

A Survey on Block-Chain Technology Security and Privacy

Md Merazul Islam

School of Computer Science, Department of Software Engineering,
China West Normal University, Nanchong City, Sichuan Province, China

E-mail: md.miraj.br@gmail.com

Mohammad Abdullah

Software Engineer, China West Normal University, China

E-mail: abdullah917828@gmail.com

Abstract

Blockchain offers a progressive approach to storing facts, executing transactions, performing functions, and organizing beliefs in an open environment. Many do not forget blockchain as a technology breakthrough for cryptography and cybersecurity, with use instances starting from globally deployed cryptocurrency systems like Bitcoin, to smart contracts, smart grids over the net of things, and so forth. Although blockchain has acquired developing interests in both academia and industry within the latest years, the security and privacy of blockchains continue to be at the center of the controversy whilst deploying blockchain in specific programs. This text gives a complete review of the security and privacy of blockchain. To facilitate the discussion, we first introduce the notion of blockchains and its software in the context of Bitcoin-like online transactions. Then, we describe the basic security residences that might be supported because of the important necessities and constructing blocks for Bitcoin-like cryptocurrency systems, accompanied by way of imparting the additional security and privacy properties that are preferred in lots of blockchain programs. subsequently, we review the security and privacy techniques for reaching these security properties in block-chain-primarily based systems, including representative consensus algorithms, hash-chained storage, mixing protocols, nameless signatures, non-interactive zero-knowledge proof, and so on. We conjecture that this survey can assist readers to benefit from an in-depth understanding of the security and privacy of blockchain with an appreciation of ideas, attributes, strategies, and systems.

Keywords

CCS standards:

- Security and privacy
Privacy -maintaining
protocols;
allotted structures
security;

Additional Key-word
and phrases: Block
chain, security, privacy
and Bitcoin.

1. Introduction

Blockchain technology is the latest development in at-ease computing without centralized authority in an open community machine. From a statistics management perspective, a blockchain is a dispensed machine. Database that information an evolving list of transaction records organizing them into a hierarchy chain of blocks. From a security perspective, the blockchain is created and maintained through the use of a peer-to-peer overlay system including through the smart and decentralized use of cryptography with crowd computing.

It's far anticipated [30] that the once-a-year revenue of blockchain-primarily based business enterprise applications international will reach \$19.9 billion by 2025, an annual increase rate of 26.2% from about \$2.5 billion in 2016. Meanwhile, Goldman Sachs, Morgan Stanley, Citibank, HSBC, Accenture, Microsoft, IBM, Cisco, Tencent, Ali, and different global economic institutions, consulting agencies, IT companies, and groups. internet giants are accelerating laboratory research and capital distribution in blockchain technology. Blockchain, along with artificial intelligence and big data, are taken into consideration as the three core computing technologies for the next-generation financial industry. In addition to Bitcoin.com, numerous orthogonal efforts, which include the Hyper ledger challenge subsidized with the aid of IBM and the Apache basis, Ethereum [2, 23], and FileCoin [57] offer open supply structures and repositories for blockchain. investigation and improvement.

Governments have posted white papers and technical reports on blockchain to reveal their tremendous attitude in the direction of the development of blockchain generation. Inside the UK, the authorities the leader medical advisor posted a brand new document outlining the destiny of allotted ledger technology [90]. The EU principal financial institution published files at the distribution of accounting technologies in securities publish-trading [76]. The Chinese government posted. White papers on blockchain

generation and its improvement in China [85]. Inside the US, the governor of Delaware released the "Delaware Blockchain Initiative", which is a comprehensive software to construct a prison and regulatory environment for the improvement of blockchain technology. The governor of the country of Delaware officially signed a blockchain invoice in July 2017, which, if signed into regulation, will formally legitimize and approve the agencies registered within the state to control their accounting and different commercial enterprise transactions the usage of blockchain [24].

In academia, lots of papers on blockchain have been published within the past five years, including a dozen study reports on blockchain security and privacy threats. Joseph Bonneau et al. [twenty] provided the first systematic elaboration on Bitcoin and different cryptocurrencies, analyzed anonymity troubles, and revised methods to improve privacy. Ghassan Karame [54] evaluated and systematically analyzed the supply of blockchain security in Bitcoin, such as risks and assaults on Bitcoin as digital forex structures they also described and evaluated mitigation measures. Strategies to eliminate some of the risks. Mauro Conti et al. [32] reviewed the security and privacy of Bitcoin, such as current loopholes, which create numerous protection dangers in the course of the implementation of the Bitcoin system. Li et al. [61] tested the security dangers of famous blockchain systems, reviewed the assault cases suffered by way of blockchain, and analyzed the vulnerabilities exploited in those cases.

Maximum blockchain security and privacy studies have targeted two threads: (1) discover some assaults suffered by blockchain-based totally structures to this point, and (2) present precise proposals to appoint a few subsequent technology countermeasures against a subset of such attacks. but, very little effort has been made to provide an in-intensity evaluation of the security and Blockchain privacy properties and different blockchain implementation strategies. This survey offers a comprehensive assessment of blockchain security and privacy. First, we describe the belief in blockchains for online transactions and speak

about basic and extra security and privacy attributes of blockchains. We then analyze a hard and fast of corresponding security strategies, especially cryptographic solutions, to attain both basic and further security goals. We hold that as blockchain generation continues to attract interest and be applied in numerous programs, it is crucial to advantage of deep information of the security and privacy properties of blockchain and the diploma of accept as true with that blockchain can provide. Such knowledge can shed light on the basic causes of vulnerabilities in modern-day blockchain implementation fashions and offer technological foresight and innovation on strong defense strategies and countermeasures.

This survey article is designed with two objectives. First, it'll offer an access factor for non-security professionals to gain a better know-how of the security and privacy houses of blockchain. technology. Secondly, it'll assist specialists and researchers in discovering cutting-edge technology in security and Blockchain privacy strategies. moreover, we identify basic security attributes of blockchain. and extra security and privacy residences, speak of some security solutions to attain those security targets, and hint at open challenges. We assume that this survey can even guide the domain scientists and engineers to find blockchain models and techniques suitable for many domain-particular software situations.

We arrange the rest of the thing as follows. section 2 describes the basic ideas of blockchain. segment 3 describes the safety attributes that might be inherent or preferred in blockchain structures. phase 4 introduces consensus algorithms that can be utilized in blockchain-based systems. segment 5 analyzes the safety and privacy strategies that may be utilized in blockchain. 6 Security and privacy concern of Blockchain Technology. 7 Discussion, and phase 8 concludes the survey.

2 Overview of Block-Chain

The original documented blockchain design was in 2008, and the primary open supply implementation of Blockchain technology changed into applied in 2009 as an imperative element of Bitcoin, the primary decentralized digital machine. Financial system to distribute bitcoins via the open supply version of Bitcoin peer-to-peer software.

Ewesproposed by using a nameless entitys Satoshi Nakamoto [67]. The Bitcoin gadget uses the blockchain as its distributed public ledger, which facts and verifies all Bitcoin transactions on the open peer-to-peer Bitcoin community system. An extremely good innovation of the Bitcoin blockchain is its capability to prevent double spending on Bitcoin transactions negotiated on a fully decentralized peer-to-peer community, without dependence change relied-on exchange authority.

The blockchain is a decentralized and transparent digital ledger that securely records and verifies transactions across multiple computers or nodes. It was first introduced with the invention of Bitcoin, but its potential extends far beyond just cryptocurrencies. Think of the blockchain as a chain of blocks, where each block contains a list of transactions. These transactions are added to the blocks sequentially and permanently. Every time a new transaction occurs, it is verified by multiple nodes in the network, and once validated, it is added to a new block [68]. The blockchain's distinctive feature is its decentralized nature. Instead of relying on a central authority like a bank or government, the blockchain operates on a peer-to-peer network. This means that anyone can participate in the network and help validate transactions, ensuring transparency and security. By using cryptographic techniques, the blockchain ensures that transactions are tamper-proof and cannot be altered once they are

recorded. This makes it particularly useful for applications that require trust, such as financial transactions, supply chain management, voting systems, and more. Overall, the blockchain brings together the benefits of transparency, security, and decentralization potential to revolutionize various industries, enabling new forms of collaboration and innovation.

2.1 Working mechanisms of the Blockchain

1. Distributed Ledger: At its core, the blockchain functions as a decentralized and distributed ledger. A ledger is simply a record of transactions. In the case of the blockchain, this ledger is maintained by multiple participants, known as nodes, located all around the world. 2. Transaction Validation: When a new transaction is initiated, it is broadcast to the network of nodes. These nodes collectively validate the transaction using consensus algorithms, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). This validation ensures that the transaction is legitimate and follows the rules of the blockchain network. 3. Block Formation: Validated transactions are grouped into a block. Each block [68] typically contains multiple transactions, along with a unique identifier called a hash. The hash of each block is derived from the data within the block, and it also includes the hash of the previous block. This creates a chain of blocks, hence the term "blockchain." 4. Block Mining: Some blockchain networks, like Bitcoin, use a mining process to add new blocks to the chain. Miners compete to solve complex mathematical puzzles, and the first miner to solve the puzzle gets the opportunity to add the next block to the chain. This process adds security to the network and incentivizes miners with rewards, like cryptocurrency. 5. Consensus Mechanisms:

Consensus mechanisms determine how agreement is reached among the nodes on the validity of transactions and the order in which they are added to the blockchain. Different blockchain networks use various consensus mechanisms, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or other consensus algorithms. 6. Immutable and Transparent: Once a block is added to the blockchain, it becomes immutable, meaning it cannot be altered or deleted. This immutability ensures the integrity of the data. Additionally, the blockchain's transparency allows anyone to view and audit the transactions recorded on the network. 7. Smart Contracts: Many blockchains support the execution of smart contracts. These are self-executing contracts with predefined conditions and rules. Smart contracts eliminate the need for intermediaries and enable automated and secure transactions based on predetermined conditions. These are just the basic concepts behind blockchain functionality. The technology has evolved and continues to be explored for various use cases, offering tremendous potential in terms of transparency, security, efficiency, and trust in digital transactions.

3 Security and Privacy properties of Block Chain Technology

First, we analyze the security requirements of online transactions, each of these requirements targets a type of known vulnerability. Next, we describe basic (and inherent) security blockchain properties based on its first implementation in Bitcoin and present the set of additional important security and privacy properties of blockchain, which are present in some existing or desired blockchain systems by many blockchain applications.

3.1 Security and Privacy Requirements of Online Transactions

Broadly speaking, we classify the security and privacy requirements for online transactions into the following seven types

3.1.1 Consistency of the ledger across institutions.

In conciliation, compensation, and settlement between financial institutions, because the architecture and business processes vary from different financial institutions and the involvement of manual processes, not only leads to high transaction fees generated by the client but the business side of financial institutions but is also prone to errors and inconsistencies between ledgers held maintained by different financial institutions.

3.1.2 *Transaction Integrity.* whilst using on-line transactions for investments and asset control, you control shares, bonds, notes, profits statements, warehouse receipts, and other belongings by means of different intermediaries. No longer best does it boom transaction prices, but it additionally contains the chance of deliberately falsify or falsify certificates. consequently, the gadget should assure the integrity of transactions and save you transactions from being manipulated.

3.1.3 *System and information Availability.* Users of online structures ought to be able to get admission to transaction statistics anytime, everywhere. Availability right here refers to each system stage and transaction level. At the system level, the system ought to perform reliably even in the case of a network assault. At the transaction level, transaction records may be accessed by way of legal human's users without being unreachable, inconsistent or corrupt.

3.1.4 *Prevention of double-spending.* An important challenge in digital forex in a decentralized network is how to keep away from double spending, that is, spending one coin extra than as soon as. Inside the centralized surroundings, a depended on valuable third celebration is accountable for verifying whether a digital currency has been spent twice or now not.

For transactions finished in some decentralized community surroundings, we need sturdy safety mechanisms and countermeasures to save you double-spending.

3.1.5 *Confidentiality of Transactions.* In maximum online economic transactions, users want to have minimum disclosure of their transactions and account records at an internet service provider gadget. Minimal disclosure consists of the subsequent: (1) user transaction statistics cannot be accessed through any unauthorized user; (2) the device administrator or network player might not disclose any user's facts to others without her permission; (3) all user's data have to be stored and accessed constantly and securely, even inside the occasion of surprising screw ups or malicious cyber-attacks. This confidentiality is ideal in many non-financial settings.

3.1.6 *Anonymity of the identity of customers.* The issue of effectively and securely sharing user information among more than one economic establishment can bring about a high cost of repeated consumer authentication. He is additionally indirectly carries the risk of disclosure of customers' identities by using a few intermediaries. moreover, one or each event in the transaction can be reluctant to expose their real identification to the alternative party in a few instances.

3.1.7 *Unlinking of Transactions.* Different from identity anonymity (not revealing one's actual identification), users need to demand that transactions associated with them cannot be connected. Once all applicable transactions for a consumer may be linked, it is simple to deduce other information approximately of the user, which includes the account balance and the sort and frequency of their transactions. the usage of such statistical statistics approximately transactions and accounts along with some background expertise a person, curious or hostile parties can guess (infer) the user's proper identification with high confidence.

3.2 Basic Security Properties

The simple security residences of blockchain come from each advance in cryptography and Bitcoin. Layout and implementation. Theoretically, the first at ease blockchain was formulated using cryptography in 1991 [49]. An offer to improve the efficiency of the cryptographic chain of blocks was proposed in

1993 [14] incorporating Merkle trees and placing more than one documents in a block. The blockchain is constructed to ensure several inherent protection attributes, which include consistency, tamper resistance, to a dispensed denial of service (DDoS) attack, pseudonym, and resistance to double-spending attack. But, to use blockchain correctly distributed storage, extra security and privacy houses are required.

Table 1. Summarization of Security and Privacy Requirements, Properties, and Techniques:

	S&P requirements	S&P properties	Corresponding S&P techniques
Support in Bitcoin	Consistency (3.1.1) Integrity (3.1.2) Availability (3.1.3) Prevention of double-spending (3.1.4) Anonymity (3.1.6)	Consistency (3.1.2) Temper-resistance (3.2.2) Resistance to DDoS attacks (3.2.3) Resistance double-spending attacks (3.2.4) Pseudonymity (3.2.6)	Consensus algorithms (2.1) Hash chained storage (2.1) Consensus algorithms with Byzantine faults (4) Signature and Verification (2.1) Public key as pseudonyms (2. 1)
Need to be enhanced	Unlike ability (3.1.7) Confidentiality (3.1.5)	Unlike ability (3.3.1) Confidentiality (3.3.2) Resistance to majority (51%) Consensus attack (3.2.5)	Mixing (5.1) anonymous signature (5.2) ABE (4.5) He (5.3), SMPC (5.5), NIZK (5.6), TEE-based solutions (5.8) Consensus algorithm that do not depend On computing power (4)

The set of basic and extra safety and privacy properties that need to be guaranteed to conform the corresponding necessities described in segment.

3.1. At the top we show the set of security and privacy requirements that can be ensured by way of security and privacy homes and the strategies provided inside the unique blockchain gadget, i.e., Bitcoin. Within the lower element, we display the security and privacy necessities and properties that need to be reinforced by means of a few

additional security and privacy residences and techniques. We describe basic security and privacy properties in segment.

3.2 and further residences in segment 3.3. We've got in brief stated the set of primary security and privacy strategies in section 2.1, we can detail some of them in phase 4, and we can commit phase 5 to discuss additional techniques that may be leveraged to in addition improve the security and privacy of blockchains.

3.2.1 Consistency. The concept of consistency inside the context of blockchain as a distributed system worldwide ledger refers to the property that every node has an identical ledger at the same time. The consistency of belongings has sparked a controversial debate. A few argue that Bitcoin systems offer very last consistency [91], that is a susceptible consistency. Others claim that Bitcoin guarantees strong consistency, no longer eventual consistency [84].

Eventual consistency is a consistency version proposed for allotted computing structures seeking out stability between availability and consistency. formally, it ensures that everyone updates to replicas are lazily propagated and any read get right of entry to a statistics object will eventually achieve the remaining updated price if the element does no longer receive new updates [89]. In other words, the final consistency ensures that the data of every entry in each node of the gadget sooner or later will become steady, and hence reaching excessive availability and coffee latency at the danger of returning out-of-date records. with eventual coherence, the time it takes for device nodes to grow to be coherent won't be defined. therefore, statistics ultimately will become consistent manner that (1) it will take time for updates to propagate to different replicas; and (2) if a person reads from a reproduction that is not yet updated (due to the fact that replicas are updated in the end), then there may be some threat of returning obsolete facts [89].

Inside a blockchain network system, the robust consistency model method that each node has an identical ledger at the same time, and at some stage in the time that the dispensed ledger is up to date with new facts, any subsequent read/write requests will need to wait until the dedicate is showed of this replace. In comparison, the eventual consistency version means that the blockchain on every node gadget will become steady ultimately, even though some examine/write requests to the blockchain may additionally return stale information. The important thing task to attaining sturdy consistency is that the fee of overall performance (w.r.t.latency/availability) is too excessive to be

low-priced in all instances. The key challenge for eventual consistency is how to eliminate inconsistency that can be because of old statistics. The blockchain in Bitcoin adopts a consistency model that seeks a better trade-off between strong consistency and eventual consistency to obtain partition tolerance (P) and consistency (C) with deferred availability.

In Bitcoin, transactions are grouped into blocks. while a sending node sends a transaction to the blockchain network, mining nodes will mine it by way of adding it to a block with other unverified transactions and acting an evidence-of-work assignment game. Upon finishing their evidence-of-work challenge, a miner sends their block and proof to the network to request acceptances from other nodes to verify all transactions within the block. The other nodes receive the block by running on generating the next block with the use of the hash of the block general as the previous hash. The miner whose block is contained within the longest chain and who is the first to achieve confirmations (aka blocks are added on the pinnacle of the block, and = 6 using default inside the Bitcoin consensus protocol) is the winner for chaining this transaction on the global allotted ledger. We can see the parameter as a mechanism to provide robust configurable or parameterized consistency in blockchain.

3.2.2 Resistance to Manipulation. Tamper resistance refers to resistance to any kind of intentional manipulation. Manipulation of an entity by using customers or adversaries to get entry to the entity, whether a system, product, or other logical/bodily object. Blockchain's tamper resistance manner that any transaction facts stored in the blockchain cannot be altered throughout and after the process block technology. Mainly, in a Bitcoin system, mining nodes generate new blocks. There are feasible ways to modify the transaction statistics: (1) miners can try to adjust the obtained transaction statistics; (2) an adversary can try to modify the data saved inside the blockchain. We analyze why such manipulation attempts are elegantly prevented way to Bitcoin's blockchain protocols.

For the first form of manipulation, a miner can attempt to exchange the deal with the beneficiary of the transaction to himself. However, such an attempt cannot be successful, because every transaction is compressed with the use of a secure hash characteristic, together with SHA-256, then signed by way of the payer the usage of a comfy signature algorithm, along with ECDSA, on a Bitcoin network; subsequently, the transaction is dispatched to the entire network for verification and approval thru mining. Therefore, multiple miners can get hold of and choose to upload the transaction to mine, that is achieved non-deterministically. If a miner alters any transaction data, others will come across this once they confirm the signature with the public key of the payer, because the miner cannot generate a valid signature on the modified records without the payer's private key. This is assured using the forgery of the comfortable signature algorithm.

3.2.3 Resistance to DDoS attacks. A denial of service (DoS) attack on a host is a form of cyber assault that disrupts hosted net offerings by making the host machine or the network resource on the host unavailable to meant customers. DoS assaults attempt to overload the host device or the host network's useful resource by flooding it with superfluous requests, which therefore stops the achievement of valid services [63]

A DDoS attack refers to a "distributed" DoS assault, that is, the incoming traffic flooding assault. Approximately a victim originates from many disparate assets allotted across the net. In a DDoS the attacker can compromise and use a character's computer to assault any other laptop using exploiting security vulnerabilities or weaknesses. Leveraging a fixed of such commitments computer systems, a DDoS attacker can send big amounts of data to a website hosting internet site or send spam to personal email addresses [63]. This makes it very tough to prevent the attack using virtually blocking off person's assets one at a time. The arms race depends on the tempo of restoration of such compromised nodes versus the achievement rate of compromised compute nodes in the network.

The extreme subject in a DDoS attack is the supply of the blockchain and is related to the query of whether or not a DDoS attacker could make the blockchain unavailable via deleting a partial or entire network. The answer to this question is no, thanks to the fully decentralized system. Construction and maintenance of the blockchain and Bitcoin system, and the consensus protocol for the generation of new blocks and their addition to the blockchain, ensuring that the processing of Blockchain transactions can continue even if multiple blockchain nodes go offline. For a cyber-attacker to succeed in taking blockchain offline, the attacker would have to collect enough Computational resources that compromise overwhelmingly large portions of the blockchain nodes throughout Bitcoin. The larger the Bitcoin network becomes, the harder it is to succeed in such a large-scale DDoS attack.

3.2.4 Resistance to double-spend attacks. The double spending attack in the context of the Bitcoin blockchain refers to a specific problem unique to digital currency transactions (recall Section 3.1). Please note that the double spending attack can be considered as a general security issue. Since digital information can be reproduced relatively easily. Specifically, in the case of transactions that exchange digital tokens, such as electronic currency, there is a risk that the holder may Duplicate the digital token and send multiple identical tokens to multiple recipients. If an inconsistency may be incurred due to duplicate digital token transactions (for example, double spending of the same

Bitcoin token), then the double spending problem becomes a serious security threat.

To prevent double spending, Bitcoin evaluates and verifies the authenticity of each transaction using the transaction records on your blockchain with a consensus protocol. By ensuring that all transactions are included on the blockchain, the consensus protocol allows everyone to publicly verify the transactions in a block before sending the block to the global blockchain, ensuring that the sender of each transaction only spends the bitcoins they rightfully own. Additionally, each

transaction is signed by the sender using a secure digital signature algorithm. He assures that yes if someone fakes the transaction, the verifier can easily detect it. The combination of transactions. Signed with digital signatures and public verification of transactions with majority consensus ensures that the Bitcoin blockchain can be resistant to double spending attacks.

3.2.5 Resistance to majority consensus attack (51%). This attack refers to the risks of cheating in the majority consensus protocol. One of these risks is often called a 51% attack, especially in the context of double-spending. For example, 51% attacks can occur in the presence of malicious miners. For example, if one miner (verification user) controls more than 50% of the computing power to maintain the blockchain, the distributed ledger of all transactions trades a cryptocurrency. Another example of the 51% attack can occur when a group of miners conspire to carry out a conspiracy, for example, regarding the counting of miners' votes for verification. Yeah, a powerful user or a group of colluding users controls the blockchain, then various security systems and Privacy attacks can be launched, such as illegally transferring bitcoins to some target wallets. Reverse genuine transactions as if they never occurred, and so on.

3.2.6 Pseudonymity. The pseudonym refers to a state of disguised identity. In Bitcoin, addresses in the blockchain are hashes of public keys of a node (user) on the network. Users can interact with the system using your public key hash as a pseudo-identity without revealing your real identity name. Therefore, the address that a user uses can be seen as a pseudo-identity. We can consider the pseudonym of a system as a privacy property to protect a user's real name. Furthermore, users you can generate as many key pairs (multiple addresses) as they want, similar to what a person can do. Create multiple bank accounts as you wish. Although the pseudonym can achieve a weak form of anonymity through public keys, there are still risks of revealing the identity information of users.

4 Consensus Algorithms

Consensus algorithms play a crucial role in blockchain networks as they determine how agreement is reached among the participating nodes. Here are a few common consensus algorithms:

1. Proof-of-Work (PoW): This consensus algorithm is famously used by Bitcoin. Miners compete to solve complex mathematical puzzles, requiring significant computational power. The first miner to solve the puzzle gets the right to add the next block to the chain and is rewarded with cryptocurrency. PoW ensures security by making it computationally expensive to alter the blockchain.

2. Proof-of-Stake (PoS): PoS is an alternative to PoW. Instead of miners competing based on computational power, validators are chosen to create new blocks based on their stake or ownership of cryptocurrency. Validators are selected at random, usually in proportion to the amount of cryptocurrency they hold. PoS consumes less energy compared to PoW and is often considered more environmentally friendly.

3. Delegated Proof-of-Stake (DPoS): DPoS is a variation of PoS that introduces a voting process. Token holders elect a limited number of delegates who are responsible for validating transactions and creating new blocks. These delegates take turns to propose and validate blocks, reducing the number of participants involved in the consensus process. DPoS is known for its scalability and faster transaction confirmation times.

4. Byzantine Fault Tolerance (BFT): BFT-based consensus algorithms aim to provide consensus even in the presence of malicious or faulty nodes. They rely on a certain percentage of nodes (often referred to as "validators" or "replicas") agreeing on the order and validity of transactions. Some popular BFT-based algorithms include Practical Byzantine Fault Tolerance (PBFT) and Tendermint.

5. Proof-of-Authority (PoA): PoA is a consensus mechanism where a limited number of trusted validators (often called "authorities" or "validators") are pre-approved to create new blocks and validate transactions. Validators are typically known entities, such as reputable organizations or individuals. PoA is considered efficient and suitable for private or consortium blockchains.

These are just a few examples of consensus algorithms used in blockchain networks. Each algorithm has its own advantages, trade-offs, and specific use cases. The choice of consensus algorithm depends on factors like network goals, desired level of decentralization, security requirements, scalability, and energy efficiency considerations.

4.1 Proof of Work (PoW)

Proof of Work (PoW) is a consensus algorithm used in blockchain networks to secure the system and prevent malicious activities. Here's how PoW works in the context of the blockchain security system: 1. Computational Puzzle: In a PoW-based blockchain, miners compete to solve a computational puzzle. This puzzle requires significant computational power and involves finding a specific hash value that satisfies certain criteria, such as having a certain number of leading zeros. The difficulty of the puzzle is adjusted to control the rate at which new blocks are added to the chain. 2. Mining Process: Miners in the network continuously perform computations to find the solution to the puzzle. They take the transactions waiting to be added to the block, along with other data like a timestamp, and create a block candidate. 3. Hashing and Validation: Miners repeatedly hash the block candidate by applying cryptographic hash functions. They modify a specific part of the block called the "nonce" to generate different hash outputs. The goal is to find a nonce value that, when hashed with the rest of the block data, produces a hash value that satisfies the specific criteria. This process requires significant computational effort and energy. 4. Difficulty and

Network Consensus: The difficulty of the PoW puzzle is adjusted by the network based on the total computational power (hash rate) of the network. The higher the network's hash rate, the more difficult the puzzle becomes. This adjustment is crucial to maintaining a consistent block creation rate and preventing the blockchain from being overtaken by malicious actors. 5. Block Validation: Once a miner finds a valid solution to the puzzle, they broadcast the solution and the new block to the network. Other miners verify the solution and ensure that all transactions within the block are valid based on the blockchain's rules. Consensus is reached when the majority of miners agree that the block is valid, and it is added to the blockchain. 6. Security Benefits: PoW provides security to the blockchain system in multiple ways. Firstly, it ensures that the majority of participants in the network have invested computational resources to solve the puzzle, making it difficult for any single entity to control the network. Secondly, because finding a valid solution to the puzzle requires significant computational effort, it acts as a deterrent against malicious activities like double-spending or altering past blocks since it would require an immense amount of computational power to rewrite the blockchain's history. Overall, PoW in the blockchain security system helps maintain the integrity of the network, prevents fraud, and ensures that the decentralized nature of the blockchain is preserved.

4.2 Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus algorithm used in blockchain networks to secure the system and maintain the integrity of the blockchain. Let's explore how PoS works in the context of a blockchain security system: 1. Validators and Staking: In a PoS-based blockchain, instead of miners, validators are selected to create new blocks and validate transactions. Validators are chosen based on the number of coins they hold and "stake" in the network. The more coins a validator holds, the higher their chances of being chosen as a validator. 2. Block Validation:

Validators take turns proposing and validating new blocks. When it is their turn, they create a block and include a set of transactions. They also include a "proof" that demonstrates their ownership of a certain amount of coins (their stake). 3. Block Selection: Validators broadcast their proposed block to the network. Other validators then verify the validity of the proposed block and check if the validator has the required stake. Consensus is reached when a certain percentage of validators agree that the proposed block is valid. 4. Chances and Rewards: Validators with a higher stake have a greater chance of being selected to create a new block. This stake-based selection process provides an incentive for validators to act honestly and follow the rules of the network. Validators who successfully create and validate blocks are rewarded with transaction fees or newly minted coins, depending on the blockchain's design. 5. Security Benefits: PoS provides security to the blockchain system in several ways. Since validators are chosen based on their stake, they have an economic interest in maintaining the integrity of the network. The cost of attacking the blockchain by acquiring a majority stake would be economically unviable. Additionally, PoS consumes significantly less energy compared to PoW, making it more environmentally friendly. 6. Fork Resolution: In the event of multiple proposed blocks at the same time, conflicts or forks can occur. Various mechanisms, such as longest-chain selection or weight-based selection, are used to resolve forks in the PoS consensus. Validators will typically choose to extend the longest or heaviest chain based on the underlying rules and protocols. Overall, PoS in a blockchain security system provides a decentralized and efficient approach to consensus. It encourages validators to act honestly, reduces energy consumption, and enhances the overall security of the network.

4.3 BFT-based Consensus Algorithms

Blockchain technology has revolutionized various industries by providing a decentralized and secure platform for transactions and data storage. One of the key components that ensure the integrity and

reliability of blockchain networks is the consensus algorithm. Among the various consensus algorithms available, BFT-based consensus algorithms have gained significant attention.

BFT-based consensus algorithms, short for Byzantine Fault Tolerance-based consensus algorithms, are designed to address the challenges posed by malicious actors or faulty nodes in a decentralized network. These algorithms ensure that the network reaches a consensus on the validity of transactions, even in the presence of these adversarial nodes.

The key idea behind BFT-based consensus algorithms is to require a certain threshold of agreement among a majority of nodes in the network before finalizing a transaction. This threshold can be adjusted based on the desired level of fault tolerance. By utilizing a voting mechanism, BFT-based consensus algorithms enable honest nodes to differentiate between correct and malicious behaviors, ensuring the integrity of the blockchain network.

One popular BFT-based consensus algorithm is the Practical Byzantine Fault Tolerance (PBFT) algorithm. PBFT provides a high degree of fault tolerance by dividing the nodes into three groups: primary, backup, and clients. The primary node proposes a block of transactions, and the backup nodes validate and agree upon the proposed block through a multi-round voting process. Once a consensus is reached, the block is added to the blockchain.

Another well-known BFT-based consensus algorithm is Honey BadgerBFT. This algorithm utilizes a cryptographic protocol to achieve consensus in an asynchronous network. It combines ideas from classical consensus algorithms with cryptographic primitives to ensure both safety and liveness properties.

BFT-based consensus algorithms offer several advantages over other consensus mechanisms. Firstly, they provide a high level of fault tolerance, ensuring the integrity of the blockchain

network even in the presence of malicious nodes. Secondly, they offer low latency and high throughput, making them suitable for applications that require quick transaction confirmations. Additionally, BFT-based consensus algorithms are highly scalable, allowing for the inclusion of more nodes in the network without sacrificing performance.

In conclusion, BFT-based consensus algorithms play a crucial role in ensuring the integrity, fault tolerance, and scalability of blockchain networks. These algorithms provide a robust mechanism for achieving consensus in decentralized environments, making them highly desirable for various blockchain applications. By continually improving and extending BFT-based consensus algorithms, the blockchain industry can further enhance the security and efficiency of blockchain technology.

5. Privacy and Security Techniques Used in Block chain

In this section, we offer a detailed dialogue on a spread of strategies that may be leveraged to beautify the security and privacy of current and destiny blockchain systems.

5.1 Mixing

Mixing in Blockchain technology has revolutionized the security and privacy system, providing a robust and reliable solution for various industries. Blockchain technology, known for its decentralized nature, ensures that data is securely stored and transactions are transparent. By incorporating mixing techniques into this technology, an additional layer of security and privacy is added, making it even more resilient against potential threats.

Mixing in Blockchain refers to the process of obfuscating the transaction history by combining multiple transactions into a single transaction. This technique helps to hide the origin and destination of funds, providing users with increased anonymity. With the integration of

mixing, Blockchain technology becomes an ideal choice for industries that prioritize privacy, such as finance, healthcare, and supply chain management.

5.1.1 Mixcoin. Mixcoin is a revolutionary blockchain technology that aims to enhance privacy and security in the world of digital transactions. Built on a decentralized network, Mixcoin offers a unique and robust solution to the challenges faced by traditional cryptocurrencies. One of the key features of Mixcoin is its advanced mixing technology, which ensures that each transaction is thoroughly obfuscated and untraceable. By combining multiple transactions and shuffling their inputs and outputs, Mixcoin provides users with an unprecedented level of privacy. This groundbreaking approach makes it incredibly difficult for anyone to link transactions to specific individuals or addresses. In addition to its exceptional privacy features.

5.1.2 CoinJoin. CoinJoin is a revolutionary technique in blockchain technology that enhances privacy and security in transactions. It is designed to obscure the link between the sender and receiver, making it difficult to trace the flow of funds. By combining multiple transactions into a single, larger transaction, CoinJoin ensures that the source of funds cannot be easily identified.

With CoinJoin, multiple participants voluntarily combine their transactions into one, thereby creating a pool of inputs and outputs. This pooling of funds makes it challenging to determine which participant initiated a specific transaction, effectively breaking the traceability of transactions on the blockchain.

This technique offers significant benefits in terms of privacy, as it prevents the identification of individual users and their transaction history. It also enhances security by minimizing the risk of targeted attacks or surveillance. Additionally, CoinJoin can help combat the fungibility issue, where certain coins may be blacklisted or stigmatized due to their transaction history.

Implementing CoinJoin on the blockchain requires the collaboration of multiple participants, each contributing their transaction inputs and outputs. These participants can be individuals or services that offer CoinJoin functionality. To ensure fairness and prevent malicious behavior, CoinJoin protocols often rely on cryptography and require participants to follow certain rules during the process. Despite its advantages, CoinJoin does have some limitations.

5.2 Anonymous Signatures

Anonymous signatures are a crucial element in the realm of blockchain technology, contributing to the enhancement of privacy and security in digital transactions. By integrating anonymous signatures into blockchain networks, individuals can maintain their anonymity while securely participating in various transactions and interactions.

The concept of anonymous signatures revolves around the ability to validate and sign transactions without revealing one's true identity. This is achieved by utilizing cryptographic techniques that ensure the authenticity and integrity of the transaction while concealing the identity of the signer. Through the use of advanced encryption algorithms, anonymous signatures allow users to participate in blockchain networks while protecting their personal information.

Firstly, it enables individuals to maintain their privacy and confidentiality, as their true identity remains undisclosed throughout the transaction process. This aspect is especially crucial in scenarios where users wish to conduct business transactions without revealing sensitive information or personal details.

Furthermore, anonymous signatures contribute to the overall security of blockchain networks. By concealing the identity of the signer, potential malicious actors are deterred from targeting specific individuals or their transactions. This enhances the trust and reliability of blockchain technology, as users can confidently engage in

transactions without fear of their personal information being compromised.

Moreover, the use of anonymous signatures promotes inclusivity within blockchain networks. It allows individuals who may be concerned about their privacy to actively participate in digital transactions, eliminating any barriers that may arise from revealing their true identity. With the ability to transact anonymously, blockchain technology becomes more accessible and appealing to a wider range of users.

The integration of anonymous signatures in blockchain technology brings forth significant advantages. It ensures privacy, enhances security, and promotes inclusivity within digital transactions. As technology continues to advance, the importance of anonymous signatures in safeguarding personal information and facilitating secure transactions will only grow, establishing them as a fundamental component of blockchain networks.

5.3 Homomorphic Encryption (HE)

Homomorphic encryption (HE) is an effective cryptography. It could carry out certain varieties of calculations immediately on encrypted text and ensure that operations executed on encrypted statistics, by decoding the calculated effects, it will generate effects equal to those achieved through the equal operations in simple textual content. There are several in part homomorphic cryptosystems [37,71, 77] as well as absolutely homomorphic structures [41, 87].

Homomorphic encryption strategies may be used to store statistics at the blockchain without good sized changes in blockchain properties. This guarantees that the facts on the blockchain be encrypted, addressing privacy concerns related to public blockchains. The use of homomorphic encryption method gives privacy protection and lets in smooth get admission to to encrypted facts through public blockchain for audits and different functions, which include worker fee control. Ethereum smart contracts provide homomorphic

encryption of statistics saved at the blockchain for greater manipulate and privacy.

5.4 Attribute-Based Encryption (ABE)

Attribute-based encryption (ABE) is a cryptographic method in which the attributes are what define and regulation factors for cipher text encrypted using a user's secret key. One can decipher the data encrypted using the user's secret key if its attributes match the attributes of the cipher text. Collusion resistance is an important security property of ABE. Ensures that when a malicious user colludes with other users, cannot access other data except what they can decrypt with your private key. The concept of attribute-based encryption was proposed in 2005 [81] with single authority. From then, a number of extensions to the basic ABE have been proposed, including ABE with multiple authorities to jointly generate users' private keys [26, 52, 60] and ABE schemes that support arbitrary predicates [40, 47]

Attribute-based encryption is very powerful, but to date few applications implement it due to the Lack of understanding of both the basic concepts and their efficient implementation. ABE has not yet been implemented in any form on a blockchain for real-time operation to date. In 2011, a decentralized system the ABE scheme [60] was proposed to employ ABE in a blockchain. For example, in a blockchain, Permissions could be represented by ownership of access tokens. All nodes in the network, which have a certain token issued to them, they will be granted access to special rights and privileges associated with the token. The token provides a means of tracking who has certain attributes and such monitoring must be carried out in an algorithmic and consistent manner by the authority entity that distributes the token. Tokens can be seen as badges that represent attributes or qualifications, and should be used as non-transferable quantifiers of reputation or attributes.

In ref. [60], it is shown that there is no need for a fixed authority to perform attribute-based encryption. It is possible to have multiple

authorities in a decentralized network and comply with the same achievement. For example, it may be possible to rely on witnesses to determine the role of these authorities. On a blockchain, with technologies recently made possible, such as Steemit [7], Storj [93], Inter Planetary File System (IPFS) [15] and Secure Access for Everyone (SAFE) Network [69], although an implementation of attribute-based encryption using a blockchain approach remains an open challenge.

5.5 Secure Multi-Party Computation

The multi-party computing (MPC) model defines a multi-party protocol to allow them to jointly perform some calculations on your private data inputs without violating your input privacy, such that an adversary learns nothing about the entry of an authentic part but rather the exit of the joint calculation.

Andrew Yao officially described secure-party computing in 1982 [94] and generalized it in 1986 [95] for the Millionaire's trouble. Goldreich et al. proposed a generalization of the two-partisan calculus to multiparty calculus in 1987 [45], assuming that all entries in the zero-information computing and proofs are a part of mystery sharing. This generalization has served as the idea for plenty of subsequent and increasingly green MPC protocols. The fulfillment of employing MPC in allotted vote casting, non-public bidding, and personal statistics retrieval has made it a famous method for many real-international issues. The primary huge-scale deployment of MPC turned 2008 into an actual auction problem in Denmark [19].

In current years, MPC has been utilized in blockchain systems to shield personal privacy. Andrychowicz et al. designed and implemented secure multi-celebration calculation protocols within the Bitcoin device in 2014 [10]. They built protocols for secure multiparty lotteries with no reliance on authority. Their protocols can guarantee fairness for honest customers irrespective of how dishonest one behaves. If a consumer violates or interferes with the protocol,

then he will become the loser, and her bitcoins are transported to honest customers.

Zeskind et al. proposed a decentralized SMP computing platform, referred to as Enigma, in 2015. [96]. Using a sophisticated model of SMP computation, Enigma employs a verifiable mystery-sharing scheme to ensure the privacy of its computational version.

Furthermore, Enigma encodings share mystery records of the use of a modified disbursed hash desk for an efficient garage. Moreover, take gain of an external blockchain as a corruption-resistant occasion log and peer-to-peer network regulator for identification management and access management. Similar to the Bitcoin machine, Enigma provides self-reliant control and safety of personal information at the same time as getting rid of the want and dependence on a dependent on the third party.

5.6 Non-Interactive Zero-Knowledge (NIZK) Proof

Every other cryptographic technology that has powerful privacy-maintaining properties is zero-knowledge proof, proposed in the early Nineteen Eighties [46]. The fundamental idea is that a formal proof can be formulated to verify that a program performed with a few entries privately recognized by the user can produce a few publicly open results without revealing any other statistics. In other phrases, a certifier can reveal to a verifier that a few declare is accurate without imparting any beneficial information statistics to the verifier.

As a variant of zero-knowledge proofs, it's shown in Ref. [18] that, with the non-interactive variant of zero-knowledge proofs, coined as NIZK, computational 0-understanding may be performed without requiring the certifier and verifier to have interaction at all, as long as the certifier and verifier stocks a not unusual reference chain. In a blockchain utility, all account balances are encrypted and saved at the chain. when a user transfers money to another user, he can without difficulty show that has sufficient stability for the

switch with zero-knowledge proofs, without disclosing the account balance.

Another version is the zero-knowledge non-interactive succinct know-how argument. (zk-SNARK), supplied in 2012 by way of Bitansky and his co-authors [16] and which serves as a basis spine of the Zcash protocol [82]. Zcash [82] makes use of zk-SNARK [17, 48] to verify transactions at the same time as shielding the privacy of customers.

These days, the Zcash institution stepped forward the Ethereum contract language to correctly offer zk SNARK evidence verification. more particularly, they followed a snark-checking precompile (as an opcode) for a fork of "Parity", which uses lib-snark to test generic tests. in addition, they used the new zk-SNARK verifier for enforcing an authentic coin blending agreement, adopting a simplified model of Zerocash, an academic protocol whose implementation is used to build Zcash. that's what it is called "child" ZoE, which represents Zerocash on Ethereum. The agreement lets the consumer save discrete statistics amounts (units of ETH) by adding a "serial number" as a commitment into a Merkle tree, which is maintained by the contract.

5.7 The Trusted Execution Environment (TEE) Based Smart Contracts

Some execution surroundings are called a TEE if it gives completely isolated surroundings for going for walks packages, efficiently preventing different software program applications and operating systems from controlling and understanding the nation of the utility that runs on it. Intel software guard eXtensions (SGX) is a representative technology for imposing a TEE. As an instance, Ekiden [29] is an SGX-based answer for confidentiality-preserving smart contracts. Ekiden separates computing from consensus. perform clever agreement calculations in TEE on a powered-down compute nodes chain, then use a faraway attestation protocol to validate the correctness of the computation execution nodes inside the chain. Consensus nodes are used to

maintain the blockchain and are no longer required. Use reliable hardware. Enigma [96] makes use of TEE in its modern-day version to allow users to create privacy-maintaining smart contracts with the usage of a decentralized credit scoring algorithm. more than one factors are weighted inside the credit rating, together with the range and varieties of accounts, payment history, and use of credit score.

5.8 Game-based Smart Contracts

The game-based totally solutions for smart contracts verification are very recent trends, represented with the aid of TrueBit [86] and Arbitrum [53].

TrueBit [86] uses an interactive “verification recreation” to determine whether or not a computational undertaking become effectively completed or no longer. TrueBit gives rewards to inspire players to check computation duties and locate insects, such that a smart settlement can securely carry out a computation project with verifiable properties. similarly, in each round of “verification recreation,” the verifier recursively assessments a smaller and smaller subset of the computation, which permits TrueBit to substantially lessen the computational burden on its nodes.

Arbitrum [53] has designed an incentive mechanism for parties to agree off-chain on the behavior of digital machines, in order that it best calls for the verifiers to verify virtual signatures of the contracts. For dishonest parties who attempt to lie approximately the conduct of digital machines, Arbitrum has designed a green undertaking-based protocol to become aware of and penalize the cheating events the inducement mechanism of off-chain verification of digital device’s conduct has significantly progressed the scalability and the privacy of clever contracts.

6. Security and privacy concern of Blockchain Technology

Concern about security and privacy when it comes to blockchain technology. Rest assured,

there are several features and mechanisms in place to address these concerns. First, let's talk about security. One of the key strengths of blockchain is its decentralized nature, which means that the data is stored across multiple computers or nodes. This makes it exceptionally difficult for hackers to tamper with the data because they would need to gain control of the majority of the nodes simultaneously. Additionally, blockchain uses cryptographic algorithms to secure the data. Each transaction is encrypted and linked to the previous transaction, forming a chain of blocks. This makes it extremely challenging to alter any past transactions without the consensus of the network. Now, let's move on to privacy. While it is true that blockchain is transparent and all transactions are visible to network participants, it also offers various levels of privacy depending on the type of blockchain you're dealing with. For example, public blockchains like Bitcoin provide pseudonymity, where transactions are linked to wallet addresses rather than real-world identities. On the other hand, private blockchains can restrict access to authorized participants, providing a higher level of privacy. Furthermore, recent advancements in blockchain technology, such as zero-knowledge proofs and secure multi-party computation, enable even greater privacy while maintaining the integrity of the data. It's important to note that while blockchain technology does offer enhanced security and privacy compared to traditional systems, no technology is completely infallible. It's always recommended to follow best practices, such as keeping your private keys secure and being cautious with the information you share. I hope this helps alleviate some of your concerns

6.1 Main weaknesses of blockchain technology security and privacy

One of the main weaknesses of blockchain technology is the potential for 51% attacks. In a blockchain network, consensus is achieved through a majority of participants agreeing on the validity of transactions. However, if a single entity or group of entities manages to control more than 50% of the network's computing

power, they can manipulate the blockchain and potentially reverse transactions or double-spend coins. This highlights the importance of ensuring a distributed and decentralized network to mitigate the risks associated with 51% attacks.

Another weakness of blockchain technology lies in its vulnerability to smart contract bugs. Smart contracts are self-executing contracts with the terms of the agreement directly written into code and stored on the blockchain. While smart contracts offer automation and transparency, they are not immune to bugs or vulnerabilities. If a flaw exists in the code, it can potentially be exploited, leading to financial losses or privacy breaches. Careful code review and rigorous testing are essential to minimize the risks associated with smart contract vulnerabilities.

Additionally, blockchain technology faces challenges regarding privacy. Contrary to popular belief, blockchains are not inherently anonymous. Public blockchains, such as Bitcoin, have transparent transaction records that anyone can access and analyze. While public blockchains offer transparency and traceability, they may not be suitable for applications that require privacy, such as healthcare or financial services. Efforts are being made to develop privacy-enhancing solutions, such as zero-knowledge proofs and privacy-focused blockchains, to address these concerns.

Furthermore, scalability is a weakness that hampers blockchain technology adoption. Public blockchains typically have limited transaction processing capabilities, which can result in slow transaction speeds and high fees during periods of high demand. This scalability challenge has hindered the widespread adoption of blockchain technology for mainstream applications. Various solutions, such as layer 2 protocols and sharding, are being explored to improve scalability and enable blockchain technology to handle a larger volume of transactions.

While blockchain technology offers significant security and privacy benefits, it is important to acknowledge and address its weaknesses.

By focusing on solutions to mitigate the risks associated with 51% attacks, smart contract vulnerabilities, privacy concerns, and scalability limitations, we can enhance the overall security and privacy of blockchain technology, making it more robust and suitable for various applications.

6.2 Solution of blockchain technology Security and privacy concern

Blockchain technology has revolutionized various industries by providing decentralized and secure solutions. However, 51% attacks remain a concern that can compromise the integrity and security of blockchain networks. In this article, we will explore effective strategies to solve and prevent such attacks, ensuring the continued trust and reliability of blockchain technology.

6.2.1 What is a 51% Attack: A 51% attack, also known as a majority attack, occurs when a single entity or group controls more than 50% of the total hash power in a blockchain network. This control enables them to manipulate transactions, reverse confirmed transactions, or even double-spend funds. Preventing and mitigating these attacks is crucial to maintain the integrity of blockchain systems.

6.2.2 Strengthening Network Consensus Mechanisms: One way to combat 51% attacks is to fortify the consensus mechanisms employed by blockchain networks. For example, proof-of-work (PoW) algorithms can be modified to make it more computationally expensive to acquire a majority of the network's hash power. Additionally, alternative consensus mechanisms such as proof-of-stake (PoS) or delegated proof-of-stake (DPoS) can be explored, where validators are chosen based on their stake or reputation.

6.2.3 Increasing Network Hash Power: To render 51% attacks economically unfeasible, blockchain networks must strive to increase overall hash power. This can be achieved by encouraging more participants to contribute computational resources to the network through mining or staking. Incentives, such as rewards or transaction fee reductions, can be provided to attract more miners or validators to secure the network effectively.

6.2.4 Implementing Consortium or Private Blockchains: In certain use cases where decentralization is not the primary concern, implementing consortium or private blockchains can be an effective strategy. These blockchains restrict participation to a select group of trusted entities, preventing the possibility of a 51% attack. Consortium or private blockchains are particularly suitable for industries like supply chain, healthcare, or finance, where limited participants can maintain the desired level of security and consensus.

6.2.5 Network Monitoring and Detection: Proactive monitoring and detection systems are essential to identify potential 51% attacks early on. Nodes in the network should be continuously monitored to detect any abnormal behavior or sudden increase in hash power distribution. By promptly detecting and responding to such incidents, blockchain network operators can take necessary actions to mitigate the damage caused by attackers.

As blockchain technology continues to evolve, it is vital to address and resolve potential vulnerabilities such as 51% attacks. Through strengthening consensus mechanisms, increasing network hash power, considering alternative blockchain models, and implementing robust monitoring systems, the risk of 51% attacks can be significantly reduced. By adopting these strategies, we can ensure the continued growth and trustworthiness of blockchain technology across various industries.

7 Discussion

To acquire security and privacy in a complex blockchain gadget that desires to meet a couple of security and privacy requirements with preferred properties, we would like to make the following 3 remarks: (1) No single technology is a panacea for the protection and privacy of Blockchain. therefore, the appropriate security and privacy techniques ought to be selected based on the security and privacy requirements and the context of utility. As well known, the mixture of multiple

technologies works more efficiently than the use of an unmarried generation. for example, Enigma [96] combines the slicing aspect cryptographic method SMPC and hardware privacy technology TEE with blockchains to provide computation over encrypted statistics at scale. (2) there's no technology that has no defects or is perfect in all aspects. Whilst we add a brand new technology to a complicated system, it continually causes other troubles or a brand new shape(s) of assaults. This requires careful attention to the pitfalls and ability harms brought about by integrating some protection and privacy techniques into the blockchains (3) there is always a tradeoff between security, privacy, and efficiency. We must the ones recommend.

8 Concluding remarks

We've offered a survey on blockchain security and privacy with numerous contributions. First, we characterize the safety and privacy attributes of blockchain into two broad categories: inherent attributes and further attributes in the context of on line transactions. 2nd, we describe security and privacy techniques to acquire these security and privacy attributes. In blockchain based totally structures and applications, such as representative consensus algorithms, mixing, anonymous signatures, encryption, secure multiparty computing, non-interactive zero-knowledge evidence, and at ease smart agreement verification. With growing interest in blockchain in educational and industry studies, the security and privacy of blockchains have attracted large hobbies, even though only a small part of blockchain platforms can achieve the set of aforementioned protection goals in exercise. We argue that a deep expertise of the security and privacy properties of blockchain performs a vital position in improving the degree of consider that Blockchain can provide and increase technological innovation on sturdy protection strategies and countermeasures. We conjecture that developing lightweight cryptographic algorithms like in addition to different realistic security and privacy strategies will be key to allowing technology inside the destiny improvement of blockchain and its programs.

References



- [1] [n.d.]. Bitcoin—Open source P2P money. Retrieved from <https://bitcoin.org/en>.
- [2] [n.d.].Ethereum Project. Retrieved from <https://www.ethereum.org>.
- [3] [n.d.]. IBM Blockchain based on Hyperledger Fabric from the Linux Foundation. Retrieved from <https://www.ibm.com/blockchain/hyperledger.html>.
- [4] [n.d.]. PlatON. Retrieved from <https://www.platon.network/#/>.
- [5] [n.d.]. Monero. Retrieved from <http://www.getmonero.org>.
- [6] [n.d.]. What is Bit Shares. Retrieved from <http://docs.bitshares.org/bitshares/whatis.html>.
- [7] 2017. Steem: An incentivized, blockchain-based, public content platform.
- [8] 2017. ZooKeeper: A Distributed Coordination Service for Distributed Applications.
- [9] Aigents. 2017. Proof of Reputation as Liquid Democracy for Blockchain.
- [10] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. [n.d.]. Secure multiparty computations on bitcoin. In SP 2014. 443–458.
- [11] Kristov Atlas. [n.d.]. CoinJoin Sudoku: Weaknesses in SharedCoin.
- [12] Kristov Atlas. 2014. Weak Privacy Guarantees for SharedCoin Mixing Service.
- [13] Adam Back. 2002. Hashcash—A denial of service counter- measure. In USENIX Technical Conference.
- [14] Dave Bayer, Stuart Haber, and W. Scott Stornetta. 1993. Improving the Efficiency and Reliability of Digital Time Stamping. 329–334.
- [15] Juan Benet. 2015. IPFS—Content Addressed, Versioned, P2P File System (DRAFT 3).
- [16] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. [n.d.]. From extractable collision resistance to succinct non- interactive arguments of knowledge, and back again. In ITCS 2012. 326–349.
- [17] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Omer Paneth, and Rafail Ostrovsky. [n.d.]. Succinct non-interactive arguments via linear interactive proofs. In TCC 2013. 315–333.
- [18] Manuel Blum, Paul Feldman, and Silvio Micali. [n.d.]. Non-interactive Zero-knowledge and its applications. In STOC 1988. 103–112.
- [19] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P. Jakobsen, Mikkel Krøigaard, JanusDam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. [n.d.]. Securemultiparty computation goes live. In FC 2009. 325–343.
- [20] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. [n.d.]. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In SP 2015. 104–121.
- [21] Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. [n.d.].Mixcoin: Anonymity for Bitcoin with Accountable Mixes. 486–504.
- [22] Daniel R. L. Brown. 2000. The Exact Security of ECDSA. Technical Report. Advances in Elliptic Curve Cryptography.
- [23] Vitalik Buterin. [n.d.]. Ethereum’s White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.
- [24] Rebecca Campbell. 2017. Delaware Passes Groundbreaking Blockchain Regulation Bill.
- [25] Miguel Castro and Barbara Liskov. [n.d.]. Practical byzantine fault tolerance. In OSDI 1999. 173–186.

- [26] Melissa Chase. [n.d.]. Multi-authority Attribute Based Encryption. 515–534.
- [27] David Chaum and Eugène van Heyst. [n.d.]. Group Signatures. 257–265.
- [28] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. On security analysis of proof-of-elapsed time (PoET). In *Stabilization, Safety, and Security of Distributed Systems*. 282–297.
- [29] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song. 2018. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution. CoRR abs/1804.05141 (2018).
- [30] Coindesk. 2017. State of Blockchain - Q4 2017.
- [31] Nxt community. 2014. Nxt Whitepaper.
- [32] Mauro Conti, Sandeep Kumar E., Chhagan Lal, and Sushmita Ruj. 2017. A survey on security and privacy issues of Bitcoin. CoRR bs/1706.00916 (2017).
- [33] Henry Corrigan-Gibbs and Bryan Ford. [n.d.]. Dissent: Accountable Anonymous Group Messaging. 340–350.
- [34] Phil Daian, Rafael Pass, and Elaine Shi. 2016. Snow White: Provably Secure Proofs of Stake. Cryptology ePrint Archive, Report 2016/919.
- [35] Jules DuPont and Anna Cinzia Squicciarini. [n.d.]. Toward De-Anonymizing Bitcoin by mapping users location. In *CODASPY 2015*. 139–141.
- [36] Cynthia Dwork, Moni Naor, and Amit Sahai. [n.d.]. Concurrent zero-knowledge. In *STOC 1998*. 409–418.
- [37] Taher ElGamal. [n.d.]. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. 10–18.
- [38] Fangyu Gai, Baosheng Wang, Wenping Deng, and Wei Peng. 2018. Proof of reputation: A reputation-based consensus protocol for peer-to-peer network. In *Database Systems for Advanced Applications*. 666–681.
- [39] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin backbone protocol: Analysis and applications. In *EUROCRYPT 2015*. 281–310.
- [40] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. [n.d.]. Attribute-Based Encryption for Circuits from Multilinear Maps. 479–499.
- [41] Craig Gentry. [n.d.]. Fully homomorphic encryption using ideal lattices. In *STOC 2009*. 169–178.
- [42] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. Cryptology ePrint Archive, Report 2017/454.
- [43] Seth Gilbert and Nancy Lynch. 2002. Brewer’s conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News* 33, 2 (June 2002), 5–59.
- [44] GoChain. 2018. Proof of Reputation.
- [45] Oded Goldreich, Silvio Micali, and Avi Wigderson. [n.d.]. How to play any mental game or A completeness theorem for protocols with honest majority. In *STOC 1987*. 218–229.
- [46] S. Goldwasser, S. Micali, and C. Rackoff. [n.d.]. The knowledge complexity of interactive proof-systems. In *STOC 1985*. 291–304.
- [47] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. [n.d.]. Attribute-based encryption for circuits. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013)*. 545–554.
- [48] Jens Groth. [n.d.]. Short Pairing-Based Non-interactive Zero-Knowledge Arguments. 321–340.
- [49] Stuart Haber and W. Scott Stornetta. 1991. How to time-stamp a digital document. *J. Cryptology* 3, 2 (1991), 99–111.

- [50] Intel. 2017. Sawtooth Lake. Retrieved from <https://intelledger.github.io/>.
- [51] Don Johnson, Alfred Menezes, and Scott Vanstone. 2001. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* 1, 1 (2001), 36–63.
- [52] T. Jung, X. Y. Li, Z. Wan, and M. Wan. [n.d.]. Privacy preserving cloud data access with multi-authorities. In *INFOCOM2013*. 2625–2633.
- [53] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. [n.d.]. Arbitrum: Scalable, private smart contracts. In *USENIX Security 2018*. 1353–1370.
- [54] Ghassan Karame. [n.d.]. On the security and scalability of Bitcoin’s Blockchain. In *CCS 2016*. 1861–1862.
- [55] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. [n.d.]. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. 357–388.
- [56] Sunny King and Scott Nadal. 2012. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. (2012).
- [57] Protocol Labs. 2017. Filecoin: A Decentralized Storage Network.
- [58] Leslie Lamport. 2016. Paxos made simple. *ACM Sigact News* 32, 4 (2016).
- [59] Leslie Lamport, Robert Shostak, and Marshall Pease. [n.d.]. The byzantine generals problem. *ACM Trans. Program.Lang. Syst.* 4, 3 ([n. d.]), 382–401.
- [60] Allison Lewko and Brent Waters. [n.d.]. Decentralizing attribute-based encryption. In *EUROCRYPT 2011*. 568–588.
- [61] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2017. A survey on the security of blockchain systems. *Future Generation Computer Systems* (2017).
- [62] Gregory Maxwell. 2013. CoinJoin: Bitcoin privacy for the real world. Retrieved from bitcointalk.org.
- [63] Mindi McDowell. 2013. Understanding Denial-of-Service Attacks.
- [64] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. [n.d.]. A fistful of Bitcoins: Characterizing payments among men with no names. In *IMC 2013*. 127–140.
- [65] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. [n.d.]. The honey badger of BFT protocols. In *CCS2016*. 31–42.
- [66] H. Moniz, N. F. Neves, M. Correia, and P. Verissimo. [n.d.]. Experimental comparison of local and shared coin randomized consensus protocols. In *SRDS 2006*. 235–244.
- [67] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. Retrieved from www.bitcoin.org, 9. (2008).
- [68] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.
- [69] SAFE Network. 2018. A SAFE Network Primer—An Introductory guide to the world’s first fully autonomous data network.
- [70] Diego Ongaro and John Ousterhout. [n.d.]. In search of an understandable consensus algorithm. In *USENIX ATC 2014*. 305–320.
- [71] Pascal Paillier. [n.d.]. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT 1999*. 223–238.
- [72] Rafael Pass, Lior Seeman, and Abhi Shelat. [n.d.]. Analysis of the Blockchain Protocol in Asynchronous Networks. 643–673.
- [73] Rafael Pass and Elaine Shi. [n.d.]. FruitChains: A fair Blockchain. In *PODC 2017*. 315–324.
- [74] Rafael Pass and Elaine Shi. 2016. The Sleepy Model of Consensus. *Cryptology ePrint Archive*, Report 2016/918.

- [75] M. Pease, R. Shostak, and L. Lamport. [n.d.]. Reaching agreement in the presence of faults. *J. ACM* 27, 2 ([n. d.]), 228–234.
- [76] Andrea Pinna and Wiebe Rutenberg. 2016. Distributed ledger technologies in securities post-trading.
- [77] R. L. Rivest, A. Shamir, and L. Adleman. [n.d.]. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 2 ([n. d.]), 120–126.
- [78] Ronald L. Rivest, Adi Shamir, and Yael Tauman. [n.d.]. How to Leak a Secret. 552–565.
- [79] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. [n.d.]. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. 345–364.
- [80] Nicolas van Saberhagen, Johannes Meier, Antonio M. Juarez, and Max Jameson. 2012. *CryptoNote Signatures*.
- [81] Amit Sahai and Brent Waters. [n.d.]. Fuzzy Identity-Based Encryption. 457–473.
- [82] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. [n.d.]. Zerocash: Decentralized anonymous payments from Bitcoin. In *SP 2014*. 459–474.
- [83] Emin Gün Sirer. [n.d.]. *Hacking, Distributed*.
- [84] Emin Gün Sirer. 2016. *Bitcoin Guarantees Strong, Not Eventual, Consistency*.
- [85] China Blockchain Technology and Industry Development Forum. 2016. *China Blockchain Technology and Application Development White Paper*.
- [86] Jason Teutsch and Christian Reitwießner. 2017. *TrueBit: A scalable verification solution for blockchains*.
- [87] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. [n.d.]. Fully homomorphic encryption over the integers. In *EUROCRYPT 2010*. 24–43.
- [88] Pavel Vasin. 2018. *BlackCoin’s Proof-of-Stake Protocol v2*.
- [89] Werner Vogels. [n.d.]. Eventually consistent. *Commun. ACM* 52, 1 ([n. d.]), 40–44.
- [90] Mark Walport. 2016. *Distributed ledger technology: Beyond block chain*.
- [91] Roger Wattenhofer. 2016. *The Science of the Blockchain* (1st ed.). CreateSpace Independent Publishing Platform.
- [92] Wikipedia. [n.d.]. Proof-of-authority. Retrieved from <https://en.wikipedia.org/wiki/Proof-of-authority>.
- [93] Shawn Wilkinson, Tome Boshevski, Josh Brandof, James Prestwich, Gordon Hall, Patrick Gerbes, Philip Hutchins, and Chris Pollard. [n.d.]. *Storj: A Peer-to-Peer Cloud Storage Network*.
- [94] A. C. Yao. [n.d.]. Protocols for secure computations. In *SFCS 1982*. 160–164.
- [95] Andrew Chi-Chih Yao. [n.d.]. How to generate and exchange secrets. In *SFCS 1986*. 162–167.
- [96] Guy Zyskind, Oz Nathan, and Alex Pentland. 2015. *Enigma: Decentralized computation platform with guaranteed privacy*. *Comput. Sci.* (2015).
- [97] Christian Decker, Jochen Seidel, and Roger Wattenhofer. 2016. Bitcoin meets strong consistency. In *Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN’16)*. ACM, New York, NY, USA, Article 13, 10 pages.

Author:

	<p>Md Merazul Islam doing his Master’s degree in software engineering. Author hasn’t interest about financial issue about this article.</p>
	<p>Mohammad Abdullah doing his bachelor in Software Engineer, China West Normal University. Nanachong Sichuan Chian, China His primary research interests include artificial intelligence, wireless communication, and computer communions</p>

Access this Article in Online	
	Website: www.ijarm.com
	Subject: Computer Science
Quick Response Code	
DOI: 10.22192/ijamr.2024.11.02.001	

How to cite this article:

Md Merazul Islam, Mohammad Abdullah. (2024). A Survey on Block-Chain Technology Security and Privacy. Int. J. Adv. Multidiscip. Res. 11(2): 1-23.
DOI: <http://dx.doi.org/10.22192/ijamr.2024.12.02.001>