browsing, and they are also advised to enable two-factor authentication and back up securely. However, long-term storage, that is, safe keeping for years, leans toward cold storage methods like hardware wallets and air-gapped devices.

4.4 Crypto Mining Malware

One emerging threat is cryptocurrency mine malware, which attacks the computational power of infected systems to mine cryptocurrency without the owner's consent. Typically delivered via phishing emails or malicious websites, this malware, called cryptojacking, is a version of malware our collective mind will think of from this moment on as "cryptojacking." Once executed, the malware sits in the background and starts to mine digital currencies like Bitcoin or Monero using that system's processing power.

Cryptojacking malware is usually invisible to the user as it operates in the background, mining for coins and using the host's resources. However, with time elapsed, this can significantly drop system performance, cause overheating, and damage hardware, especially with personal computers or mobile gadgets (Gunawi et al., 2018). Sometimes, the attacker may spend much time installing malware in a large network, such as an enterprise network or cloud servers, which would scale the attack differently and cause higher economic gain. Since mining malware has some risks, the best way to mitigate them is to use powerful antivirus programs, update the systems regularly, and avoid downloading files or visiting sites from untrusted sources. In addition, companies should use network monitoring tools to detect strange activities that indicate unauthorized mining operations.

4.5 Risks from Insecure Cryptographic Algorithms

Cryptocurrency security fundamentally depends on using cryptographic algorithms to protect user data, verify transactions, and maintain the integrity of the blockchain. Using these cryptographic techniques hinged on their continued adaption, but with progressive increases in computational powers, there are inherent risks. For instance, the advances in quantum computing can weaken most of the cryptographic technology utilized by the current

cryptocurrency system, such as elliptic curve cryptography (ECC) (Mavroeidis et al., 2018). Quantum computers can theoretically crack cryptography, securing private keys and Bitcoin transaction signatures if they have sufficient computing power. Practical quantum computing is not yet mature, but the possibility of threat has led to post-quantum cryptography research, an algorithm that should resist quantum attacks (Nyati, 2018). Given the threat of quantum computing to the long-term security of cryptocurrencies, these solutions need to be implemented before quantum computing is inevitable.

Along with quantum threats, vulnerabilities exist in cryptographic algorithms that allow attackers. This includes unforeseeable keys generated by weak random number generation and a past hashing algorithm that makes the blockchain vulnerable to attacks. Any cryptographic vulnerability in any layer of a blockchain system, starting with wallet generation and going right through to block hashing, compromises the integrity of the whole network (Latifa Omar, 2017). Due to cryptographic algorithm vulnerabilities, exchange hacks and private key theft threaten these cryptocurrencies' security. The cryptocurrency ecosystem undergoes tremendous modification, as do the means to protect it from these threats. For individual users and the wider cryptocurrency network, it is very important to have robust security practices, to run a system update weekly, and to keep a background check for incoming risks.

5 Blockchain Security Solutions

Due to their decentralized, secure, and immutable properties, blockchains have become the procedure for conducting digital transactions. However, as they are adopted, security must be robust. Many blockchain security solutions are becoming a reality to alleviate the problem of securing decentralized systems and cryptocurrencies.

Table 2 Blockchain Security Solutions

Solution Type	Description	Key Technologies	Purpose
Cryptography	Ensures data integrity and privacy through encryption.	Asymmetric cryptography, Hash functions	Data security and privacy
Enhanced Consensus Protocols	Optimizes security and network validation.	PoW, PoS, DPoS	Secure transaction validation
Multi-signature Solutions	Requires multiple signatures for transaction approval.	Multi-sig wallets	Protects against single point failures
Cold Storage Solutions	Offline storage of cryptocurrency to prevent theft.	Hardware wallets, Paper wallets	Prevents online theft
Privacy Enhancements	Improves user privacy while maintaining transaction validity.	Zero-knowledge proofs, zk-SNARKs	Enhances confidentiality

5.1 Cryptography in Blockchain Security

At the core of blockchain security lies cryptography. Data security through cryptographic techniques is ensured through data integrity and privacy, and trustless transactions between parties are facilitated. Asymmetric cryptography plays a very important role in Blockchain. Public key and private key systems are the cornerstones of Blockchain. In public key cryptography, public and private keys are given to each user so they may securely send and receive funds or information (Konashevych, 2020). The private key is only known by the person who will sign a transaction and can be thought of as signing our name on that document, its signature, to glorify it as honest. The public key is made public for everyone to know so that we can determine with that public key if someone has a valid private key or not.

Hash functions are also essential for ensuring data integrity, in addition to public-key cryptography. A hash function converts the input data (for example, a transaction or a block) into a fixed-size string of characters, so every input data yields the same fixed-size string of characters. Any change in the data would yield a completely different hash, and it is almost impossible for any malicious actors to change the Blockchain without detection. This is one of the core requirements for the immutability of the Blockchain, which is an absolute guard from fraud and tampering. Cryptographic algorithms, including the elliptic curve digital signature algorithm (ECDSA) and SHA 256, are common in blockchain platforms like Bitcoin and Ether to produce secure transaction signatures (Sathya & Banik, 2020).

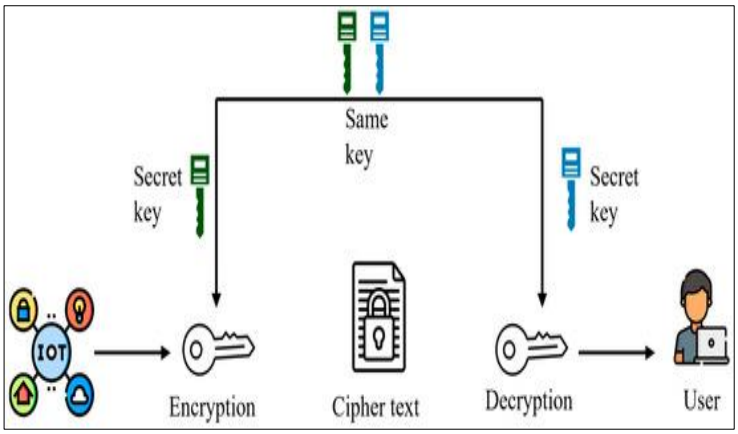

Figure 6 Conceptual framework for secure and scalable IoT integration in smart city infrastructure.

5.2 Enhanced Consensus Protocols (PoW, PoS, and DPoS)

The consensus protocols are integral to a blockchain network's security and functionality management. They decide how participants agree on the valid transactions and the blocks to be ordered. Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) are among the most used consensus mechanisms. Considered one of the best consensus algorithms, Proof of Work (PoW) is used in Bitcoin and other cryptocurrencies (Bach et al., 2018). Miners are required to solve complex mathematical problems to add new blocks to the Blockchain. As this process consumes much computational power, it is hard for attackers to manipulate the network. PoW security is based on reusing the resources necessary to mine all subsequent blocks to create a block.

Specifically, it is an energy-efficient alternative to POW, which has been popularized by Ethereum 2.0 and several other blockchain projects. Unlike these conventional methods, PoS selects validators based on the cryptocurrency they stake as collateral instead of submitting to miners to solve computational puzzles to gain cryptocurrency. The blockchain integrity is maintained by Validators who are rewarded for it. PoS is secure because of the penalties an attacker is charged for malicious activity. The staked coins of a validator are forfeited if it tries to create invalid blocks.

Delegated Proof of Stake (DPoS) is a variant of PoS that aims at scaling and speed. In a style like DPoS, the token holders will vote for a few delegates responsible for verifying transactions and protecting the Blockchain (Chaumont et al., 2019). This provides decreased security and increased efficiency from fewer validators while maintaining decentralization. Note that all these consensus mechanisms have multiple strengths and weaknesses. However, these mechanisms have been essential in preventing various attacks, including the 51% attack, in which an illegitimate entity has the majority control over the network.

5.3 Multi-signature and Cold Storage Solutions

Multi-signature (multi-sig) solutions boost the security of cryptocurrency wallets and transactions. Instead of one, multi-signature wallets require at least two (more likely, numerous) different private keys to authorize a transaction. That means even if a malicious actor gets hold of one of the private key keys, individuals still has to obtain the other key to carry out the transaction. Many people and companies use multi-signature wallets because they want an additional secure way to keep their digital assets (Di Nicola et al., 2020). For example, a business may set up a multi-sig wallet requiring three of five (keyholders) signatories to approve a transaction before it is carried out. This approach prevents unauthorized withdrawals and ensures that no one can control the funds.

An important security feature of the blockchain ecosystem is cold storage solutions. Slowly but surely, cold storage of crypto keys is becoming a trending practice, and the term is gaining popularity just like that, as it is the counterpart of hot storage. Hardware and paper wallets or air-gapped systems are widely used to achieve cold storage. Since cold storage eliminates the risk of online attacks, it is considered the most secure method of storing cryptocurrencies for long-term holding.

Cold storage is usually not done on the device we use to communicate with the network (computer) but on a hardware wallet like Trezor or Ledger, which offers a secure and user-friendly interface for managing the device's private keys (Guri, 2018). These wallets rely on secure chips, which makes it almost impossible for an attacker to bilk out private keys if they manage to snatch a device physically.

5.4 Privacy Solutions (Zero-knowledge Proofs, zk-SNARKs)

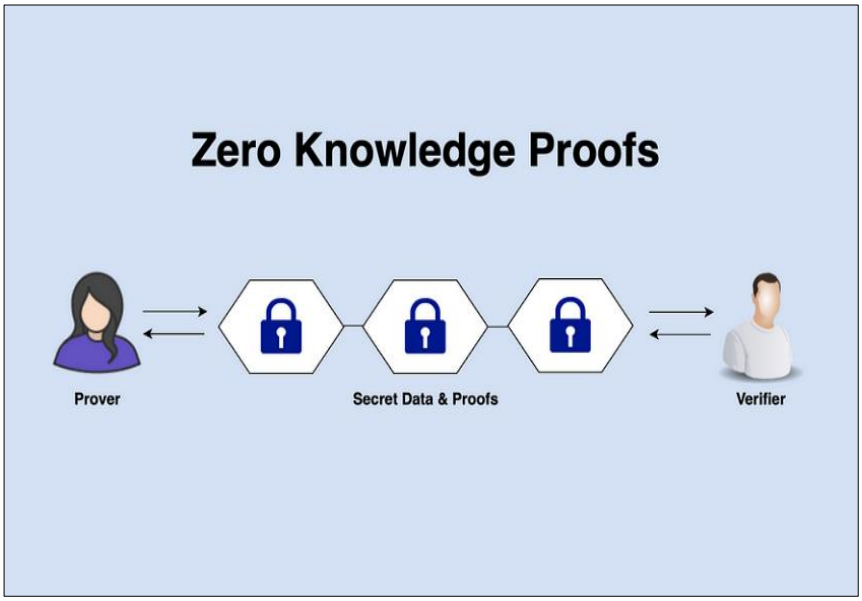

Figure 7 Zero-Knowledge Proofs

Both the strength and weakness of blockchain is transparency. It does not eliminate privacy concerns as transactions' financial details are exposed to the general public. To overcome the problem, zero-knowledge proofs (ZKPs) and zk-SNarks are created. Zero-knowledge proofs enable one party to prove without leaking that a first party knows the information, such as a secret key (Sun et al., 2021). In the context of blockchain, ZKPs facilitate the validation of transactions without revealing transaction details like the amount or the sender and receiver's addresses. The mechanism assists in enhancing privacy in that only the required information is shared across the blockchain without compromising its integrity.

Zk-SNARKs are one particular type of ZKP and can even be further improved in terms of efficient privacy preservation, as seen in privacy-aware cryptocurrencies such as zCash, which use them to mask transaction data. Using zk-SNARKs, you can ensure the privacy of the entire transaction by hiding the sender and receiver addresses, the transaction value, and the whole thing on the blockchain (Guan et al., 2020. They address one of the key challenges of a system with low trust and high transparency and provide these solutions while maintaining confidentiality, as it is in a decentralized, high-transparency system. These privacy solutions are necessary for blockchain applications that need to be more private, such as financial services or personal data management.

5.5 Blockchain Security Audits and Penetration Testing

Security audits and penetration testing are great practices in blockchain systems to identify vulnerabilities. A security audit of blockchain means analyzing blockchain architecture, smart contracts, cryptographic protocols, and consensus mechanisms to safely hunt down possible security threats to the blockchain. Exploits can present vulnerabilities and can be incorporated by coding errors, design vulnerabilities, or configuration issues.

Penetration testing, however, is the process of simulating attacks on the blockchain system to identify other holes before the hackers can exploit them. Typically, these tests can include smart contract vulnerabilities, wallet security, and attack vectors that would compromise the integrity of the network. Ethereum and Bitcoin platforms often go through extensive security audits to make sure their protocols and applications are, in fact, not vulnerable to attacks (Dika, 2017). Security audits and penetration tests are usually regularly used to prevent vulnerabilities from developing and verify that blockchain networks are secure and reliable.

5.6 Decentralized Identity Management

DID solutions are emerging as one of the key security features for blockchain networks. Traditional identity management systems naturally trust centralized authorities, such as government agencies or banks, to validate identities. However, they are open to being breached by data and fraud.

Decentralized identity management uses blockchain technology to allow individuals access and ownership over their data. DIDs allow one to build and manage identity without relying on one central authority (Dunphy & Petitcolas, 2018). Blockchain guarantees the immutability and privacy of the identities, and participants allow some part of their identity to be revealed to trusted parties without compromising privacy. DIDs are particularly useful in sectors where checking someone or something's identity is essential for security, such as healthcare, finance, and supply chain management.

5.7 Network Monitoring Tools and Intrusion Detection Systems

Blockchain networks can be tracked and responded to threats using network monitoring and intrusion detection systems (IDS). The systems are always running and scanning the network blockchain for suspicious activity – like taking some strange transaction patterns, unusual height in the network traffic, and none of the normal activity in access to the blockchain pattern. It is an alert generator sent by IDS when it detects a potential threat and allows security teams to respond in real time.

An intrusion detection system can be integrated into a stable combination of other security tools, including firewalls and antivirus software, to form a total security infrastructure. For blockchain networks, anomaly detection algorithms may be used to recognize hostile actors aiming to tamper with or undermine the network (Bhatia, 2021). Common tools used in the industry are Suricata, Snort, or Zeek to monitor network traffic in search of intrusions. The tools described above are vital for blockchain systems' continuous security and health.

Blockchain security solutions are not one-dimensional; thus, integrating multiple technologies and practices is required to ensure that the decentralized systems do not become vulnerable to new threats. Each of these solutions works for the blockchain ecosystem to keep it safe from hackers, copyright theft, or other things that are not legit in the blockchain. From cryptography to consensus mechanisms, privacy solutions, and proactive security audits.

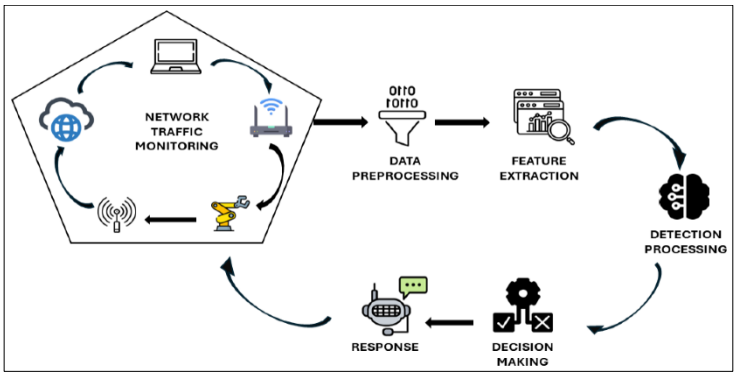

Figure 8 Architecture of NIDS in industrial and robotic systems**.**

5.8 Blockchain in Smart Contracts Security

Thanks to their automation and decentralization, smart contracts and self-executing contracts written in lines of code with the terms of the agreement have shaken all industries in which they exist. However, like any technology, there are risks associated with their security that must be effectively managed to prevent significant financial losses or exploitation of the system. In order for blockchain to become a mainstream tool, smart contract security is essential, and thesis particularly the case for decentralized finance (DeFi) and supply chain management.

Table 3 Common Smart Contract Vulnerabilities

Vulnerability Type	Description	Example	Risk Level
Reentrancy Attack	Attackers exploit the smart contract's recursive function.	DAO hack	High
Integer Overflow/Underflow	Unchecked arithmetic leading to unexpected values.	Loss of funds in contracts	High
Gas Limit Issues	Exceeding the gas limit resulting in contract failure.	Denial of service attacks	Moderate

Poor Authorization Checks	Lack of proper access control in contract functions.	Unauthorized withdrawal of funds	High

5.9 Common Smart Contract Vulnerabilities

Various vulnerabilities exist in constructing smart contracts, making them vulnerable to attack unless the smart Contract is not coded and safeguarded properly. One of the most troublesome hacks of today is reentrancy attacks, where the malicious actors exploit the smart Contract's function to repeatedly call to itself, thus changing the behavior of the Contract from what is expected (Huang et al., 2019). One example of this vulnerability that stands out because it was so public is the DAO hack on Ethereum, where attackers could pull millions of dollars out of the Contract through a reentrancy vulnerability in the escape mechanism of its withdrawal function.

Integer overflow and underflow are other common vulnerabilities in which a contract does arithmetic without verification. This error results in unanticipated values that exceed the maximum size, roll back to zero, or effectively attack contract balances. Developers should check overflow and underflow to prevent these issues. Moreover, gas limit vulnerabilities also need to be addressed (Kong, 2017). A parameter known as a gas limit dictates how much work a contract should be allowed to do. A contract can exceed the gas limit and fail to execute properly, causing the contracted functionality to be interrupted. This can be exploited by malicious actors who craft transactions to cause the gas limit to exceed, which leads to contract failure or denial of service.

Beyond that, security comes from smart contracts with no proper authorization checks, which means that any user can interact with critical functions without authorization. Conferring weak permissions allows attackers to elevate their privilege to adopt the contract logic or drain funds from the Contract.

5.10 Methods to Secure Smart Contracts

Several practices can be done to secure smart contracts and tackle the common vulnerabilities mentioned above. Among such methods, formal verification mathematically proves the correctness of a contract's logic before it is deployed. The Contract's code is analyzed against formal specifications through formal verification tools to ensure it does what it is supposed to do under all conditions. It assists in wiping out the defects that could not be identified by hand auditing or testing. Following the principle of least privilege can also be an effective strategy for making smart contracts operate with the minimum access necessary. This restricts permissions, reducing the Contract's attack and making it tougher for malicious users to exploit the system.

Smart contracts are vulnerable to vulnerabilities identified anywhere during development, such as code audits and peer reviews. Because developers should not just depend on automation, experienced professionals must perform manual audits of all aspects of the code. In open-source projects, peer reviews from the community can also include many additional layers of review, such as reviews from other developers (Wang et al., 2015). Incorporating fail-safe mechanisms such as emergency pause functions would also be safe. Consequently, these mechanisms allow contract owners or authorized entities to stop the Contract's slow if an activity is incriminated or if vulnerabilities are discovered without causing too much damage.

Figure 9 Block chain smart contracts

5.11 Best Practices for Writing Secure Smart Contracts

Trust the developers 'right from the start to secure smart contracts. It is important to minimize complexity in the contract design. A simple contract can be audited and is less likely to have vulnerabilities. Off the wall, complex logic can bring too many unforeseen risks, especially when different functions work unexpectedly. They should also look into code reusability, so it is easier to audit smaller modules independently in the future. Another best practice is developing module development, breaking a contract into smaller independent components; reviewing the individual modules for vulnerabilities is easier (Cobb et al., 2018). At the same time, developers should use existing libraries and frameworks they can rely on because they have been proven and tested by the blockchain community to be secure.

Another main practice is ensuring immutable contracts. After the smart contract is deployed to the blockchain, it should not be changeable to prevent compromising it through a vulnerability. Nevertheless, patching or upgrades require developers to employ upgradeable contract patterns that are safe from compromise to allow updates or bug fixes. Another best practice to reduce the exposure of sensitive data inside the Contract is not to store private data directly on the blockchain, such as private keys or personal information. Developers should encrypt and store sensitive information off-chain to minimize the exposure of a contract to data breaches.

5.12 Tools for Smart Contract Auditing

Several tools and platforms to audit and analyze smart ContraContract automatically check for contract vulnerabilities and go in depth. For example, MythX is an all-in-one smart contract security analysis tool that deals with vulnerabilities like reentrancy, integer overflows, and gas limits. It has hooks into common development environments such as Remix so that the compilers can get feedback on contracts in real-time as they develop. Slither is another widely used static analysis tool that checks Solidity code for common vulnerabilities and inefficiencies (Feist et al., 2019). This tool helps us not only provide developers with detailed reports on security flaws, gas optimization, and so on but also gives us feedback on best practice violations. Such tools allow developers to discover possible loops in development early in the development cycle, leading to fewer vulnerabilities getting by before their time.

ConsenSys Diligence provides an auditing service with automated analysis and manual code reviews from senior auditors for a more manual approach. This service guarantees that whatever is sent to a contract is tested throughout and that security is ironed out as soon as possible before the Contract is implemented. The other essential tool for smart contract development and testing is Truffle Suite. It is a suite of tools for smart contract compilation, migration, and testing, providing built-in support for testing in the development pipeline. Ganache from Truffle is a personal Ethereum blockchain meant to test with, run live transactions, and debug code in a safe environment (Aboualy, 2019). Using a mix of these tools and a strict audit process, smart contracts are made secure and risk-free, preventing expensive security breaches.

6 Real-World Successful Blockchain Security Case Study

Blockchain security has been repeatedly tested in real-world examples; several instances were pragmatic enough to prove the technology's integrity, and some showed what needs improvement.

Table 4 Blockchain Security Case Studies

Case Study	Incident Description	Security Lessons	Outcome
Ethereum DAO Hack (2016)	Exploited vulnerability in smart contract code.	Need for thorough code audits, importance of community response.	Ethereum fork to recover funds.
Walmart Blockchain Supply Chain	Secured food traceability system using blockchain.	Blockchain's role in supply chain transparency and fraud prevention.	Improved transparency in product tracking.
Bitcoin's Resilience to 51% Attack	Bitcoin's resistance to manipulation despite potential risks.	Importance of decentralization and mining incentives.	Bitcoin's stability due to high hash rate and decentralized network.

6.1 The Mitigation of Ethereum's "DAO Hack"

The most infamous security breach in blockchain technology history was the DAO (Decentralized Autonomous Organization) hack in 2016. Ethereum's DAO was intended to be a decentralized venture capital fund in the form of a smart contract that enabled investors to fund projects. A smart contract code vulnerability of the DAO allowed an attacker to drain a third of the DAO's funds, equaling 3.6 million ETH. The bug in this exploit resulted from a recursive call issue, which allowed the hacker to overwrite the amount after the contract updated its current balance by withdrawing funds multiple times.

Ethereum community was forced to choose how to fix things without destroying the blockchain. A hard fork was the solution, which was contentious. Such a change is called a hard fork, and it led the blockchain team to split into Ethereum (ETH) and Ethereum Classic (ETC) (Antonopoulos & Wood, 2018). The stolen funds were marked refunded with the Ethereum blockchain, while the chains remained unchanged in Ethereum Classic. Of course, this solution was not without backlash, given that immutability was being questioned, which is nothing more than the gist of blockchain technology. Nevertheless, ensuring users' investments and keeping possible confidence in the Ethereum network was considered worth it. After the DAO hack and its subsequent aftermath, it highlighted that smart contract audits are incredibly important and that dApps require even more robust testing. This was Ethereum's response on how the community can adapt, make decisions to protect the ecosystem, and impact the ecosystem, regrettably diverging from the vision of immutability.

6.2 Blockchain Security in Supply Chain Systems

Blockchain technology has increasingly secured supply chains, which provides traceability, transparency, and accountability. However, the most successful implementation has been the blockchain that major retailers like Walmart use to track food products from farm to store. The system is built over Hyperlegdear Fabric to achieve decentralization and transparency; it records any step in the supply chain as a producer, distributor, or retailer.

In this case, the ability to eliminate counterfeit goods and fraudulent claims due to blockchain is one major security advantage. In the past, consumers were not aware of the origin of consumer products, which posed health and safety risks. The immutability of the blockchain means that once a record is added, it cannot be changed, which assures the product's journey is true (Mougayar, 2016). In its use for tracking leafy greens, Walmart used blockchain in 2018 to trace its origin in seconds when it would have taken days before. This made tracking down contaminated foods easier and slowed foodborne illnesses from spreading further.

As this case shows, blockchain security practically applies to discovering supply chain security issues. By securing data in the decentralized network, businesses could eliminate single points of failure, decrease fraud, and improve global supply chain transparency. With the rise in such systems, blockchain integration is becoming a trend that will increase their security and operational efficiency (Nyati, 2018).

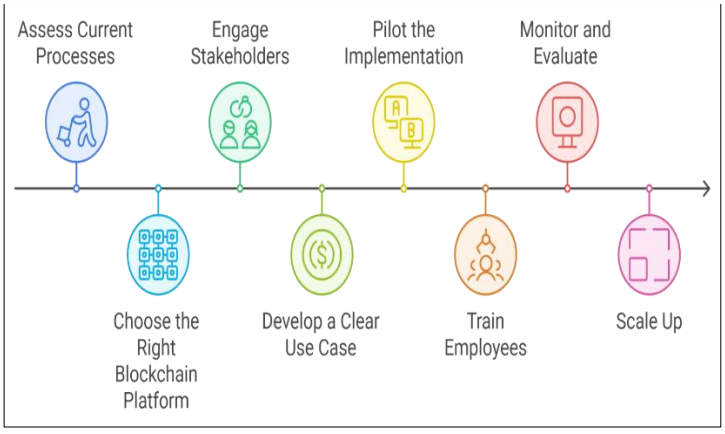

Figure 10 Supply Chain Transparency with Blockchain Technology

1.1.Bitcoin's Robust Security in Protecting Against 51% Attacks

Since 2009 Bitcoin was first created, its security has been tested rigorously, especially in terms of its vulnerability to a 51% attack. A 51% attack is when a bad actor or group of bad actors control most of a network hash power, leading to the ability to alter transaction histories and double-spend coins (Lovejoy, 2020). Even though there are theoretical risks,

Bitcoin remains strong in terms of 51% attack because the Bitcoin network is decentralized and distributed, and running a successful 51% attack on the network requires much work and money.

Likened to a 51% attack in 2014 on Bitcoin's arch-rival cryptocurrency, Litecoin, the hacker potentially stands to collect almost $400K worth of the coin. However, Bitcoin is more resistant to this type of attack than many other cryptocurrencies, with a much smaller hash rate and a more centralized network of miners. With the growth of the Bitcoin network, it is becoming more difficult for attackers to influence the blockchain, as the network's mining difficulty is adjusted dynamically according to the Bitcoin network's performance, and computational power is extremely high. The design of Bitcoin rewards miners with block rewards and transaction fees, which in turn encourages the miners to be honest (Carlsten et al., 2016).

This resilience perfectly positioned Bitcoin as a secure and trusted blockchain platform globally. However, it is easily argued that an attack of 51% is possible, albeit its economic and technical barriers to be overcome on the Bitcoin network attack such an order all but impossible. The case study of this paper shows how Bitcoin's first security model, based on proof-of-work (PoW) and incentives, keeps the network secure from potential threats.

6.3 Lessons Learned and Key Takeaways

Several of these case studies can be summarised with a few lessons learned. There is no doubt concerning the importance of thorough coding. The Ethereum's DAO hack showed the need to adopt secure smart contract coding practices and community-based responses that attenuate damage caused by discovering security flaws. Applying blockchain to secure supply chains clearly illustrates how a decentralized system can control data integrity and thwart fraud, giving a huge footing on security over traditional centralized systems (Werbach, 2018). The inherent robustness of Bitcoin against 51% attacks demonstrates the necessity of having a decentralized network structure and incentive mechanisms that prevent attacks on blockchain systems. The key takeaway from these cases is that blockchain technology is very secure in a sense, but it's not secure at all. To maintain the security of decentralized systems, there are regular audits, proper design, and community engagement. Blockchain goes beyond cryptocurrencies and has great potential in application areas, for example, improving the security of supply chain management.

7 Best Practices for Blockchain Security

Decentralized systems and cryptocurrencies depend on their blockchains' integrity and functionality, which can only be secured by this. Robust security measures are needed to mitigate risks of data security and fend against malicious threats.

7.1 Ensuring Robust Network Security (Firewalls and VPNs)

The integrity of a blockchain system relies on a secure network. Moreover, one of the main best practices in this regard is the installation of advanced firewalls and virtual private networks (VPNs). A firewall is the first security line of defense against unauthorized access to the blockchain node by filtering incoming and outgoing traffic in compliance with known security rules. Although DDoS attacks impacting blockchain nodes are preventable by redundancy, they are critical in keeping highly available system services unaffected in the case of attacks.

For instance, with VPNs, data traversing the network is protected and thus encrypted from others, which is not the case with p2p networks. It is especially essential in decentralized networks spread across several geographical locations. Participants and developers on the blockchain have to use VPNs to protect communication from being intercepted by attackers (Karbasi & Shahpasand, 2020). Moreover, the proper network segmentation of sensitive blockchain systems should be carried out to block sensitive blockchain systems from being compromised by the entire blockchain infrastructure if the vulnerabilities in one part of the blockchain paralizer do not affect the entire blockchain infrastructure.

7.2 Key Management and Securing Private Keys

Private keys are one of the most important parts of blockchain security. They are credentials that are used to prove the ownership of assets and authenticate transactions. When somebody loses a private key or a private key is compromised, permanent asset loss and unauthorized transactions are possible. For this reason, private keys need to be secured using blockchain security best practices.

Cold storage is one widely used technique for securing private keys. The keys are placed offline in hardware or paper wallets to make them immune to online threats. Multi-signature wallets provide another level of security with larger

blockchain operations by requiring multiple private keys to authenticate transactions and keeping the risk of having a single point of failure low.

Furthermore, proper backup and recovery procedures should allow for recovering private keys in the event of hardware failure or any other emergency. However, these selection keys must be stored in secure, separate, geographically located places so that if any of these keys are destroyed or are accessible by unauthorized persons, then it is critical.

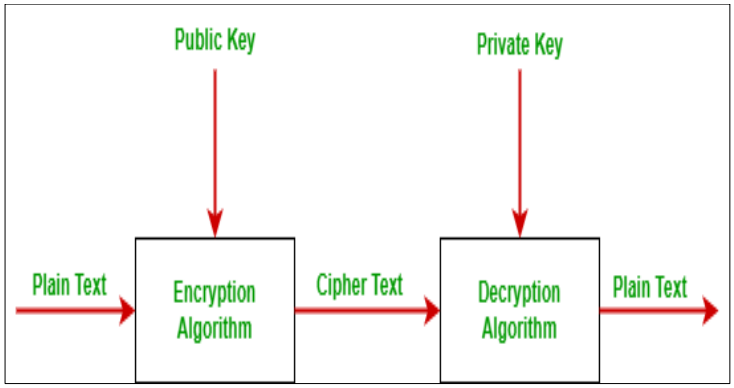

Figure 11 Public-Key Cryptography

7.3 Conducting Regular Security Audits and Penetration Testing

The security checks of blockchain systems should include regular penetration testing and security auditing to find and effectively eliminate the vulnerabilities that attackers can exploit. Audits are where one will check the blockchain's codebase, consensus mechanism, cryptographic protocols, and overall security architecture to ensure it fits the industry standards (Bhutta et al., 2021). A third-party independent person or entity should perform the security audits of the blockchain to perform an unbiased evaluation of the system's security posture.

It stimulates the blockchain attack on the infrastructure to discover the vulnerability. Pyramid Saimira says its staff participate in penetration testing to find potential vulnerabilities in the system and secure them—the aim is the same as what malicious hackers are doing. Penetration tests regularly help blockchain developers find weaknesses in smart contracts, cryptographic algorithms, and networks' protocols and patch them promptly. The effectiveness of the blockchain project is particularly dependent on conducting security audits and penetration tests to prevent it from being exposed to attacks and to offer transparency in the network.

7.4 Education and Awareness for Blockchain Users

From a blockchain perspective, developers, investors, and participants need to be educated on potential threats and best practices for maintaining security. User education is undoubtedly important in preventing social engineering attacks such as phishing, which are sometimes used to steal private keys or login credentials.

People using blockchains should be taught basic cybersecurity hygiene practices, such as using one's computer or phone to sign and verify transactions and avoiding phishing. Multi-factor authentication on user accounts is recommended as an extra security layer. Furthermore, developers developing smart contracts need to be educated about secure coding practices for smart contract development to avoid common vulnerabilities like reentrancy attacks or int overflow attacks (Zou et al., 2019). The user and developer must be informed of the emerging threats and their respective countermeasures through comprehensive training on blockchain projects.

7.5 Secure Software Development Lifecycle (SDLC) Practices for Blockchain Projects

A secure software development lifecycle (SDLC) is necessary for securing the security duty in developing blockchain systems. While blockchain development teams should consider security practices from design to deployment and maintenance, it is important to integrate such security practices at every stage of the SDLC. If blockchain developers plan and design the system, security features should be built into the system architecture. This includes selecting adequate consensus algorithms and cryptographic techniques with a high-security guarantee. In addition, developers should adopt the principle of least privilege, and every blockchain component should only have the minimum level of access required to execute the component's function.

In the coding phase, developers should use code static and dynamic analysis tools to identify code vulnerabilities and ensure smart contracts are free of critical security vulnerabilities. They should also implement regular code reviews and pair programming to discover any vulnerabilities that may arise early. In the test and deployment phase, the developers should conduct extensive functional and security testing, including stress testing and vulnerability scanning, before putting the blockchain system into production (Singh et al., 2020). Afterward, it should be monitored and patched to address any newly discovered vulnerabilities.

7.6 Regulatory Compliance and Legal Considerations for Blockchain Projects

Similar to other projects, blockchain projects should also be mindful of regulatory compliance and what is considered legal in different jurisdictions. Projects that seek to leverage blockchain technology to interact with financial systems, privacy laws, and data protection regulations must abide by applicable legal frameworks to reduce the risk of legal implications. For example, all blockchain-based implementations operating in the cryptocurrency segment must run according to anti-money laundering (AML) and know-your-customer (KYC) regulations to prevent such criminal activities as money laundering and fraud (Islam, 2021). Furthermore, Data Protection acts, such as the General Data Protection Regulation (GDPR) in the European Union, must be taken into account by projects too when handling personal data.

Besides consulting an expert legal counsel, blockchain organizations must check whether the blockchain's whole process and utilization comply with applicable legislation and avoid potential legal battles. Furthermore, they must react to emerging regulatory changes that will likely materialize as blockchain technology evolves and becomes mainstream. Implementing the above practices guarantees that blockchain systems are secure, resilient, and trustworthy. There are elegant network security practices such as regular audits, user education, effective key management, secure software development, and legal compliance, which help a comprehensive security strategy to defend blockchain ecosystems from new threats.

8 Blockchain Security and Privacy Enhancements

The transaction and data handling process has undergone a total transformation in Blockchain technology, with transparency, decentralization, and security as its strengths. On the other hand, these drawing points are also the issue that would make it unhealthy due to the lack of privacy and data protection. The Correspondence between the trustless blockchain and the ideas of privacy and security is ever stronger as blockchain applications unfold across commercial sectors of finance, supply chain management, and healthcare.

Table 5 Blockchain Privacy Protocols

Privacy Protocol	Description	Example Use Case	Security Benefit
Ring Signatures	Conceals the identity of the sender in a transaction.	Monero cryptocurrency	Enhanced user privacy
Stealth Addresses	Generates one-time addresses for transaction recipients.	Monero, ZCash	Conceals recipient identity
Confidential Transactions	Hides transaction amounts from the public.	Bitcoin's sidechain	Protects transaction value privacy
Zero-Knowledge Proofs (ZKPs)	Verifies transaction validity without revealing details.	ZCash, ZK-SNARKs	Ensures privacy without compromising security

8.1 Blockchain Privacy Protocols

By nature, blockchain networks are transparent about what is happening, as all transactions are recorded in an immutable ledger for all participants (Benchoufi et al., 2018). This, however, is beneficial to accountability, but it can also result in privacy issues, especially in public blockchains. As a result, several privacy protocols for ensuring privacy and preserving the integrity of the blockchain have been developed.

Ring Signatures are a commonly used protocol, and privacy-oriented cryptocurrencies like Monero use it. A user can sign a transaction on behalf of a group of people while keeping a secret on which member from that group signed the transaction. Privacy is thereby enhanced since the identity of the sender is blurred. Stealth addresses are another

privacy protocol that allows users to generate a separate transaction address, preventing any payment association with the user.

Another important privacy enhancement for Bitcoin has been Confidential Transactions, which are executed in sidechains such as Bitcoin or in privacy coins such as Monero. Third parties are not supposed to know the value of the transaction during CT, but the network should be able to verify that the transaction is valid. These privacy protocols are important because they avoid disclosing sensitive data to the party that is not allowed and continue to work the core functions such as decentralization and transparency.

8.2 Zero-Knowledge Proofs in Blockchain Privacy

These are known as zero-knowledge proofs (ZKPs), depending on how information is provided and received. These cryptographic techniques allow one party to prove to another that they know a value without revealing it. As such, ZKPs are essential for privacy on blockchain networks, particularly in public ledgers where the transactions are visible to everyone. Using ZKPs in blockchain systems gives one more privacy by allowing applications to be used without notifying many transaction details. This prominent implementation of ZKPs in the blockchain is Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), an efficient verification of transactions without revealing the sender's, receivers, or amount transferred details. ZCash uses zk-SNARKs to make shielded transactions, which means that users have a high level of confidentiality (Biryukov et al., 2019). In contrast, zk-SNARKs allow blockchain networks to remain secure and verifiable without losing their privacy.

An example is zk-STARKs (Zero Knowledge Scalable Transparent Arguments of Knowledge), which also enable the same but are not bound by the trusted setup, making them more transparent and scalable. For example, zk-SNARKs and zk-STARKs are among the most promising blockchain privacy advancements because they offer scalability and privacy while maintaining the security integrity of the blockchain.

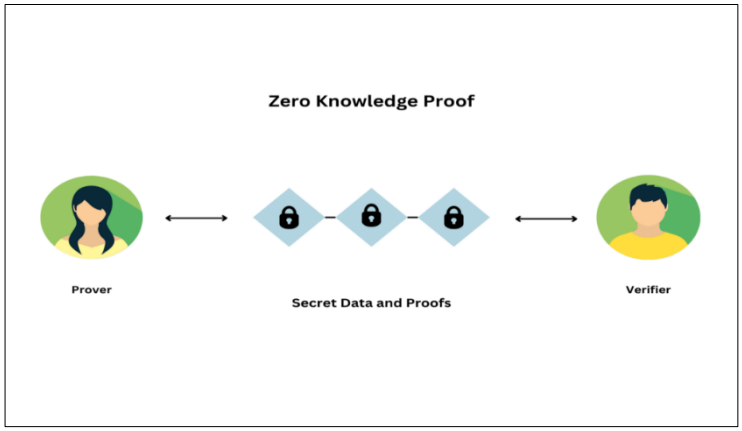

Figure 12 Zero Knowledge Proofs (ZK Proof)

8.3 Privacy Coins: Monero, ZCash, and Their Security Mechanisms

Monero and ZCash are popular privacy coins that allow regular users to decrease anonymity and make transactions more transparent. The coins utilize a very advanced cryptographic system that would not let you trace or connect them to particular users. Researchers use a combination of privacy protocols like Ring Signatures, Stealth Addresses, and Confidential Transactions, among other protocols, to provide privacy. With Ring Signatures, the sender's identity is concealed. With Stealth Addresses, each transaction uses a unique one-time address for the recipient, which does not connect the transaction to the recipient's address.

Confidential Transactions encrypt transaction amounts, so the value being transferred is also never unencrypted. Instead, ZCash uses zk-SNARKs to provide the possibility of shielded transactions. With this, users can transact privately without knowing the owner of the sender, the recipient, and the amount involved in the transaction. ZCash adopts a dual transaction model with transparent transactions (like Bitcoin) or private and shielded transactions, which allows users to choose what type of privacy they would like with their transactions. Monero and ZCash are always working on improving their privacy features to give users a greater confidentiality experience when transacting (Christensen, 2018). These coins offer excellent privacy improvements, but like any other, they have flaws, such as regulatory scrutiny and the risk of illicit use, as transactions with these coins are not traceable.

8.4 The Role of Encryption in Protecting Blockchain Data

It serves as a shield to protect blockchain data from anyone unauthorized, yet also as an aid to making blockchain data more private. The cryptographic techniques used on a blockchain network protect every transaction placed on the blockchain network and cannot be tampered with or tampered with later once added to the blockchain. Most of the time, blockchain networks rely on public and private key encryption to maintain the confidentiality and integrity of the transactions done within them.

Encryption is also used to protect users' identities in the blockchain. As a result, public key cryptography guarantees that only the recipient of a transaction can verify what data is 'hidden' within it. Encryption also protects sensitive information such as private keys, transaction details, and wallet addresses so that they can't be accessed without permission.

It is used with advanced encryption algorithms like Elliptic Curve Cryptography (ECC) to generate secure cryptographic keys in blockchain networks. The relatively small key size of ECC is favored compared to RSA because it lends itself well to providing strong security in decentralized networks, which have far fewer computational resources than centralized networks (Obert et al., 2019). Encryption is also important in smart contract protection, as smart contracts are self-executing contracts with the terms of the agreement right into the code. Encrypted smart contract data keeps private information, such as data leaks or unauthorized access, before and after the execution of smart contracts.

8.5 Balancing Privacy with Transparency

The challenge of blockchain security and privacy is balancing the privacy requirement and the blockchain's inherent unchangeability. Blockchain's transparency is one of its biggest advantages because everything is public, and each participant can verify the transactions. However, this transparency may contradict the requirement for privacy in some cases, such as when responding to the need for privacy regarding personal and financial data. The right balance is not easy to find. For use cases like confidential transactions that require privacy first, privacy-focused blockchain systems like Monero and ZCash would be perfect, as they sacrifice full transparency for privacy (Connell, 2018). At the same time, these systems may have problems in industries where regulations such as anti-money laundering (AML), know-your-customer (KYC), and others can require full transparency on the part of the system.

However, permissioned blockchains used in enterprise environments provide a greater level of controlled transparency through the permissions of different data to different user roles. The hybrid model allows for regulation and internal auditing while still maintaining confidentiality. In the future, there can be privacy-preserving consensus mechanisms and selective disclosure methods in blockchain systems that will let users share only the required part of the transaction information while keeping other parts of the transaction private (Satybaldy & Nowostawski, 2020). Some technologies, such as zk-SNARKs and other zero knowledge-proof systems, have started developing these advancements and may bring in solutions for achieving the balance between privacy and transparency the blockchain network might require.

9 Future Considerations and Evolving Blockchain Security Trends

Blockchain security is a high priority for innovation and an area of intense focus on the future of blockchain. As blockchain technology gains momentum in many industries, security becomes increasingly necessary, and it needs to be provided for decentralized systems and cryptocurrencies. As the security threat landscape expands to include new and emerging threats, blockchain attempts to address security issues while improving trade flow efficiency and new technology integration.

Table 6 Emerging Blockchain Security Trends

Trend	Description	Potential Impact	Technology Involved
AI in Blockchain Security	AI can predict and detect new threats in real-time.	Enhanced vulnerability detection	Machine Learning, AI algorithms
Quantum Computing	Quantum computing's ability to break existing cryptographic algorithms.	Need for post-quantum cryptography	Quantum-resistant algorithms

Decentralized Security Solutions	New decentralized identity management and key management protocols.	Increased user control and reduced centralized risks	Decentralized Identity Management, Blockchain IoT security
Cross-Chain Security	Ensuring secure transactions between different blockchains.	Improved blockchain interoperability	Cross-chain protocols (Polkadot, Cosmos)

9.1 The Role of AI in Blockchain Security

Blockchain security is getting increasingly enhanced with artificial intelligence (AI). AI algorithms can analyze blockchain data to discover possible vulnerabilities and avoid malicious activity. For instance, machine learning models can identify abnormal transaction patterns, unauthorized access attempts, and fraud in real time (Khurana, 2020). As an aid to blamelessness audits, AI can facilitate organizations to proactively inspect the quality of blockchain streams, keen contracts, and Dapplications (dApps).

AI is advancing the optimization of consensus mechanisms because it allows AI to react and evolve with changing network conditions to enhance security. AI models are used to train a way to predict and recognize new types of attacks, which further improves blockchain's robustness against sophisticated cyber threats like Sybil attacks or 51% attacks (Waheed et al., 2020). AI is an indispensable instrument for guaranteeing the scalability and security of a blockchain system, especially as these networks expand in their complexity and range of operations (Kumar, 2019).

9.2 Quantum Computing and Its Impact on Blockchain Encryption

The cryptographic security of blockchain is a major problem with quantum computing. On the one hand, it is claimed that quantum computers can perform exceptionally fast calculations over complex problems. On the other hand, they can undermine the existing blockchain encryption algorithms. Public key cryptography, which is so widely used to secure transactions and digital identities in blockchain networks, can easily be broken by quantum algorithms such as Shor's algorithm to efficiently factor large numbers.

As a result, the blockchain community is embarking on creating post-quantum crypto, making algorithms immune to quantum computing. The algorithms for securing blockchain transactions and user data from future quantum attacks will be designed to be new (Fernandez-Carames & Fraga-Lamas, 2020). Ensuring blockchain frameworks are secure for the long term requires that these algorithms be integrated into them. However, such changes should be implemented in an existing blockchain infrastructure, a challenge facing the industry regarding quantum resilience.

9.3 Decentralized Security Solutions

Blockchain networks' security is based on the fact that they are decentralized, which means that when a hacker is hit, the entire network – all nodes, computers, and so on – incurs damage; on the other hand, this also creates obstacles. Usually, such a decentralized environment is not used for traditional centralized security solutions (i.e., firewalls and intrusion detection systems). In today's world, as blockchain matures, it's a done deal that the industry will focus on creating innovative decentralized security solutions to shield the blockchain ecosystem against new threats while maintaining the trustworthiness of the blockchain's decentralized design.

An approach being developed is decentralized identity management systems. These systems allow the user to manage his digital identity without depending on centralized authorities, thereby helping to prevent data breaches and breaches of unauthorized access. In addition, decentralized key management protocols are being proposed to achieve key management of private keys, without which blockchain transactions would not be secured (Zhang et al., 2019). These solutions give users more control over their data and enhance the overall security of blockchain networks. Blockchain-based Internet of Things (IoT) device security solutions are being experimented with. These solutions rely on blockchain's decentralization to forge more resistant and secure networks of IoT devices, shielding them from risks of compromised devices and unauthorized access.

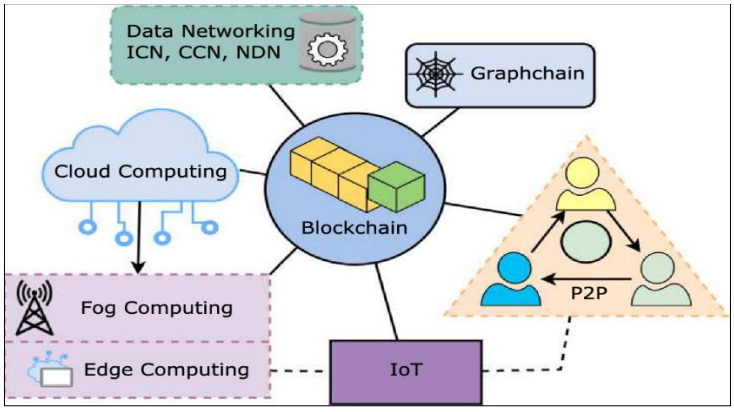

Figure 13 Blockchain components

9.4 Emerging Blockchain Security Frameworks

There is an increased demand for security frameworks adaptable to blockchain technology in several emerging industries, including healthcare, supply chain management, and finance. They aim to draft frameworks to set up how blockchain applications save our data, communicate across different blockchains, and secure them. The emerging blockchain security framework focuses on securing decentralized applications (dApps) and smart contracts and meeting regulatory and legal standards.

Such a framework is the "Blockchain Security Protocol" (BSP) to resolve certain security problems in blockchain-based applications. The BSP also promotes securing smart contracts, mitigating risks from transaction malleability, and setting a consensus algorithm standard. ISO/TC 307, which implements international standards for blockchain technology, outlines blockchain security practices and thus creates a secure environment for blockchain adoption worldwide (Al Ketbi et al., 2021). Continuing to work in the realm of blockchain, the next blockchain security frameworks are likely to emerge as a way to adapt to new threats, such as those from privately developed AI and quantum computing.

9.5 Interoperability and Cross-Chain Security Challenges

Interoperability between blockchain networks is critical to the mass adoption of blockchain technology. As more organizations and platforms use blockchain, the need to communicate across many chains is also growing. Nevertheless, this interoperability introduces distinct security constraints, especially related to exchanging secure data among chains and the chain integrity of transactions in different networks.

Cross-chain security is important since the assets and data are transferred across blockchains. These transactions are not properly secured and would be at risk of attacks such as double spending or man-in-the-middle attacks. Solutions to such concerns require new cross-chain security protocols. For example, interoperability frameworks like Polkadot and Cosmos try to establish secure bridges between blockchains, enabling seamless, secure transactions (Lohachab et al., 2021). However, ensuring that these cross-chain transactions are securely tied to validating them while preventing malicious actors from exploiting vulnerabilities remains challenging. Blockchains are expanding their coverage on different networks and creating interaction between chains, and in this regard, we will still need to invest heavily in cross-aim security.

9.6 Regulatory and Legal Landscape Evolution

Like any emerging technology, blockchain is progressing, which is true for the regulatory and legal landscape. Regulatory bodies and governments are becoming increasingly interested in creating rules and guidelines for using blockchain in various segments, especially with respect to cryptocurrencies and decentralized finance (DeFi). To be adopted as regulations, these rules will prevent money laundering and fraud, control bank consumers, and safeguard financial stability.

The future will require regulatory frameworks to adapt to this decentralized aspect, for example, not having centralized control or being able to apply traditional laws on a decentralized system platform. The regulations of blockchain networks and their security mechanisms will be changing along with landmarks like the General Data Protection Regulation (GDPR) of Europe, anti-money laundering (AML), and Know Your Customer (KYC) (Walther, 2018).

It is certainly possible that as the world becomes more 'blockchain,' regulators will need to simultaneously support innovation and protect security. Smart contracts, decentralized apps, and cross-border transactions have legal challenges for blockchain regulation that will need a dynamic approach that balances security and compliance without compromising the progress of the technology. AI integration, the difficulties of quantum computers, the development of decentralized security solutions, and emerging security frameworks set the future of blockchain security. Interoperability, security in cross-chain, and shielding blockchain technology from new threats will lead blockchain technology to grow securely and resilient to emerging regulatory environments.

10 Conclusion

The application of Blockchain technology in so many industries has introduced decentralized, secure, transparent systems. However, as blockchain's adoption extends, providing cryptographic methods to decentralized systems and crypto assets becomes more important. As the technology gets more complex and the use is larger, the blockchain security problems become even bigger. Despite the name of the technology that protects against the threats mentioned above, fundamental features make blockchain secure, namely cryptography, decentralized consensus mechanisms, and immutability. However, this built-in feature is not enough for absolute security. Security challenges of blockchain systems, especially those used for cryptocurrencies like Bitcoin and Ethereum, exist to a multitude. These challenges include risk in 51% of attacks, smart contract vulnerabilities, scalability problems, and recurring privacy issues. These risks are, in turn, massive threats to the functionality of blockchain networks and also to the trust users place in these systems. A notable case in this regard happened in 2016 at Ethereum in the form of the DAO, after which the vulnerabilities in smart contracts can result in enormous economic losses, as you can determine via inspection and strict coding practices.

Security challenges relating to ZPresentation are twofold; addressing them requires a multi-faceted approach. Advanced cryptographic techniques have been developed to achieve the said levels of privacy in the context of blockchain systems, including zero-knowledge proofs and zk-SNARKs. Consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS) are not ideal. However, they are perfectly adequate in ensuring the validity of transactions. Consensus mechanisms and hybrid models are innovations that are gaining more sophistication, yet blockchain remains resilient to new threats to security. Also, cryptocurrency assets have been secured with solutions such as multi-sig wallets and cold storage to protect private keys from theft and all other types of access.

New technologies, such as artificial intelligence (AI) and quantum computing, will affect the security of blockchain in the future. Broadly implementing AI to blockchain security can help detect vulnerabilities and prevent forgery or malicious activity in real-time by analyzing vast amounts of logistic blockchain data. With the growth of the complexity of blockchain networks, AI can be employed to optimize consensus mechanisms and fortify the whole network's security. On the other hand, quantum computing can render blockchain's cryptographic foundations vulnerable, especially in public key cryptography. With the increased power of quantum computers, today's encryption would become obsolete. The formal reaction counters have already engaged blockchain user groups in exploring post-quantum cryptography to maintain the security of blockchain systems.

Forming part of blockchain security, regulatory compliance does not necessarily mean compliance with a crypto-specific regulatory body. Since blockchain technology is now more integrated into mainstream industries, governments and regulators are creating ways to regulate and handle the legal challenges that decentralized systems bring into the picture. Researchers must find ways to balance the innovative and the secure in finance, healthcare, and supply chain management. However, blockchain networks have to evolve in order to be compliant with data protection laws such as the General Data Protection Regulation (GDPR) and adhere to anti-money laundering (AML) and know-your-customer (KYC) laws. Therefore, blockchain governance is evolving to adapt to these continuous security threats and regulatory standards.

Decentralized security solutions will also promise to fix many of the blockchain's inherent vulnerabilities. For example, decentralized identity management systems allow people to control their data, making it possible to locate private keys securely. On top of that, the necessity for cross-chain security now has to be secured as more blockchain networks interconnect. It is important to guarantee the security of cross-chain transactions and the protection from attacks, including double spending in the process of the blockchain systems integration between the different lineups. Blockchain security is a rapidly developing field that consistently demands innovations and modifications to existing technologies and dangers (Chavan, 2021). Today's blockchain, however, employs security mechanisms that must adapt to changing challenges brought by AI, quantum computing, and regulatory changes. Blockchain technology is still developing, and as it grows in other industries, maintaining a secure and sound blockchain ecosystem is of great

significance. Blockchain has the potential to stay a strong, trusted solution for decentralized systems and cryptos with the appropriate security in place.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aboualy, M. (2019). Learning Best Practices from Web Applications to Avoid Similar Security Vulnerabilities in Decentralized Applications.

[2] Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE transactions on dependable and secure computing, 15(5), 840-852.

[3] Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science Engineering and Technology.

[4] Al Ketbi, M., Shuaib, K., Barka, E., & Gergely, M. (2021). Establishing a security control framework for blockchain technology. Interdisciplinary Journal of Information, Knowledge, and Management, 16, 307.

[5] Antonopoulos, A. M., & Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media.

[6] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO) (pp. 1545-1550). Ieee.

[7] Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research, 6, 66.

[8] Bhatia, K. (2021). A Blockchain Based Framework for Reputation Management and Node Misbehaviour Detection in Wireless Sensor Networks (Doctoral dissertation, Dalhousie University).

[9] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9, 61048-61073.

[10] Biryukov, A., Feher, D., & Vitto, G. (2019, November). Privacy aspects and subliminal channels in zcash. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 1813-1830).

[11] Carlsten, M., Kalodner, H., Weinberg, S. M., & Narayanan, A. (2016, October). On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 154-167).

[12] Chaumont, G., Bugnot, P., Hildreth, Z., & Giraux, B. (2019). DPoPS: Delegated Proof-of-Private-Stake, a DPoS implementation under X-Cash, a Monero based hybrid-privacy coin. X-Cash, Irvine, CA, USA, Tech. Rep, 1-46.

[13] Chavan, A. (2021). Eventual consistency vs. strong consistency: Making the right choice in microservices. International Journal of Software and Applications, 14(3), 45-56. https://ijsra.net/content/eventual-consistency-vs-strong-consistency-making-right-choice-microservices

[14] Christensen, S. (2018). A comparative study of privacy-preserving cryptocurrencies: Monero and zcash (Doctoral dissertation, Master's thesis, University of Birmingham. 47, 79).

[15] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE access, 4, 2292-2303.

[16] Cobb, C. A., Watson, C. T., & Ellis, S. R. (2018). Establishing best practices for effective online learning modules: a single institution study. Medical Science Educator, 28, 683-691.

[17] Connell, D. (2018). Do EU Regulations Combating Money Laundering and the Financing of Terrorism Adequately Tackle Cryptocurrency: The Case of Ireland. Irish J. European L., 21, 68.

[18] Di Nicola, V., Longo, R., Mazzone, F., & Russo, G. (2020). Resilient custody of crypto-assets, and threshold multisignatures. Mathematics, 8(10), 1773.

[19] Dika, A. (2017). Ethereum smart contracts: Security vulnerabilities and security tools (Master's thesis, NTNU).

[20] Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE security & privacy, 16(4), 20-29.

[21] Feist, J., Grieco, G., & Groce, A. (2019, May). Slither: a static analysis framework for smart contracts. In 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (pp. 8-15). IEEE.

[22] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.

[23] Guan, Z., Wan, Z., Yang, Y., Zhou, Y., & Huang, B. (2020). BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs. IEEE Transactions on Dependable and Secure Computing, 19(3), 1446-1463.

[24] Gunawi, H. S., Suminto, R. O., Sears, R., Golliher, C., Sundararaman, S., Lin, X., ... & Li, H. (2018). Fail-slow at scale: Evidence of hardware performance faults in large production systems. ACM Transactions on Storage (TOS), 14(3), 1-26.

[25] Guri, M. (2018, July). Beatcoin: Leaking private keys from air-gapped cryptocurrency wallets. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1308-1316). IEEE.

[26] Huang, Y., Bian, Y., Li, R., Zhao, J. L., & Shi, P. (2019). Smart contract security: A software lifecycle perspective. IEEE Access, 7, 150184-150202.

[27] Islam, H. (2021). Adoption of blockchain in know your customer (KYC) verification process: A thematic analysis on European banking industry (Doctoral dissertation, Master's thesis]. Tallinn University of Technology).

[28] Johnstone, M. (2019). Catch Me If You Can: Resolving Bitcoin Disputes with Class Actions. Canadian Class Action Review, 15(1).

[29] Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2021). Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms. Wireless Communications and Mobile Computing, 2021(1), 4401809.

[30] Karbasi, A. H., & Shahpasand, S. (2020). A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks. Peer-to-peer networking and applications, 13, 1423-1441.

[31] Khurana, R. (2020). Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. International Journal of Applied Machine Learning and Computational Intelligence, 10(6), 1-32.

[32] Konashevych, O. (2020). Cross-blockchain protocol for public registries. International journal of web information systems, 16(5), 571-610.

[33] Kong, M. (2017). A scalable method to analyze gas costs, loops and related security vulnerabilities on the ethereum virtual machine. A scalable method to analyze gas costs loops and related security vulnerabilities on the ethereum virtual machine.

[34] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[35] Latifa, E. R., & Omar, A. (2017). Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures. Journal of Internet Banking and Commerce, 22(3), 1-29.

[36] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics, 8(10), 1782.

[37] Liu, Y., Wang, K., Lin, Y., & Xu, W. (2019). $\mathsf {LightChain} $: a lightweight blockchain system for industrial internet of things. IEEE Transactions on Industrial Informatics, 15(6), 3571-3581.

[38] Lohachab, A., Garg, S., Kang, B., Amin, M. B., Lee, J., Chen, S., & Xu, X. (2021). Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains. ACM Computing Surveys (CSUR), 54(7), 1-39.

[39] Lovejoy, J. P. T. (2020). An empirical analysis of chain reorganizations and double-spend attacks on proof-of-work cryptocurrencies (Doctoral dissertation, Massachusetts Institute of Technology).

[40] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

[41] Moroz, D. J., Aronoff, D. J., Narula, N., & Parkes, D. C. (2020). Double-spend counterattacks: Threat of retaliation in proof-of-work systems. arXiv preprint arXiv:2002.10736.

[42] Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.

[43] Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637

[44] Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230

[45] Obert, J., Cordeiro, P., Johnson, J. T., Lum, G., Tansy, T., Pala, N., & Ih, R. (2019). Recommendations for trust and encryption in DER interoperability standards (No. SAND-2019-1490). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Kitu Systems, San Diego, CA (United States); SunSpec Alliance, San Jose, CA (United States); Cable Labs, Louisville, CO (United States).

[46] Paik, H. Y., Xu, X., Bandara, H. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. Ieee Access, 7, 186091-186107.

[47] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. arXiv preprint arXiv:1904.03487.

[48] Santos, F., & Kostakis, V. (2018). The DAO: a million dollar lesson in blockchain governance. School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance.

[49] Sathya, A. R., & Banik, B. G. (2020). A comprehensive study of blockchain services: future of cryptography. International Journal of Advanced Computer Science and Applications, 11(10).

[50] Satybaldy, A., & Nowostawski, M. (2020, October). Review of techniques for privacy-preserving blockchain systems. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (pp. 1-9).

[51] Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654.

[52] Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. IEEE network, 35(4), 198-205.

[53] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM computing surveys (csur), 53(6), 1-37.

[54] Walther, M. (2018). EU General Data Protection Regulation and distributed ledgers (blockchain).

[55] Wang, J., Shih, P. C., Wu, Y., & Carroll, J. M. (2015). Comparative case studies of open source software peer review practices. Information and Software Technology, 67, 1-12.

[56] Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). Exploiting the human factor: Social engineering attacks on cryptocurrency users. In Learning and Collaboration Technologies. Human and Technology Ecosystems: 7th International Conference, LCT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22 (pp. 650-668). Springer International Publishing.

[57] Werbach, K. (2018). The blockchain and the new architecture of trust. Mit Press.

[58] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE access, 7, 118541-118555.

[59] Zhang, H., Wang, J., & Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy, 180, 955-967.

[60] Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., ... & Xu, B. (2019). Smart contract development: Challenges and opportunities. IEEE transactions on software engineering, 47(10), 2084-2106.