Article

The Role of Cryptography and AI in Enhancing Blockchain Security

Sivamuganthan A/L Mohana Dass , Sai Rama Mahalingam , Phung Li Hang , Kelvin Kelvin , Jerry Wingsky , Abdelrahman Mahmoud Mohamed Afifi Mohamed , Almero Jozelle Rebecca , Nur Iman Yusuf Bin Aili Hatmal , Aishath Raulo Ali , Ertsberg Tjahyosedjati , Tan Wei , Siva Raja Sindiramutty *

Posted Date: 6 January 2025

doi: 10.20944/preprints202501.0386.v1

Keywords: Blockchain Security; Cryptographic Techniques; Decentralized Systems; Consensus Mechanisms; AI and Blockchain

Article

The Role of Cryptography and AI in Enhancing Blockchain Security

Sivamuganthan A/L Mohana Dass, Sai Rama Mahalingam, Phung Li Hang, Kelvin, Jerry Wingsky,Abdelrahman Mahmoud Mohamed Afifi Mohamed, Almero Jozelle Rebecca, Nur Iman Yusuf Bin Aili Hatmal, Aishath Raulo Ali, Ertsberg Tjahyosedjati, Tan Wei, Siva Raja Sindiramutty

sivamuganthan.mohanadass@sd.taylors.edu.my, sairama.mahalingam@sd.taylors.edu.my, phung.lihang@sd.taylors.edu.my, 0363446@sd.taylors.edu.my, 0364627@sd.taylors.edu.my, 0368277@sd.taylors.edu.my, jozellerebecca.almero@sd.taylors.edu.my, 0375484@sd.taylors.edu.my, 0364141@sd.taylors.edu.my, 0366478@sd.taylors.edu.my, tan.wei03@sd.taylors.edu.my, magan.shiva91@gmail.com

Abstract: Blockchain technology has emerged as a very revolutionary tool facilitating secure and transparent digital interactions which is driven by its decentralised structure, cryptographic methods, and consensus protocols. There are a lot of substantial advantages such as improved confidentiality, integrity, and availability of blockchain security. But it also comes with a few drawbacks such as scalability issues, vulnerabilities system and system failures. This study examines the current trend of blockchain technology, its strengths and limitations, and its potential and proposes strategic improvements to enhance its resilience and scalability. The proposed advancement encompasses the integration of artificial intelligence (AI) and machine learning (ML) for real-time threat detection, the adoption of sophisticated cryptographic techniques like Zero-Knowledge Proofs (ZKPs) and quantum-resistant algorithms, as well as the implementation of adaptive consensus mechanisms aimed at optimising resource utilisation. These enhancements are pivotal for overcoming most of the drawbacks in blockchain security and discovering its complete potential. Through ongoing interdisciplinary exploration and innovation, blockchain has a very high potential to revolutionise all industries by providing strong security, enhancing operational efficiency, and ensuring scalability, thus creating secure, reliable, and decentralised digital ecosystems.

Keywords: blockchain security; cryptographic techniques; decentralized systems; consensus mechanisms; AI and blockchain

1. Background Studies

I. Overview of Blockchain

Blockchain is a way to record information while protecting it from hackers who would attempt to manipulate it. Figure 1 shows a basic ideology of how blockchain works. Blockchain works by having an interconnected network of blocks or can also be described as a chain of blocks. Due to its nature as a distributed ledger, blockchain technology will duplicate and distribute transactions to various computers under the network. Each block stores a transaction record made by the user in the network. This method is commonly known as a 'Digital Ledger' because it is stored virtually. Every transaction would be authorised by a digital signature of the owner which enhances its security (A S, 2022).

doi:10.20944/preprints202501.0386.v1

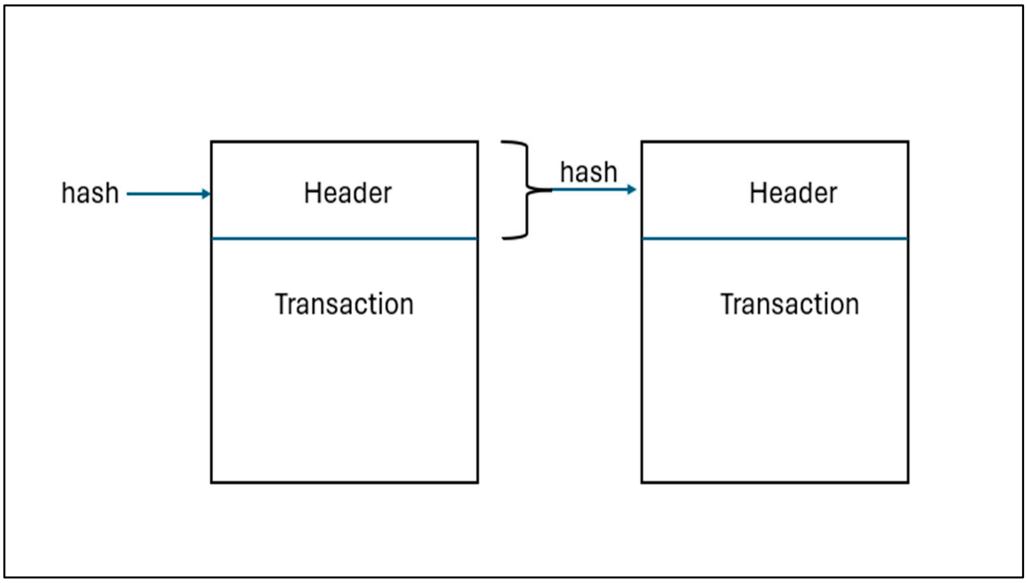

Figure 1. Blockchain Diagram (Sheth and Dattani, 2019).

II. History of Blockchain

Blockchain history begins in the early 1980s. Cryptographer David Chaum introduced an innovative idea in his study (Tripathi, Ahad and Casalino, 2023), which laid the theoretical source of secure digital transactions. The concept was about blind signatures which allowed payments to be automated. With the early concepts, Stuart Haber and W. Scott Stornetta published an article which proposed a cryptographic chain of blocks, designed to prevent users from altering documents through the timestamping method. (Sheldon, 2021)

In 2008, Satoshi Nakamoto anonymously published a thesis called "Bitcoin: A Peer-to-Peer Electronic Cash System". The aim was to create a safe currency like Bitcoin without involving third parties like banks using blockchain infrastructure. The first Bitcoin transaction happened in 2009 when Nakamoto made a transaction of 10 Bitcoins to his friend Hal Finley. This was when the vision of the technology materialised. By the year 2010, the first Bitcoin exchange platform was set up going by the name “Bitcoin Market”. (Tripathi, Ahad and Casalino, 2023)

III. Revolutionary Period

As blockchain gains momentum, its application extends beyond cryptocurrencies. In 2013, Vitalik Buterin introduced Ethereum. It is a platform that uses blockchain technology to allow decentralised applications through smart contracts. With the release of Ethereum in 2015, the potential of blockchain technology increased significantly, enabling developers to create programs on a decentralised platform. In the same year, the Linux Foundation also introduced Hyperledger, a collection of tools to support blockchain development. (Tripathi, Ahad and Casalino, 2023; Ananna et al., 2023).

Blockchain technology started growing in company applications and decentralised finance (DeFi) platforms from the year 2018. Ethereum inspired advancements in DeFi and Non-Fungible Tokens (NFT) which opened doors to brand new industries. Technologies like Hyperledger and R3 Corda were developed to personalise blockchain solutions. By the year 2020, blockchain has set itself as an innovative technology with uses in various fields such as supply chain management, healthcare and banking.

2. Types of Blockchain

I. Permissionless Blockchain

The best example of a permissionless blockchain is Bitcoin. There is no obstruction to whichever user can access it. This means any user in the network can create a cryptocurrency mining tool. This type of blockchain is also known as public blockchain. This is the reason that distributed ledger technology (DLT) has become popular in recent years.

II. Permissioned Blockchain

This type of blockchain can also be known as private blockchain. It operates on a closed network while also working well for private companies. These companies can use private blockchains to customise their accessibility preferences or any other security factors. Due to being a closed network, only one authority is able to manage a private blockchain network.

III. Consortium Blockchain

This type of blockchain combines characteristics of both public and private blockchains. The only difference between this blockchain and the others is that this type is usually handled by multiple organisations. Consortium blockchain provides more security but with the cost of a more difficult initial set-up.

3. How Blockchain Security Works

I. Components

Creating a system for working in blockchains involves working with many interdependent components and their interaction through data transfer. A blockchain network is analogous to a bustling city, with nodes serving as sentries, securing and sharing transactions recorded in a decentralised ledger. Consensus mechanisms maintain harmony, cryptography protects data, and smart contracts automate procedures. Peer-to-peer networks allow for direct connection, while hashing ensures data integrity, resulting in a secure and efficient environment (GeeksforGeeks, 2021; Azam, Dulloo, Majeed, Wan, Xin, & Sindiramutty, 2023). Combining these elements leads to a secure, transparent, and efficient ecosystem.

II. Nodes

Nodes are separate computers with the hardware that make up the Blockchain Network. Depending on their role, there are three types of nodes. The workhorses of the network, full nodes hold an entire copy of the blockchain and thoroughly verify and process transactions. Partial nodes also known as light nodes, the network’s lightweight helpers, by contrast, only save a fraction of transactions, eliminating the need for all those disk storage and computational resources. Mining nodes which secure the network validate transactions and write them onto the chain through a process called mining. Figure 2 shows types of nodes in blockchain.

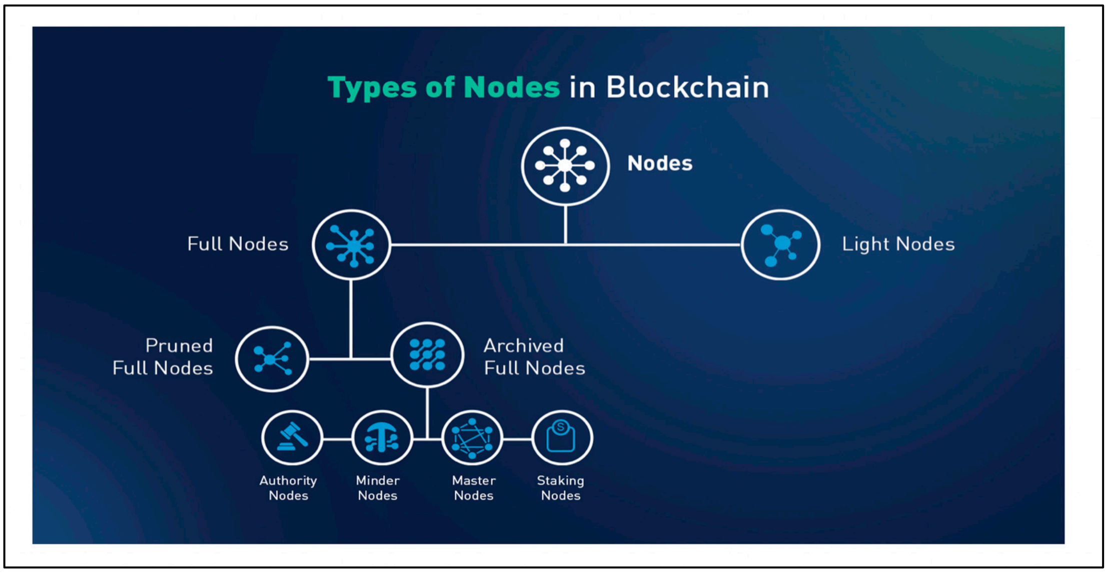

Figure 2. Type of Nodes in Blockchain (Team, 2024).

III. Ledgers

The blockchain is a sort of shared, digital notebook that has a record of every single transaction and other changes made that cannot be altered or lost. It is composed of pages (blocks) connected as a chain, and each page contains some entries (transactions) and a timestamp. This distributed notebook is managed by a network of nodes that need to collaborate to verify and log the transactions. It's a public digital notebook into which anyone can read or write; distributed, in that every computer holds a copy; and decentralized, in that no single computer has control, providing fairness and removing single points of failure (GeeksforGeeks, 2021; Azam, Dulloo, Majeed, Wan, Xin, Tajwar, et al., 2023).

IV. Transactions

Besides that, the transactions are the most primitive of blockchain build blocks. Transactions are formed, approved by parties on the network, and subsequently written to the blockchain permanently. This contains information such as the sender and receiver, the transaction amount, and a digital signature to confirm its validity (GeeksforGeeks, 2021; Azam, Tajwar, Mayhialagan, Davis, Yik, Ali, et al., 2023). Blockchain uses cryptography to secure its records. Participants use private keys which are unique to them to sign each transaction, which acts as a digital signature. Any change to a record would cause the signature to be incorrect and raise an immediate alarm to the rest of the network. Such a system of timely notification is critical for limiting damage (LCX Team, 2024).

V. Consensus mechanisms

Proof of Work (POW) is a consensus mechanism that forces participants to solve complex computational puzzles to validate transactions, and in turn, it gives newly minted tokens to the successful solvers. (GeeksforGeeks, 2021; Azam, Tan, Pin, Syahmi, Qian, Jingyan, et al., 2023) As shown in Figure 3, with an increasing number of miners on the blockchain network, the energy consumption required to process these calculations also increases. This bootstrapping fashion increases complexity which begs the question of high energy consumption and possible wasted computational resources. A significant risk is a 51% attack in which a malicious user could acquire control over more than half of the network's computing power to corrupt the blockchain. (ImmuneBytes, 2020)

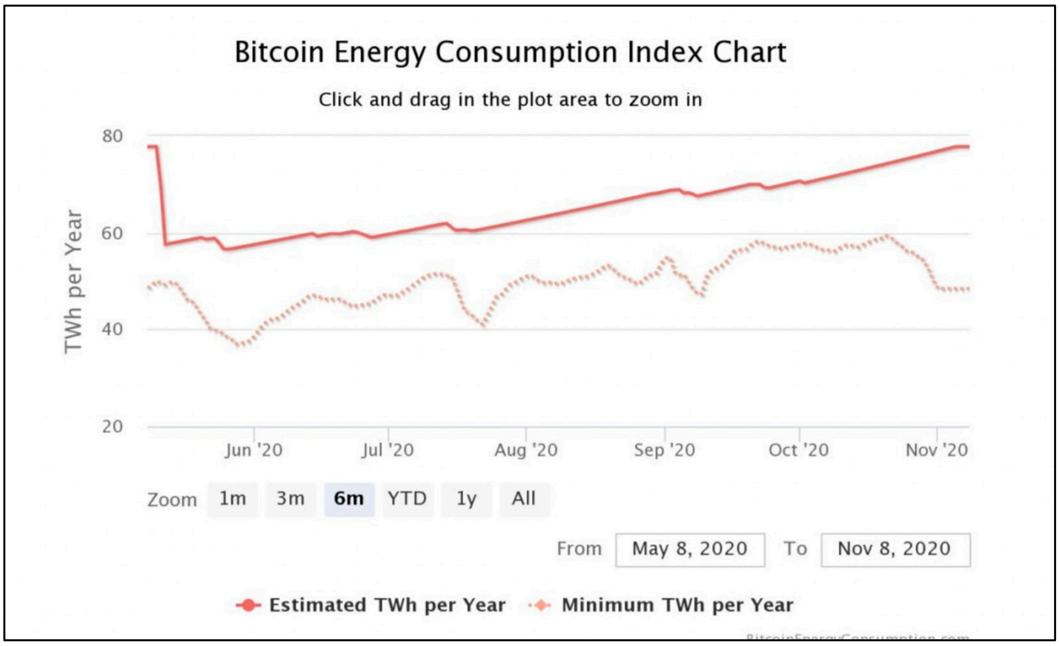

Figure 3. Bitcoin energy consumption index chart (ImmuneBytes, 2020).

VI. Peer-to-Peer Network

Blockchain's decentralized architecture is established on peer-to-peer (P2P) communication, allowing participants to communicate directly and conduct transactions without the need for intermediaries. The nodes connected in a P2P network interact, conduct transactions, and keep records in a clear, unalterable, and non-counterfeitable way. Such a decentralized approach improves security, resistance to attacks and censorship resistance. P2P networks are classified into three types: structured P2P, which provides efficient data access but requires complex setup; unstructured P2P, which provides flexibility but is less efficient with large amounts of data; and hybrid P2P, which combines central node guidance with decentralised interactions (Vietnam blockchain. Asia,n.d; Hussain et al., 2024).

VII. Process of Blockchain

The process begins with a user who requests a new transaction on the blockchain network. This includes using one's digital wallet to transfer, for instance, cryptocurrency to another or status updates on the blockchain ledger. All the information that needs to be transmitted is doubly encrypted using public and private keys (Ujjawal, 2024). This commonly exists in Bitcoin as the transaction is secured by using public-private key encryption. Figure 4 shows the process of blockchain.

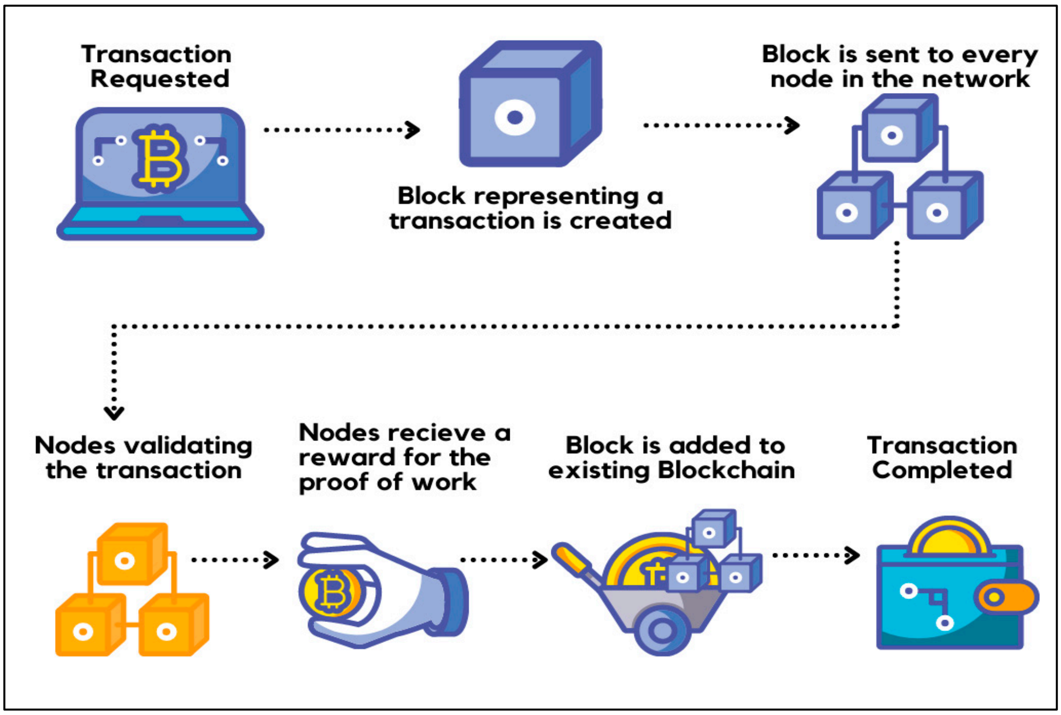
Transaction Requested
Block representing a transaction is created
Block is sent to every node in the network
Nodes validating the transaction
Nodes recieve a reward for the proof of work
Block is added to existing Blockchain
Transaction Completed

Figure 4. The process of Blockchain (Tagade, 2021).

Once requested, a block is created in the blockchain network which then will be used for storing the data of the transaction. The block contains a header and data that refers to the transaction, including its details and timestamp. The block's timestamp is used to help create an alphanumeric string called "hash" (Pratt, 2023; Jun et al., 2024). These are a cryptographic-generated codec which can be referred to as a digital fingerprint. It's also involved in the linking of blocks as new blocks are created from the previous block's hash code providing an arrangement in chronological sequence as well as the checksum to ensure that the record has not been altered. Any tampering with these codes produces an entirely different string of random characters and participants can easily identify misfit blocks (Becher, 2024).

The block then will be sent to all of the nodes in the peer-to-peer network. All changes in the network result in most nodes having to verify and work on new data based on permissions or incentives. This is what is known as consensus mechanisms. The consensus mechanism used in blockchain networks is Proof of Work (PoW). In PoW, nodes, which are also known as miners, will attempt to solve a complex mathematical puzzle and give out a solution. It requires computational power and whoever solves the puzzle as soon as possible will mine the next block. (GeeksforGeeks, 2019; Manchuri et al., 2024). When a consensus is reached, a new block of transaction details is added to the chain and updated to match the blockchain ledger (McKinsey & Company, 2022). The node that is selected to add a block to the blockchain will get a reward to prove the legitimacy of a transaction receiving an economic incentive. This process is called "mining" (Ujjawal, 2024).

After the block has got its hash and is also authenticated, it is now ready to be added to the blockchain. This will be sent across all nodes in the network so each node will have an up-to-date copy of the blockchain. Once it's been added, it can be referenced further in subsequent blocks, but it can't be changed since the transaction has been made, and the details of the transactions are now immutable (Pratt, 2023). Blockchains operate in one way and once a certain operation is called then there can be no undoing it. It is an alteration that is vital in part because it gives transparency across the network and a reliable record of every transaction on the blockchain (Becher, 2024; Ravichandran et al., 2024).

4. Threats to Blockhain

As Blockchain holds countless important things such as users and transaction data, it is predictable that cyber criminals hold a huge interest in making it one of their attack targets. To be able to disrupt the Blockchain is to gain authority over all the content in it. Theft, scams and ransom are the most common desires for the hackers. Numerous techniques of cyber-attacks will be launched to threaten the security of Blockchain and here are some of the most famous examples.

I. Phishing attacks

Phishing attacks are a common cyber-attack that happen across the wireless network realm. This means that it also happens to blockchain since wireless platforms are used. In general, phishing is a technique where an impersonation method is implemented to confuse victims leading to leakage of personal information such as username and password. The various ways of doing this are sending fake emails and or suspicious website links to trap victims which is often called email phishing. The other type is spear phishing where an attacker masquerades himself as a trusted personality by gathering all necessary information on an individual. After that, people with close relationships with the individual will willingly provide anything asked by the attacker unconsciously (Ibm, 2024b; Seng et al., 2024). Figure 5 shows what is phishing attack.

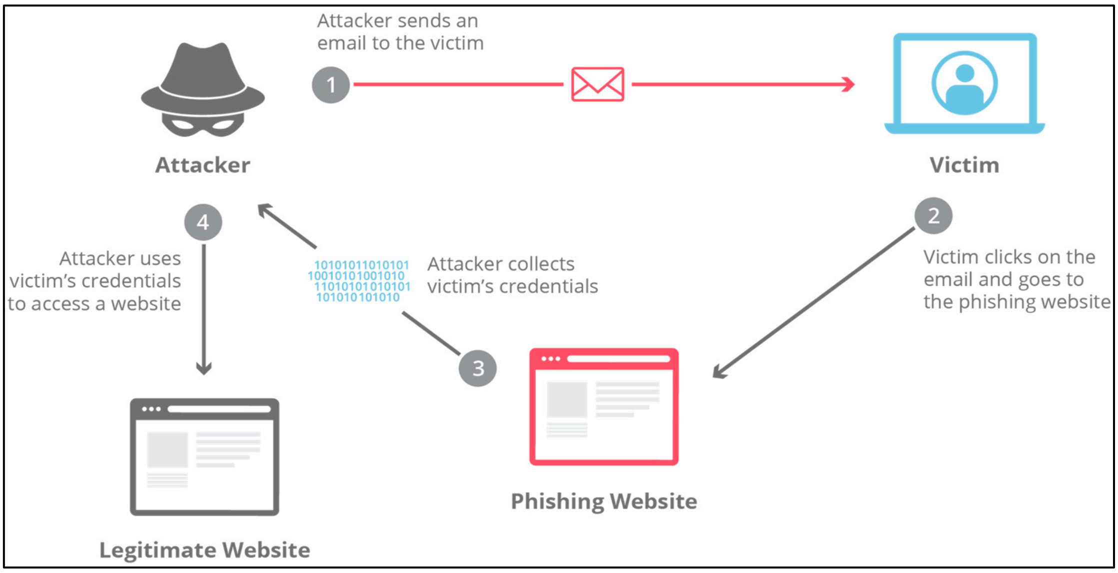
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

Figure 5. What is a phishing attack (Cloudflare, 2023).

This same method will be utilised in Blockchain to uncover the victim's credentials. It doesn't matter what type of phishing is used; the goal will remain the same which is to uncover sensitive information. This is very dangerous, especially with the rise of Bitcoin usage, an account that falls into the hands of criminals will cause a huge and unrecoverable loss for an individual. It will also give a wider opening for follow-up cyber-attacks such as ransomware making the overall environment feel less safe.

II. Routing attacks

Routing attacks operate by manipulating the path between networks from different routers. The attackers will position themselves in between the normal route or redirect the route to different destinations during the transfer of data, giving them an opening to exploit, intercept or disrupt the information and process. This will result in a decline in performance and unauthorised access to personal details (Sindiramutty et al., 2024). The most famous example of this attack is Man in The Middle and Denial of Service. In Blockchain, there are inside chain and outside chain node communication. During the exchange of data between the two nodes, attackers intercept the information by locating themselves in the middle of the route. The exchanged data then will be eavesdropped or worse manipulated without both sides knowing. The most common cases are when a successful transaction was redeemed unsuccessful (Ledger, 2024).

III. Sybil attacks

In Blockchain, transactions and the creation of blocks are authenticated by a mechanism called Proof-of-Stake (PoS). It is an upgrade from the Proof-of-Work (PoW) mechanism by providing more energy-efficient maintenance in the network. The way this method works is that someone called "stalker" will be chosen to do the validations and block creations. To be a stalker, the sum of cryptocurrencies becomes an important factor. Some of the total cryptocurrencies owned will be locked in the network, the higher the amount, the higher the chances of being selected as a stake (Sindiramutty, Jhanjhi, Tan, Khan, Shah, & Manchuri, 2024). After speakers were appointed, a proposal for block transactions was initiated. If voted by other speakers as the majority, then it will be part of the Blockchain. However, it can be a double-edged sword as it comes with both advantages and disadvantages. Successful block validation will be rewarded and failing means losing the staked cryptocurrencies (Starknet, 2024).

Sybil attack is one of the special attacks focusing on decentralised networks. It works indirectly by creating several fake identities to overwhelm the network with fake users. Later then, the fake account will be all controlled by the attackers to exert influence over the network. Direct methods also exist by initiating communication with honest nodes to obey their malicious plan (Chainlink, n.d.). With most accounts at hand, the voting system becomes unreliable as votes can be cast by the fake account. Feedback and ratings will also be bombed to tarnish certain reputations. As a result, the legit block of transactions got out-voted and trust among others declined (Imperva, 2023).

IV. 51% attacks

51% of attacks are an attack that happens when a singular unit or organisation achieves more than 50% control over a network. The amount of power gained can give authority to an attacker to alter some important things in a Blockchain. The usual victims of this attack are Blockchains with low computational power as it is easier to be overpowered. Launching an attack on higher powered Blockchain could cost a lot, from hardware and electricity to stake tokens, depending on the system used, either Proof of Work (PoW) or Proof of Stake (PoS). After successfully overpowering a network, several operations can be executed. One of them is double spending where the same coin is being used repeatedly as attackers can reverse their transactions. Transaction censorship can also occur as attackers can manipulate targeted or every latest transaction validation (Investopedia, 2024; Sindiramutty, Jhanjhi, Tan, Khan, Shah, Yun, et al., 2024).

5. Examples of Blockchain Security

I. Bitcoin Blockchain

Bitcoin is widely regarded as the first and the largest cryptocurrency with a decentralised peer-to-peer network. It is a virtual type of cash that people may use to buy or sell goods from shops that accept bitcoins. The process of maintaining the decentralised public ledger is called Mining. This is accomplished by utilising highly advanced computers that can solve complex computer math problems (Tripathi, 2021; Sindiramutty et al., 2024). Transactions are verified by public nodes and subsequently added to publicly distributed ledgers by minors, who are rewarded with new bitcoins for their work. The transactions are all stored in the bitcoin network which makes it impossible to manipulate or even to hack the network as it is stored on multiple computers due to bitcoin being decentralised (Anwar *et al.*, 2020).

II. Ethereum Blockchain

Ethereum is a global software platform that allows developers to create and deploy decentralised applications - which implies that it is not run by a centralised authority - and it is powered by blockchain technology. Ethereum features include Smart Contracts, Ether, Ethereum Virtual Machine, Decentralised Applications (DApps) and Decentralised Autonomous Organisations (DAO). Ether - or ETH - is simply Ethereum cryptocurrency. This runs the network and aids the system in building DApps, smart contracts, and making peer-to-peer payments. Smart contracts are computer programs allowed in Ethereum that facilitate the exchange of any assets between two parties. This is due to the Ethereum Virtual Machine which allows the interaction with smart contracts by providing the architecture and the software needed. DApps allow the developers to build decentralised applications while DAOs allow the creation of these for democratic making (Kelley, 2024).

Ethereum uses blockchain security, which stores information in blocks containing data encoded from the previous block and the new information. This results in an encoded chain of information that cannot be changed. In Ethereum, the ether is assigned to the validator's address, and each block is built with new ether tokens provided to the validator for the work required to validate the information stored in one block while proposing a new one. The proposed new block will then be validated by a network of automated programs that reach a consensus on the transaction information validity after data and hash have been passed between the consensus and the execution layer. An appropriate number of validators must demonstrate that they had the same comparative results before the block is finalised (Frankenfield, 2021; Sindiramutty, Tan, Shah, et al., 2024).

III. Hyperledger Fabric for Healthcare

Hyperledger Fabric is a permissioned blockchain framework, where all network participants must have known identities (IBM, 2023). Since the healthcare environment requires the distribution of different levels of control accessible to different types of users, permissioned frameworks such as hyper ledger fabric are suitable for Electronic Health Records (EHR). It provides scalability, storage and sharing, improves decision-making for medical care and reduces the cost overall (Uddin et al., 2021; Sindiramutty, Tan, & Wei, 2024). Additionally, Hyperledger fabric provides capabilities such as the use of identity management which allows the usage of user authentication and authorization, and private channels which are restricted messaging paths that provide confidentiality and privacy for transactions (Antwi et al., 2021). The network is made up of different peer nodes with each peer node being either an endorser or a committer node, as well as an ordering service component that accepts endorsed transactions from the client, organises them into groups of blocks with ordering peers' cryptographic signatures and broadcasts the blocks to committing peers within the network for validation against endorsement policies (Uddin et al, 2021; Waheed et al., 2024). Figure 6 shows the benefits of Blockchain Hyperledger fabric.

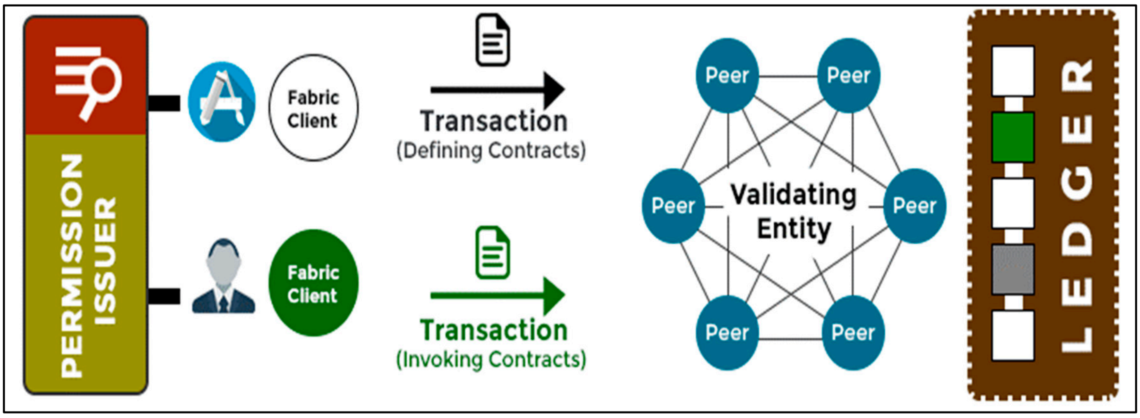

Figure 6. Benefits of Blockchain Hyperledger Fabric (Tarasenko, 2023).

6. Impact of Blockchain Security

I. Benefits of Blockchain Security

Blockchain security ensures the application of the CIA triad (Confidentiality, Integrity, and Availability) within a blockchain network. The utilization of decentralized architecture, cryptographic techniques, and consensus mechanisms ensures the security of data and transactions. Its architecture eliminates the risks of cyber-attacks and single points of failure. It ensures the authority to prevent any unauthorized access. These features make blockchain a robust solution for securing digital ecosystems.

II. Decentralized Architecture

Third parties in the traditional centralized systems can modify the data privately affecting the data security. Unlike traditional centralized systems, blockchain's decentralized system eliminates the need for third parties. In a blockchain network, there is no single controlling entity or central device; instead, each device functions as a node with equal rights and responsibilities. Each node has a backup in case the data gets tampered then it will fail in the global network's consistency checks (Zeng *et al*., 2020; Wen et al., 2023). Figure 7 shows security features of the blockchain technology.

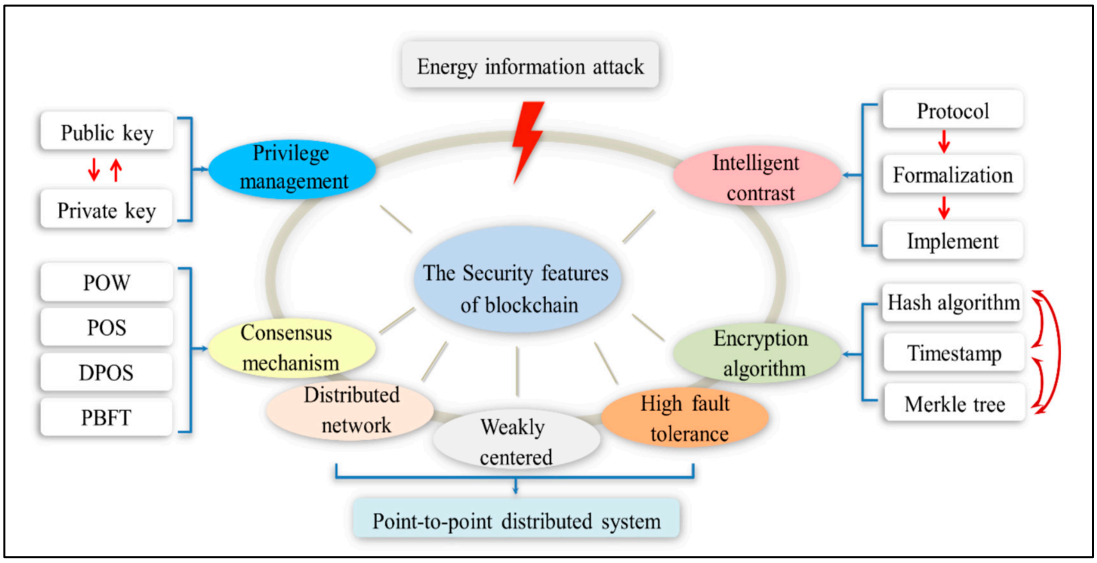

Figure 7. Security features of the blockchain technology (Zeng et al., 2020).

III. Cryptography and Consensus Mechanisms

Blockchain technology ensures security and data integrity using cryptographic algorithms and consensus mechanisms. Cryptographic techniques, such as public-key cryptography, are employed to encrypt data and create digital signatures, thereby maintaining confidentiality and authenticity. Only users with the appropriate private keys can access or validate the data. Furthermore, consensus mechanisms, including Proof of Work (PoW) and Proof of Stake (PoS), manage the process of adding new blocks to the blockchain, preventing unauthorized modifications and ensuring the integrity of the network. These components work together to enhance the overall reliability and security of blockchain systems (Cherian, 2024).

IV. Smart contracts

Smart contracts are self-executing programs where the terms and conditions of an agreement are written directly into code. These contracts automatically enforce and execute the agreed-upon actions when specific conditions are met, without the need for intermediaries. This automation reduces the risk of errors and fraud by ensuring that the contract operates exactly as intended, improving efficiency and reliability in transactions (Ram and Verma, 2024).

7. Limitations of Blockchain Security

I. Scalability

Scalability is a significant challenge for blockchain technology as it requires the processing of multiple transactions at once. As more people use blockchain, the number of transactions increases, which can slow down transaction processing. The ability to manage a large number of users at a single time is still a challenge for the blockchain industry. Blockchain technology involves several complex algorithms to process a single transaction, and as more people become used to it, the average transactions have also increased dramatically. This severely impacts the processing speed of transactions as more computers write and access the network, creating an overall cumbersome system. First, the system throughput of blockchain is very limited. It can only handle small volumes of transactions. For example, the Bitcoin blockchain can only process 7 transactions per second which is considered slow (CrCroman K, Decker C.2016; Alex et al., 2022). While VISA's credit card platform can process about 2000 transactions per second, PayPal's payment platform can process 170 transactions per second (Albrecht S., Reichert S., Schmid J., Strüker J., Neumann D., Fridgen G.2018; Alferidah & Jhanjhi, 2020). In short, existing blockchain systems may not be suitable for high-volume applications.

II. System Failures

Human error is a very common means of system failure. This applies to blockchain technology too. The blockchain can be a database and every block can be considered a storage container. However, the data that enters the blockchain network is fed by humans. This data needs to be of good quality as there is no practical mechanism that monitors the quality of data that is being transmitted in a blockchain network. The data stored in a blockchain is not inherently trustworthy and can contaminate the data of the entire network. Manual errors can lead to outdated log information or create mismatching data while entering the database. In the context of blockchain technology, there are not many developers with specialized expertise in blockchain technology, which is a hindrance to developing anything on the blockchain (Sharma, S., Rosmin, P. and Bhagat, A. 2021; Alkinani et al., 2021).

8. Future Potentials

The future of blockchain technology has huge potential, thus allowing a system to process multiple transactions and reducing transaction time. It is also supposed to protect blockchain networks by preventing malicious attackers through high-security mechanisms, making sure data is accessible and safe. As blockchain continues to grow, it will be imperative to consider cyber threats while protecting this system's integrity. Following are the future trends in Blockchain Security (Technologies, 2024; Aimasterclass.com, 2024; TEAM, 2023).

I. Integration of AI and ML

Using Artificial Intelligence and Machine Learning in blockchain security can make security measures more effective and detect threats. It mitigates security vulnerabilities, avoids compromising sensitive data, and lowers the risk of failure. AI and ML can assist system security in identifying patterns, behaviours, activities, or anomalies in blockchain networks, hence improving the system response to the problem and resilience against potential threats (Technologies, 2024; Cherian, 2024; Aimasterclass.com, 2024; Babbar et al., 2021). Furthermore, numerous healthcare companies employ blockchain security to securely store patient data. AI and ML can identify any breaches; by leveraging this, blockchain provides strong privacy and security (Wissen, 2024; Brohi et al., 2020).

II. Improve Cybersecurity

Security provided by blockchain helps in improving cybersecurity by providing strong protection for sensitive data. This protects security on one hand and guarantees data privacy due to reduced risk against hacker attacks (Cherian, 2024; TEAM, 2023). An example of a cybersecurity activity that blockchain security helps mitigate is Phishing (IBM, 2021; Chesti et al., 2020). Blockchain improves cybersecurity such as Decentralised Identity Management (DID). This innovative approach can create and manage their own identities and can minimize the information to share with whom. It can reduce the risk of phishing whereas DID can hide or eliminate our passwords for safety purposes when opening an email. By using DID, users have full access to control their data which hackers can't access due to strong security (McCann, 2024; www.dock.io, 2024; Dogra et al., 2021). Hence, blockchain has a very positive impact on cybersecurity.

III. Improve Interoperability

Interoperability in blockchain refers to the ability of different blockchain networks to communicate and exchange data with each other. The future potential of interoperability becomes

doi:10.20944/preprints202501.0386.v1

even more important for organizations or individuals as it improves and achieves the potential of decentralized networks. Additionally, it also makes blockchain security more compatible with one another and reduces the cost of blockchain management for both organizations (@coinbase, 2024) (Henry and Pawczuk, 2021; Fatima-Tuz-Zahra et al., 2020).

Cosmos is a blockchain interoperability that allows blockchain security to share data or any transaction with other organizations with ease without worrying about hackers or breaches during that process. Additionally, it increases security and privacy in the process, so no fraud is happening. Interoperability plays a key role in driving efficiency and security (Pittamand, 2022; Gopi et al., 2021) (Cosmos Network, n.d.) (Henry and Pawczuk, 2021). This improves blockchain security for future trends. Figure 8 shows cosmos blockchain.

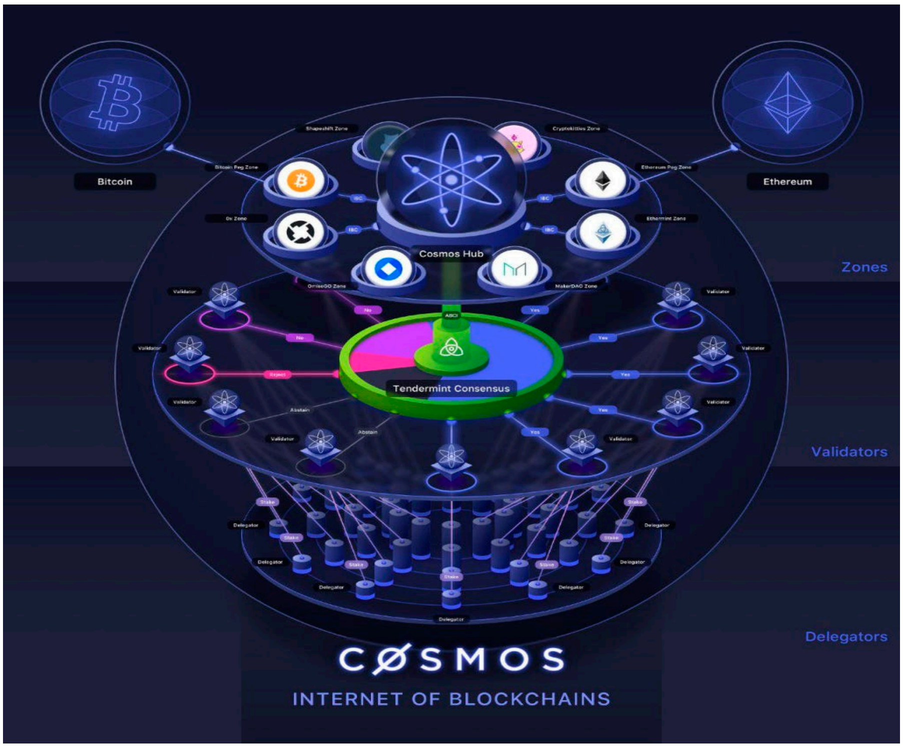

Figure 8. Cosmos Blockchain (Koh, 2018).

IV. Decentralized File Storage

In blockchain security, traditional file storage is prone to data breaches. It's easily hacked by hackers because the files are stored in a single location. So, when the file is compromised, all sensitive data in that storage can be stolen. Hence, blockchain is decentralized to reduce the risks by encrypting and distributing the data across the network (Gouda et al., 2022). So even though the file storage is being hacked, the data remains secure due to encryption that disallows the hacker to access the file and private data can only be accessed by authorized users. This method enhances data privacy, ensuring that private data remains accessible only to authorized users, even during the transmission (McCann, 2024; Delwiche et al., 2023). Hence, making it a key innovation for future trends in blockchain security. An example is BitTorrent. BitTorrent is the most popular decentralized data storage network. It is designed to reduce storage costs and improve the capability of a system to deliver to one another. Usually, users use BitTorrent to transfer files and store files inside the storage because it enables users to remove any illegal or copyrighted media inside the systems.

9. Security Measures

I. Existing Security Measures

Despite being secure through design, blockchain technology still faces constant challenges as it continues to advance progressively and enter various industries. To address these challenges, current security measures have been used to maintain the integrity, confidentiality and availability of blockchain technology. These measures are made to keep data safe from unauthorised access, ensuring that transactions and records are reliable, while maintaining a secure system.

II. Cryptographic Hashing

A cryptographic hash function is a mathematical algorithm that takes data and creates a fixed-size hash. This hash will act as a unique digital identifier for the original input, ensuring the integrity and authenticity of data without showing the original information (Investopedia, 2024). An example of cryptographic hashing would be the SHA-256 (Secure Hash Algorithm) hash function, which takes any text and converts it to an alphanumeric string of 256 bits (Lepcha, 2023; Humayun et al., 2022). SHA-256 has been used in various applications such as digital signatures to verify the integrity and authenticity of digital documents. It is also used for SSL/TLS (Secure Sockets Layer/Transport Layer Security) to secure web communications, as well as password hashing. But most importantly; blockchain technology - to secure transactions and the integrity of the technology (White, 2024). Figure 9 shows SHA 256 process diagram.

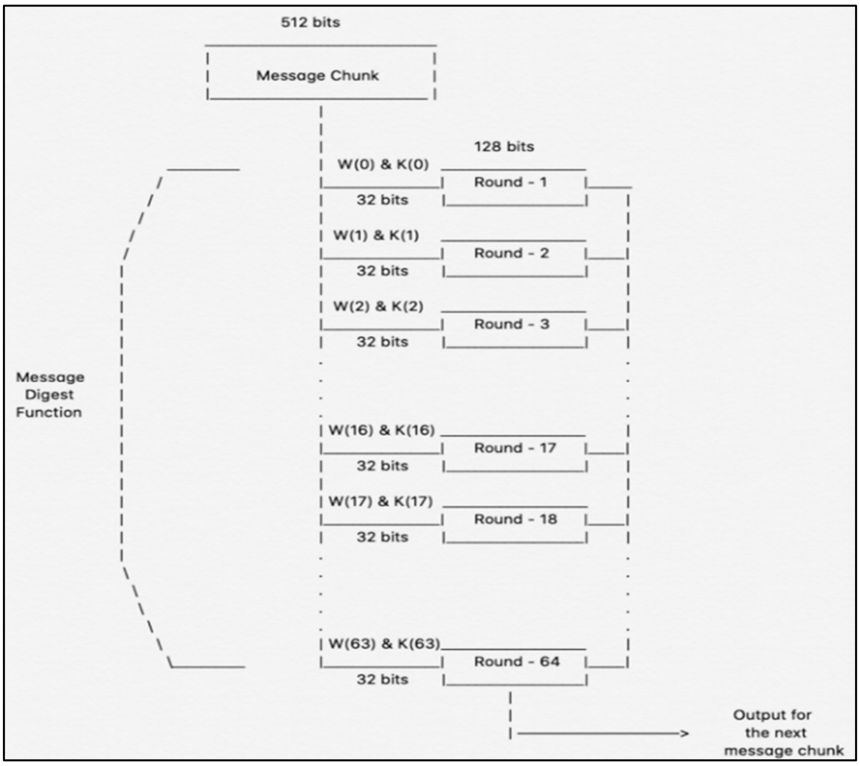

Figure 9. SHA-256 Process Diagram (Jena, 2024).

III. Decentralisation

By distributing data storage and validation among a network of independent nodes rather than relying on a central authority, decentralisation in blockchain technology strengthens security. This avoids having single points of failure as each node keeps a full copy of the ledger, thus making it hard to change authorised data without being detected. In addition, trust is placed in the network's collective validation rather than a central authority, which results in reducing tampering risk while ensuring data integrity (LCX Team, 2024; Jhanjhi et al., 2021). Decentralization utilises mechanisms such as a Transparent Peer - - Peer Network, which promotes transparency and trust by allowing individual nodes to effectively validate transactions in real-time. Furthermore, a transaction is nearly impossible to change once it has been added to the blockchain, thus offering a high degree of security due to the consensus mechanism that requires the agreement of most nodes before any changes are made (Tamplin, 2023).

IV. Public-Key Cryptography (PKC)

Public-key cryptography (PKC) secures blockchain technology by allowing the encryption of transactions with users' public keys and verifying them with private keys. This procedure ensures that only authorised receivers can access transaction data and ensures authenticity through digital signature, preventing unauthorised access and maintaining data integrity across the network (Cryptopedia, 2022). The keys generated are large prime numbers that are mathematically related to one another. With, any data that has been encrypted by the public key can only be decrypted with a private key (Preveil, 2024; Kumar et al., 2021). PKC technology offers several advantages such as how it ensures that the data it receives matches with what the sender has initially sent as well as verifying the sender's identity. This procedure ensures security as it can verify confidentiality, authenticity and integrity when data exchange takes place (Preveil, 2024).

V. Proof Of Work (PoW)

Proof of Work (PoW) helps secure transactions as well as achieving decentralisation by making 'miners', network participants, to solve complex mathematical problems. The process involves validating transactions and generating a unique 'hash' for each block, linking it to the previous block thus forming a secure chain of data. Altering a block in any way would require calculations for all blocks, which can be a difficult process, thus securing the system from any form of tampering Nevil (2024). PoW's procedure first begins with nodes in a blockchain network, where it verifies new transactions to ensure that they are valid. For example, the nodes will verify that the sender has enough balance and that the funds are not being sent to multiple receivers. Once this process has been verified, these transactions are later grouped into a block that needs to be added to the blockchain (Bitcoin Store, 2022; Lim et al., 2019).

To add a block to the blockchain, the miners in the network must solve a complex cryptographic problem. This procedure requires a large amount of computational effort, and miners need to compete with one another to find the solution first. Once a miner has solved the problem, the solution will be shared with other miners to confirm its accuracy before adding the block to the blockchain, which cannot be altered (Bitcoin Store, 2022).

VI. Smart Contracts

Smart Contracts eliminate the need to rely on a central authority, like decentralization as previously mentioned. However, it aims to automate the execution of agreements between different parties. To verify that transactions are carried out automatically and cannot be changed once they have been executed, these self-executing programs have been programmed to initiate particular actions when preset conditions are met. By providing a clear and unchangeable method of enforcing agreements, Smart Contracts as a security measure lowers the risk of fraud and disputes (Investopedia Team, 2024; Nayyar et al., 2021).

The Smart Contracts procedure contains numerous steps, starting with the terms and conditions for the transaction that are first established by an agreement between parties. It includes whether the contract will run automatically and the conditions in which it will be carried out. The agreed terms are then converted into code to create the Smart Contract, which describes the guidelines and penalties, like a legal contract. However, it is important to ensure that the contract is secure as it can no longer be changed or terminated. The contract then monitors for predetermined conditions or triggers, which can be digitally verified, such as the completion of a payment or certain dates (Garnett, 2024).

10. Proposed Security Measures

Blockchain technology's current security features, like cryptographic hashing, decentralization, public-key cryptography, Proof of Work (PoW), and smart contracts, provide a great deal of protection, but as the technology develops and expands across industries, new security features are

doi:10.20944/preprints202501.0386.v1

needed to handle new threats. The security of blockchain systems can be further improved by using the new security methods we suggest below.

I. Proofs of Zero-Knowledge (ZKPs)

Cryptographic procedures known as Zero-Knowledge Proofs (ZKPs) enable one party to demonstrate to another that they are aware of a piece of information without actually disclosing it. By protecting user privacy and reducing the quantity of sensitive data transferred around the network, ZKPs can significantly enhance blockchain security. ZKPs can be used in blockchain technology to verify transactions without exposing the specifics of the transaction. For example, ZKPs make sure the transaction is legitimate without revealing private information, such as the sums being transferred or the identities of the parties. This improves privacy and confidentiality while maintaining data integrity and transaction validity (Simplilearn, 2009; Science Direct, 2024).

II. AI-Powered Threat Detection

As blockchain networks develop in dimensions, so does the possibility of cyberattacks and nefarious actions. AI-powered threat detection systems can detect and prevent security breaches by monitoring blockchain activity for unusual behaviours or vulnerabilities. Machine learning algorithms may be trained to look for trends in blockchain transactions and identify potential risks including double-spending, Sybil attacks, and abnormal transaction volumes (Shah et al., 2022). These AI algorithms can function in real-time, detecting any unexpected behaviour and allowing blockchain administrators to respond swiftly to avert damage. AI might also be used to improve consensus protocols, uncover network weaknesses, and automate responses to security attacks (www.techtarget.com, n.d.).

III. Adaptive Consensus Mechanisms

Current consensus systems, such as Proof of Work (PoW) and Proof of Stake (PoS), enable decentralized validation but are either resource-intensive or vulnerable to certain sorts of attacks (for example, 51% assaults in PoW). Adaptive consensus techniques provide a more dynamic approach to validation by modifying consensus criteria in response to network circumstances and the kind of transaction being processed. An adaptive consensus system, for example, may include PoW, PoS, and Practical Byzantine Fault Tolerance (PBFT), switching between them based on transaction size, complexity, and urgency (Yaga et al., 2018; Sharma et al., 2021). This method saves energy when high processing power is not required, and it improves security by offering more effective protection against specific assaults.

IV. Layered Security Architecture

A layered security architecture that incorporates multiple layers of protection to protect data and transactions can be advantageous for blockchain networks. This method offers a defence-in-depth strategy against possible assaults by integrating current security features like access control, authentication, and encryption at various system levels (Satpal Singh Kushwaha et al., 2022; Singhal et al., 2020). Each layer would be made to safeguard facets of the blockchain, like network connection, user identification, and data integrity. One layer might, for instance, concentrate on encrypting transaction data, while another might put multi-factor authentication into place to grant access to blockchain nodes.

11. Conclusion

Blockchain security can be identified as a game changer because it provides exceptional security through decentralised architecture, cryptographic protocols, and consensus mechanisms. There is no doubt that blockchain is a very reliable foundation for securing and safeguarding digital transactions. It also increases the transparency in transactions by ensuring data confidentiality, integrity, and availability. Our key findings highlight blockchain security's capacity to eliminate single points of failure, restrict unauthorised data access, and enable automated, tamper-proof procedures using smart contracts. However, there are a few obstacles, particularly in terms of scalability, interoperability, and human-related vulnerabilities. Blockchain networks have limited transaction throughput, lagging centralised systems such as VISA. In addition, the quality of data input and the technical skills necessary to construct blockchain solutions are ongoing problems.

Future Improvement Suggestions

As there are a few limitations and drawbacks mentioned, there are a few steps that can be taken to improve blockchain security. Scalability is one of the most significant challenges for blockchain technology. Advanced consensus methods such as adaptive protocols can increase resource allocation and efficiency. Besides that, the combination of artificial intelligence and machine learning can also transform blockchain security to the next level. These technologies enable anomaly detection and real-time threat monitoring, which improves system reliability. They can also help to identify flaws and react to new dangers, strengthening blockchain's resilience to advanced cyber threats such as Sybil attacks and double-spending.

Moreover, Zero-Knowledge Proofs (ZKPs) can improve privacy by allowing transactions to be confirmed without disclosing sensitive information. This improves data security and maintains secrecy in blockchain networks. Researching quantum-resistant encryption is critical for preparing blockchain systems for future threats posed by quantum computing and assuring long-term stability. Furthermore, Interoperability standards are critical for facilitating seamless communication and data exchange between many blockchain networks. Solutions such as the Cosmos blockchain mentioned in 4.3.3 Improve Interoperability, show how interoperability may improve operational efficiency and lower costs while retaining security. Such frameworks will be critical in increasing blockchain's usefulness across multiple industries.

By addressing these issues, blockchain technology can become a fundamental cornerstone of secure and efficient digital ecosystems. All thanks to its ability to protect data, provide secure communication, and enable creative applications. Blockchain has the highest potential to change most of the existing industries and will improve global digital security through interdisciplinary research and strategic advances.

References

1. @coinbase. (2024a). What is blockchain interoperability? [online] Available at: https://www.coinbase.com/en-gb/learn/crypto-glossary/what-is-blockchain-interoperability.
2. @coinbase. (2024b). What is Delegated Proof of Stake (DPoS)? [online] Available at: https://www.coinbase.com/en-gb/learn/crypto-glossary/what-is-delegated-proof-of-stake-dpos.
3. A S, R. (2022). What is Blockchain Technology and How Does It Work? [online] Simplilearn.com. Available at: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology.
4. Aimasterclass.com. (2024). What is Blockchain for AI Security? [online] Available at: https://www.aimasterclass.com/glossary/blockchain-for-ai-security.
5. Alex, S. A., Jhanjhi, N., Humayun, M., Ibrahim, A. O., & Abulfaraj, A. W. (2022). Deep LSTM Model for Diabetes Prediction with Class Balancing by SMOTE. Electronics, 11(17), 2737. https://doi.org/10.3390/electronics11172737
6. Alexandra, S. (2023). What is Phishing and How to Prevent It? [online] GlobalSign. Available at: https://www.globalsign.com/en/blog/what-is-phishing.
7. Alferidah, D. K., & Jhanjhi, N. (2020). Cybersecurity Impact over Bigdata and IoT Growth. 2020 International Conference on Computational Intelligence (ICCI). https://doi.org/10.1109/icci51257.2020.9247722
8. Alkinani, M. H., Almazroi, A. A., Jhanjhi, N., & Khan, N. A. (2021). 5G and IoT Based Reporting and Accident Detection (RAD) System to Deliver First Aid Box Using Unmanned Aerial Vehicle. Sensors, 21(20), 6905. https://doi.org/10.3390/s21206905

9. Amazon Web Services, Inc. (2022). What is Ethereum? - Ethereum Explained - AWS. [online] Available at: https://aws.amazon.com/web3/what-is-ethereum/.
10. Ananna, F. F., Nowreen, R., Jahwari, S. S. R. A., Costa, E. A., Angeline, L., & Sindiramutty, S. R. (2023). Analysing Influential factors in student academic achievement: Prediction modelling and insight. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.254
11. Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Habib ur Rehman, M. and Kerrache, C.A. (2021). The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications. Blockchain: Research and Applications, 2(1), p.100012. doi:https://doi.org/10.1016/j.bcra.2021.100012.
12. Anwar, S., Anayat, S., Butt, S., Butt, S. and Saad, M. (2020). Generation Analysis of Blockchain Technology: Bitcoin and Ethereum. International Journal of Information Engineering and Electronic Business, 12(4), pp.30–39. doi:https://doi.org/10.5815/ijieeb.2020.04.04.
13. Appinventiv.com. (2024). Available at: https://appinventiv.com/wp-content/uploads/2023/03/How-blockchain-resolves-data-privacy-and-security-issues-for-businesses-04.webp.
14. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.255
15. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., Tajwar, M. A., & Sindiramutty, S. R. (2023). Defending the digital Frontier: IDPS and the battle against Cyber threat. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.253
16. Azam, H., Tajwar, M. A., Mayhialagan, S., Davis, A. J., Yik, C. J., Ali, D., & Sindiramutty, S. R. (2023). Innovations in Security: A study of cloud Computing and IoT. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.252
17. Azam, H., Tan, M., Pin, L. T., Syahmi, M. A., Qian, A. L. W., Jingyan, H., Uddin, M. F., & Sindiramutty, S. R. (2023). Wireless Technology Security and Privacy: A Comprehensive Study. Preprints.org. https://doi.org/10.20944/preprints202311.0664.v1
18. Babbar, H., Rani, S., Masud, M., Verma, S., Anand, D., & Jhanjhi, N. (2021). Load balancing algorithm for migrating switches in software-defined vehicular networks. Computers, Materials & Continua/Computers, Materials & Continua (Print), 67(1), 1301–1316. https://doi.org/10.32604/cmc.2021.014627
19. Becher, B. (2024). What Is Blockchain Technology? How Does Blockchain Work? | Built In. [online] Builtin.com. Available at: https://builtin.com/blockchain.
20. Berlove, O. (2021). What are public and private key pairs and how do they work. [online] PreVeil. Available at: https://www.preveil.com/blog/public-and-private-key/.
21. Bitcoin Store. (n.d.). What is Proof-of-Work? The definition, features, and benefits. [online] Available at: https://www.bitstore.net/en/blog/what-is-proof-of-work/.
22. Brohi, S. N., Jhanjhi, N., Brohi, N. N., & Brohi, M. N. (2020). Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19.pdf. TECHRxiv. https://doi.org/10.36227/techrxiv.12115596.v1
23. CEPF®, T.T., BSc (n.d.). Decentralization in Blockchain | Definition, How It Works. [online] Finance Strategists. Available at: https://www.financestrategists.com/wealth-management/blockchain/decentralization-in-blockchain/.
24. Chainlink (2024). What Is a Sybil Attack? [online] Chain.link. Available at: https://chain.link/education-hub/sybil-attack.

25. Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. (2020). Evolution, Mitigation, and Prevention of Ransomware. 2020 2nd International Conference on Computer and Information Sciences (ICCIS). https://doi.org/10.1109/iccis49240.2020.9257708
26. CloudFlare (2023). What is a Phishing attack? Cloudflare. [online] Available at: https://www.cloudflare.com/learning/access-management/phishing-attack/.
27. Cointelegraph. (2024). Wormhole Price Today, W to USD Live Price, Market Cap & Chart. [online] Available at: https://cointelegraph.com/learn/articles/stablecoins-101-what-are-crypto-stablecoins-and-how-do-they-work.
28. Cosmos Network. (n.d.). Cosmos Network - Internet of Blockchains. [online] Available at: https://v1.cosmos.network/intro.
29. Delwiche, O. (2023). Blockchain Technology and its Future Implications | OxJournal. [online] www.oxjournal.org. Available at: https://www.oxjournal.org/blockchain-technology-and-its-future-implications/.
30. Dogra, V., Singh, A., Verma, S., Kavita, N., Jhanjhi, N. Z., & Talib, M. N. (2021). Analyzing DistilBERT for Sentiment Classification of Banking Financial News. In Lecture notes in networks and systems (pp. 501–510). https://doi.org/10.1007/978-981-16-3153-5_53
31. Fatima-Tuz-Zahra, N., Jhanjhi, N., Brohi, S. N., Malik, N. A., & Humayun, M. (2020). Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. 2020 2nd International Conference on Computer and Information Sciences (ICCIS). https://doi.org/10.1109/iccis49240.2020.9257607
32. Frankenfield, J. (2019). 51% Attack. [online] Investopedia. Available at: https://www.investopedia.com/terms/1/51-attack.asp.
33. Frankenfield, J. (2021a). Cryptographic hash functions definition. [online] Investopedia. Available at: https://www.investopedia.com/news/cryptographic-hash-functions/.
34. Frankenfield, J. (2021b). Ethereum. [online] Investopedia. Available at: https://www.investopedia.com/terms/e/ethereum.asp.
35. Frankenfield, J. (2021c). What Is Proof of Work (PoW) in Blockchain? [online] Investopedia. Available at: https://www.investopedia.com/terms/p/proof-work.asp.
36. Frankenfield, J. (2023). Smart Contracts. [online] Investopedia. Available at: https://www.investopedia.com/terms/s/smart-contracts.asp.
37. Fueler. (2022). How Does Blockchain Security Work? [online] Available at: https://fueler.io/blog/how-does-blockchain-security-work.
38. Garnett, A.G. (2023). Britannica Money. [online] www.britannica.com. Available at: https://www.britannica.com/money/how-smart-contracts-work.
39. GeeksforGeeks. (2019). Blockchain - Proof of Work (PoW). [online] Available at: https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/.
40. GeeksforGeeks. (2021). Components of Blockchain Network. [online] Available at: https://www.geeksforgeeks.org/components-of-blockchain-network/.
41. GeeksforGeeks. (2022). Blockchain Interoperability. [online] Available at: https://www.geeksforgeeks.org/blockchain-interoperability/.
42. Gemini. (n.d.). Public and Private Keys: What Are They? [online] Available at: https://www.gemini.com/cryptopedia/public-private-keys-cryptography.
43. GmbH, micobo (2018). Technical difference between Ethereum, Hyperledger fabric and R3 Corda. [online] Medium. Available at: https://micobo.medium.com/technical-difference-between-ethereum-hyperledger-fabric-and-r3-corda-5a58d0a6e347.
44. Google Books. (2020). Digital Finance. [online] Available at: https://books.google.com.my/books?hl=en&lr=&id=5W0DEAAAQBAJ&oi=fnd&pg=PR9&dq=tokens+components+for+blockchain+security&ots=dMvo6x2zaW&sig=GsETSDBw9M4DmDG_mdtT4UG8T6A#v=onepage&q=tokens%20components%20for%20blockchain%20security&f=false.

45. Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N. Z., & Luhach, A. K. (2021). Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. Multimedia Tools and Applications, 81(19), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6
46. Gouda, W., Almurafeh, M., Humayun, M., & Jhanjhi, N. Z. (2022). Detection of COVID-19 based on chest x-rays using deep learning. Healthcare, 10(2), 343. https://doi.org/10.3390/healthcare10020343
47. Hameed, T.M. (2022). Study of the Impacts of Block Chain Technology on Private Sector Banks Performance. [online] Available at: https://www.researchgate.net/publication/364715545_Study_of_the_Impacts_of_Block_Chain_Technology_on_Private_Sector_Banks_Performance.
48. Hayes, A. (2024). Blockchain Facts: What Is It, How It Works, and How It Can Be Used. [online] Investopedia. Available at: https://www.investopedia.com/terms/b/blockchain.asp.
49. Hendrickson, L. (2023a). What Are Smart Contracts on the Blockchain? [online] Identity. Available at: https://www.identity.com/what-are-smart-contracts/.
50. Hendrickson, L. (2023b). What Is Hashing (Hash) in Blockchain? [online] Identity. Available at: https://www.identity.com/what-is-hashing-in-blockchain/.
51. Henry, W. and Pawczuk, L. (2021). Blockchain: Ready for business. [online] Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/blockchain-trends.html.
52. Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022). A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma. Healthcare, 10(6), 1058. https://doi.org/10.3390/healthcare10061058
53. Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. a. U., & Sindiramutty, S. R. (2024). Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), 2, 1–8. https://doi.org/10.1109/khi-htc60760.2024.10482197
54. Hyperledger Foundation (2023). Hyperledger Fabric. [online] Lfdecentralizedtrust.org. Available at: https://www.lfdecentralizedtrust.org/projects/fabric.
55. IBM (2021). What is Blockchain Security? [online] IBM. Available at: https://www.ibm.com/topics/blockchain-security.
56. IBM (2023). What is Hyperledger Fabric. [online] www.ibm.com. Available at: https://www.ibm.com/topics/hyperledger.
57. ImmuneBytes (2020). Consensus Mechanisms Explained. [online] ImmuneBytes - Best Smart Contract Auditing | Blockchain Auditing Services. Available at: https://www.immunebytes.com/blog/consensus-mechanisms-explained/.
58. Imperva (n.d.). What Is a Sybil Attack | Examples & Prevention | Imperva. [online] Learning Center. Available at: https://www.imperva.com/learn/application-security/sybil-attack/.
59. Jena, B.K. (2023). What Is SHA-256 Algorithm: How it Works & Applications | Simplilearn. [online] Simplilearn.com. Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm.
60. Jhanjhi, N., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. Computer Systems Science and Engineering, 37(3), 361–380. https://doi.org/10.32604/csse.2021.015206
61. Jun, A. Y. M., Jinu, B. A., Seng, L. K., Maharaiq, M. H. F. B. Z., Khongsuwan, W., Junn, B. T. K., Hao, A. a. W., & Sindiramutty, S. R. (2024). Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions. Preprints.org. https://doi.org/10.20944/preprints202409.1325.v1
62. Kumar, M. S., Vimal, S., Jhanjhi, N., Dhanabalan, S. S., & Alhumyani, H. A. (2021). Blockchain based peer to peer communication in autonomous drone operation. Energy Reports, 7, 7925–7939. https://doi.org/10.1016/j.egyr.2021.08.073

63. Ledger (2019). Blockchain Security & Beyond | Ledger. [online] Ledger. Available at: https://www.ledger.com/blockchain-security-beyond.
64. Ledger. (2024). Routing Attack Meaning | Ledger. [online] Available at: https://www.ledger.com/academy/glossary/routing-attack.
65. Lim, M., Abdullah, A., Jhanjhi, N., Khan, M. K., & Supramaniam, M. (2019). Link Prediction in Time-Evolving Criminal Network with deep Reinforcement learning technique. IEEE Access, 7, 184797–184807. https://doi.org/10.1109/access.2019.2958873
66. Ltd, M.C. (n.d.). Security in Blockchain: The Benefits of Blockchain Security Services | Microminder Cybersecurity | Holistic Cybersecurity Services. [online] Microminder Cybersecurity. Available at: https://www.micromindercs.com/blog/security-in-blockchain-the-benefits-of-block-chain-security-services.
67. Manchuri, A., Kakera, A., Saleh, A., & Raja, S. (2024). pplication of Supervised Machine Learning Models in Biodiesel Production Research - A Short Review. Borneo Journal of Sciences and Technology. https://doi.org/10.35370/bjost.2024.6.1-10
68. Marr, B. (2023). The 5 Biggest Problems With Blockchain Technology Everyone Must Know About. [online] Forbes. Available at: https://www.forbes.com/sites/bernardmarr/2023/04/14/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/.
69. McCann, K. (2024). Top 10 Uses of Blockchain in Cybersecurity. [online] Cybermagazine.com. Available at: https://cybermagazine.com/articles/top-10-blockchain-strategies.
70. McKinsey & Company. (2022). What is blockchain? [online] Available at: https://mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain#/.
71. Medium. (2024). Medium. [online] Available at: https://juliankoh.medium.com/a-deep-look-into-cosmos-the-internet-of-blockchains-af3aa1a97a5 [Accessed 29 Nov. 2024].
72. Merehead. (n.d.). Benefits of Blockchain Hyperledger Fabric. [online] Available at: https://merehead.com/blog/benefits-of-blockchain-hyperledger-fabric/.
73. Microminder Cybersecurity Ltd (2024). Future of Blockchain Cybersecurity: Emerging Trends and Solutions | Microminder Cybersecurity | Holistic Cybersecurity Services. [online] Microminder Cybersecurity. Available at: https://www.micromindercs.com/blog/future-of-block-chain-cybersecurity-emerging-trends-and-solutions.
74. Mitra, M. (2018). 6 Challenges of Blockchain. [online] Mantra Labs. Available at: https://www.mantralabsglobal.com/blog/challenges-of-blockchain/.
75. mpeintner (2024). [New research] How well does SHA256 protect against modern password cracking? [online] Specops Software. Available at: https://specopssoft.com/blog/sha256-hashing-password-cracking/.
76. Nayyar, A., Gadhavi, L., & Zaman, N. (2021). Machine learning in healthcare: review, opportunities and challenges. In Elsevier eBooks (pp. 23–45). https://doi.org/10.1016/b978-0-12-821229-5.00011-2
77. nordlayer.com. (n.d.). Common blockchain security issues and how to prevent them. [online] Available at: https://nordlayer.com/blog/blockchain-security-issues/.
78. OKX (2023). Delegated Proof of Stake (DPoS) Explained. [online] OKX. Available at: https://www.okx.com/learn/delegated-proof-of-stake-explained.
79. Prashant Gangwal (2019). AI and ML Technologies: What They Mean For Federal Agencies. [online] Simplilearn.com. Available at: https://www.simplilearn.com/what-ai-and-ml-technologies-mean-for-federal-agencies-article.
80. Pratt, M.K. (2023). What is blockchain and how does it work? [online] SearchCIO. Available at: https://www.techtarget.com/searchcio/definition/blockchain.
81. Ram, B. and Verma, P. (2024). Application of blockchain technology in data security. IP Indian Journal of Library Science and Information Technology, 9(1), pp.51–55. doi:https://doi.org/10.18231/j.ijlsit.2024.008.
82. Ravichandran, N., Tewaraja, T., Rajasegaran, V., Kumar, S. S., Gunasekar, S. K. L., & Sindiramutty, S. R. (2024). Comprehensive Review Analysis and Countermeasures for

Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. Preprints.org. https://doi.org/10.20944/preprints202409.1369.v1

83. Review on Blockchain Technology : Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications. (2023). Mesopotamian Journal of Cyber Security, pp.73–85. doi:https://doi.org/10.58496/mjcs/2023/012.
84. Sangfor Technologies. (2024). Blockchain Security: Key Concepts, Threats, and Future Trends. [online] Available at: https://www.sangfor.com/glossary/cybersecurity/blockchain-security-key-concepts-threats-and-future-trends.
85. Satpal Singh Kushwaha, Amit Kumar Bairwa, Sandeep Chaurasia, Soni, V. and Shankar, V.G. (2022). Security Measures for Blockchain Technology. CRC Press eBooks, pp.79–94. doi:https://doi.org/10.1201/9781003252009-5.
86. Science Direct (2024). ScienceDirect.com | Science, Health and Medical journals, Full Text Articles and books. [online] Sciencedirect.com. Available at: https://www.sciencedirect.com/.
87. SearchStorage. (n.d.). 7 decentralized data storage networks compared. [online] Available at: https://www.techtarget.com/searchstorage/tip/Comparing-4-decentralized-data-storage-offerings.
88. Seng, Y. J., Cen, T. Y., Raslan, M. a. H. B. M., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., & Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. Preprints.org. https://doi.org/10.20944/preprints202408.2261.v1
89. Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2022). Cybersecurity and blockchain usage in contemporary business. In Advances in information security, privacy, and ethics book series (pp. 49–64). https://doi.org/10.4018/978-1-6684-5284-4.ch003
90. Sharma, R., Singh, A., Kavita, N., Jhanjhi, N. Z., Masud, M., Jaha, E. S., & Verma, S. (2021). Plant disease diagnosis and image classification using deep learning. Computers, Materials & Continua/Computers, Materials & Continua (Print), 71(2), 2125–2140. https://doi.org/10.32604/cmc.2022.020017
91. Sharma, S., Rosmin, P. and Bhagat, A. (2021). Blockchain Technology. Blockchain Applications in IoT Security, pp.140–151. doi:https://doi.org/10.4018/978-1-7998-2414-5.ch009.
92. Sheldon, R. (2021). A timeline and history of blockchain technology. [online] WhatIs.com. Available at: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology.
93. Sheth, H. and Dattani, J. (2019). Overview of Blockchain Technology. Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146. [online] Available at: http://asianssr.org/index.php/ajct/article/view/728.
94. Shoemaker, P. (2024). What Is a Peer-to-Peer (P2P) Network? [online] Identity. Available at: https://www.identity.com/peer-to-peer-network/#What_Are_the_Types_of_Peer-to-Peer_P2P_Networks.
95. Simplilearn (2009). Online Certification Training Courses for Professionals | Simplilearn. [online] Simplilearn.com. Available at: https://www.simplilearn.com/.
96. Simplilearn.com. (n.d.). What is Ethereum: Understanding Its Features and Applications. [online] Available at: https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-ethereum.
97. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., & Manchuri, A. R. (2024). Cybersecurity measures for logistics industry. In Advances in information security, privacy, and ethics book series (pp. 1–58). https://doi.org/10.4018/979-8-3693-3816-2.ch001
98. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., Yun, K. J., Ray, S. K., Jazri, H., & Hussain, M. (2024). Future trends and emerging threats in drone cybersecurity. In Advances in information security, privacy, and ethics book series (pp. 148–195). https://doi.org/10.4018/979-8-3693-0774-8.ch007

99. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Yun, K. J., Manchuri, A. R., Ashraf, H., Murugesan, R. K., Tee, W. J., & Hussain, M. (2024). Data security and privacy concerns in drone operations. In Advances in information security, privacy, and ethics book series (pp. 236–290). https://doi.org/10.4018/979-8-3693-0774-8.ch010
100. Sindiramutty, S. R., Jhanjhi, N., Tan, C. E., Lau, S. P., Muniandy, L., Gharib, A. H., Ashraf, H., & Murugesan, R. K. (2024). Industry 4.0. In Advances in logistics, operations, and management science book series (pp. 342–405). https://doi.org/10.4018/979-8-3693-1363-3.ch013
101. Sindiramutty, S. R., Tan, C. E., & Wei, G. W. (2024). Eyes in the sky. In Advances in information security, privacy, and ethics book series (pp. 405–451). https://doi.org/10.4018/979-8-3693-0774-8.ch017
102. Sindiramutty, S. R., Tan, C. E., Shah, B., Khan, N. A., Gharib, A. H., Manchuri, A. R., Muniandy, L., Ray, S. K., & Jazri, H. (2024). Ethical considerations in drone cybersecurity. In Advances in information security, privacy, and ethics book series (pp. 42–87). https://doi.org/10.4018/979-8-3693-0774-8.ch003
103. Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Kavita, N., Rodrigues, J. J. P. C., Jhanjhi, N. Z., Ghosh, U., Jo, O., & Iwendi, C. (2020). Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned railway level crossings. IEEE Access, 8, 113790–113806. https://doi.org/10.1109/access.2020.3002416
104. Starknet (2024). Understanding Staking in Blockchain. [online] Starknet.io. Available at: https://www.starknet.io/blog/understanding-staking-in-blockchain/ [Accessed 29 Nov. 2024].
105. Tagade, K. (2021). An Introduction to Blockchain Security. [online] www.getastra.com. Available at: https://www.getastra.com/blog/knowledge-base/blockchain-security/.
106. Team, C. (2023). The Importance of Blockchain Security - Chainalysis. [online] Chainalysis. Available at: https://www.chainalysis.com/blog/blockchain-security/#The%20future%20of%20blockchain%20security.
107. Team, L.C.X. (2024a). Blockchain Security: Transaction Data Safety. [online] LCX. Available at: https://www.lcx.com/blockchain-security-transaction-data-safety/.
108. Team, L.C.X. (2024b). What is Decentralization in Blockchain. [online] LCX. Available at: https://www.lcx.com/what-is-decentralization-in-blockchain/.
109. Team, M. A. (2024, June 14). Exploring the types of nodes in blockchain networks. MaskEX Blog. https://blog.maskex.com/news/maskex-daily-digest/exploring-the-types-of-nodes-in-blockchain-networks
110. Techopedia. (2023). SHA-256. [online] Available at: https://www.techopedia.com/definition/sha-256.
111. Tripathi, G., Ahad, M.A. and Casalino, G. (2023). A Comprehensive Review of Blockchain technology: Underlying Principles and Historical Background with Future Challenges. Decision Analytics Journal, [online] 9(1), p.100344. Available at: https://www.sciencedirect.com/science/article/pii/S2772662223001844.
112. Tripathi, V. (2021). How Bitcoin Works | Cryptocurrency Technologies. [online] Trendpickle. Available at: https://trendpickle.com/how-bitcoin-works-cryptocurrency-technology/.
113. Uddin, M., S. Memon, M., Memon, I., Ali, I., Memon, J., Abdelhaq, M. and Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. Computers, Materials & Continua, 68(2), pp.2377–2397. doi:https://doi.org/10.32604/cmc.2021.015354.
114. Ujjawal, A. (2018). How Does the Blockchain Work? [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/how-does-the-blockchain-work/.
115. vietnamblockchain.asia. (n.d.). Vietnam Blockchain Corporation. [online] Available at: https://vietnamblockchain.asia/post/5666316/5-basic-components-of-blockchain.
116. Waheed, A., Seegolam, B., Jowaheer, M. F., Sze, C. L. X., Hua, E. T. F., & Sindiramutty, S. R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure. preprints.org. https://doi.org/10.20944/preprints202407.2338.v1

117. Wen, B. O. T., Syahriza, N., Xian, N. C. W., Wei, N. G., Shen, T. Z., Hin, Y. Z., Sindiramutty, S. R., & Nicole, T. Y. F. (2023). Detecting cyber threats with a Graph-Based NIDPS. In Advances in logistics, operations, and management science book series (pp. 36–74). https://doi.org/10.4018/978-1-6684-7625-3.ch002
118. Wissen, D. (2024). The intersection of Artificial Intelligence (AI) and Blockchain technology represents a transformative frontier with the potential to redefine industries, from finance and healthcare to supply chain and beyond. While both technologies are powerful in their own right—AI for its data-driven intelligen. [online] Linkedin.com. Available at: https://www.linkedin.com/pulse/ai-blockchain-revolutionizing-security-efficiency-decentralization-yyjpf/ [Accessed 29 Nov. 2024].
119. www.dock.io. (n.d.). Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2023. [online] Available at: https://www.dock.io/post/decentralized-identifiers.
120. www.google.com. (n.d.). Redirect Notice. [online] Available at: https://www.google.com/url?q=https://www.bing.com/ck/a?.
121. www.techtarget.com. (n.d.). Data security and privacy | Resources and Information from TechTarget. [online] Available at: https://www.techtarget.com/searchsecurity/resources/Data-security-and-privacy.
122. www.tripwire.com. (n.d.). Blockchain Security: Understanding vulnerabilities and mitigating risks | Tripwire. [online] Available at: https://www.tripwire.com/state-of-security/blockchain-security-understanding-vulnerabilities-and-mitigating-risks.
123. Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018). Blockchain Technology Overview. National Institute of Standards and Technology, 1(1). doi:https://doi.org/10.6028/nist.ir.8202.
124. Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D. and Zeng, X. (2020). Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. Energies, 13(4), p.881. doi:https://doi.org/10.3390/en13040881.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.