Blockchain Security Using Confidentiality, Integrity, and Availability for Secure Communication

Chukwuebuka Francis Ikenga-Metuh and Abel Yeboah-Ofori *

Posted Date: 22 October 2025

doi: 10.20944/preprints202510.1488.v1

Keywords: blockchain technology; confidentiality; integrity; availability; SHA512; RSA encryption; network security

 doi:10.20944/preprints202510.1488.v1

Article

Blockchain Security Using Confidentiality, Integrity, and Availability for Secure Communication

Chukwuebuka Francis Ikenga-Metuh and Abel Yeboah-Ofori*

University of West London, UK

* Correspondence: abel.yeboah-ofori@uwl.ac.uk

Abstract

Network Security in blockchain Technology provides transparency, decentralization of user records during transactions, and immutability through consensus. However, integrating Confidentiality, Integrity and Availability (CIA) in blockchain Technology in Network Security environment cannot be over emphasized due to vulnerabilities on blockchain network nodes, and the security challenges including Private Key theft, Sybil attacks, Smart Contract exploits, 51% attacks and spear phishing attack that has led to data theft, data manipulation and breaches, financial losses and distrust. The paper explores network security issues and vulnerabilities in blockchain technology, focusing on the CIA to improve security. The contribution of the paper is threefold. First, it explores the various blockchain vulnerabilities and exploits during transactions. Secondly, it develops a blockchain system called MasterChain in a virtual environment as a testbed. An attack on the MasterChain blockchain system will then be orchestrated to exploit vulnerabilities. Finally, it models the system to conform to the CIA Triad and recommends control mechanisms to improve security. The results show that the CIA triad can be used to prevent possible Blockchain attacks during the exploitation of blockchain vulnerabilities.

Keywords: blockchain technology; confidentiality; integrity; availability; SHA512; RSA encryption; network security

1. Introduction

Blockchain Technology is remarkable for its innovation in leveraging consensus mechanisms, cryptographic algorithms, decentralized and verified transactions, transparency, and secured data records [1]. However, the challenges in securing the blockchain to ensure its security have become increasingly daunting due to issues with decentralization, peer-to-peer computing, data integrity violations and privacy issues, scalability, and data breaches during transmission over the network. Blockchain technology has become one of the most reliable systems for storage operating in a network environment. It provides transparency and decentralization of user records during transactions and immutability through consensus. However, integrating security protocols into blockchain Technology in a network environment brought with it challenges due to vulnerabilities in the blockchain network infrastructure. That has led to security challenges, including Private Key theft, Sybil attacks, Smart Contract exploits, 51% attacks, and spear phishing attacks. Such attacks can lead to data theft, data manipulation and breaches, financial loss, distrust, system hijacking, among others. These can be attributed to the rising cyberattacks that are now targeting and plaguing most businesses, especially in the financial sector [2]. Since the blockchain is seen as very secure, institutions with highly sensitive information are exploring the effectiveness of the technology in mitigating cyberattacks to improve security. Several challenges and risks exist which impact Blockchain technology leading to network vulnerabilities such as improperly installed hardware or software, outdated operating systems or firmware, and inadequate access control mechanism among others. Figure 1 shows a blockchain network architecture and areas that are susceptible to attacks.

 doi:10.20944/preprints202510.1488.v1

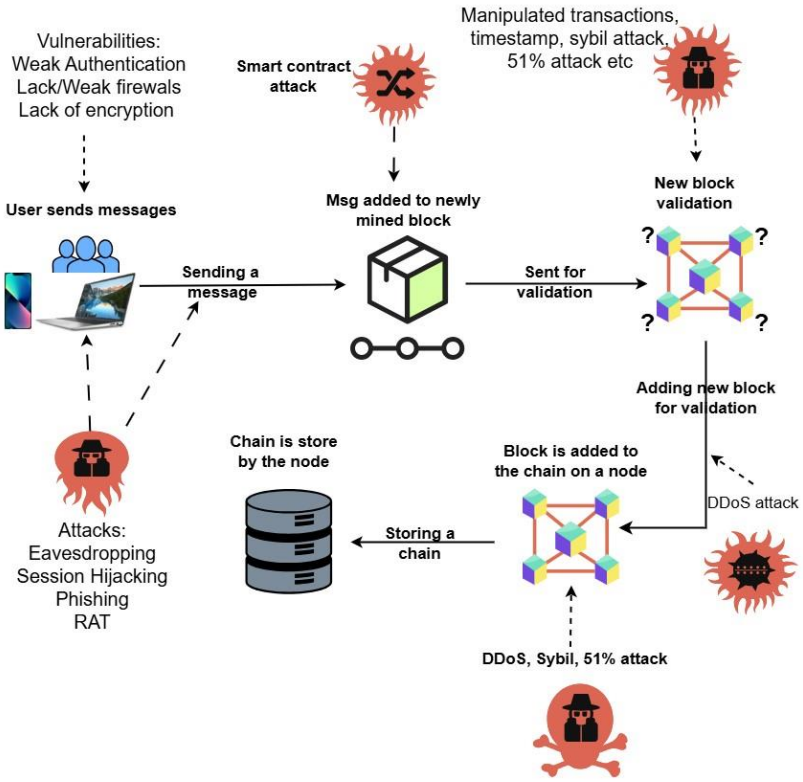

Figure 1. Blockchain Model and Vulnerable Spots.

Furthermore, the study will be narrowed down to explore and present issues with network security and a system that will model a solution by demonstrating how technology of the blockchain can be enhanced with Confidentiality, Integrity, and Availability security principles through the implementation of security systems like encryption mechanism, access control mechanism, blockchain platform development and cryptographic hashing, distributed blockchain networking, and decentralized storage structure.

The paper explores network security issues and vulnerabilities in blockchain technology, focusing on the CIA to improve security. The contribution of the paper is threefold. First, it explores the various blockchain vulnerabilities and exploits during transactions. Secondly, it develops a blockchain system called *MasterChain* in a virtual environment as a testbed. An attack on the *MasterChain* blockchain system will then be orchestrated to exploit vulnerabilities. Finally, it models the system to conform to the CIA Triad to improve security.

2. State of the Art

This section reviews existing literature and the state-of-the-art of blockchain systems and technologies that underpin the blockchain as a network and its security architecture, encompassing cryptography and hashing functions. The analysis will subsequently evaluate the blockchain in relation to the core principles of network security, notably the CIA Triad: Confidentiality, Integrity, and Availability. Additionally, this review will address network security challenges and their implications for general computing practices.

2.1. Blockchain Technology and Network

The blockchain operates as a decentralized network comprising secure yet inherently untrusted peers, where updates are permissible exclusively through consensus among participants. As highlighted in [3], blockchain technology is increasingly utilized for robust record keeping, inventory management, and registry applications. Further use cases include voting systems for secure and

 doi:10.20944/preprints202510.1488.v1

transparent elections, decentralized InterPlanetory File Systems (IPFS) for addressing issues with vehicle network data storage, creation of new business models with blockchain technologies such as Non-Fungible Tokens (NFT) and Play to Earn (P2E), among others [4]. [5] emphasizes that blockchain implementation adds an additional application layer running concurrently with existing protocols, thus enabling participants to conduct economic transactions without dependence on trusted third parties. Moreover, blockchain-based software plays a pivotal role in enabling key operations such as contract execution, asset monitoring, and the tracing of crypto-assets [2].

The blockchain architecture ensures transactions are logged in a list forming a way of keeping records that are put together to form a block at the end. When a block closes, it connects with the already formed chain of blocks, and thus the name *blockchain*. Every block in the chain is preceded by one block and followed by another block, except for the last one, which only has a preceding block and the very first block, which is called the genesis block [6]. The values on the blocks accompany the cryptographic technique of hashing which mathematically connects the blocks to each other. This makes their digital identity impervious to any change. The interconnectivity of these blocks over each other's chain thus creates a tamper-proof condition because any slight change made in one block can affect all the others connected to it, except a general agreement is reached by the majority of nodes. This refers to the unique feature of the blockchain, which is termed immutability. Nodes represent participating computers and devices in the blockchain network. These nodes verify the process by having, running, and managing complete sets of databases each. As a result, data integrity is maintained since the system is always unchanged and protected.

There is a need for the verification of new transactions as well as the edited ones during the formation of a block. The determination of the eligibility of freshly proposed block or blocks is dependent on the ability of most of the nodes participating in that blockchain's network to solve the algorithmic verification tasks that confirm a block. The new block gets added to the chain if there is a consensus among majority of the participating nodes [7]. This verification process in combination with encryption mechanisms forms a strong security setup that can prevent any unauthorized access or manipulation. It aids in providing digital trails of network activities for auditing and digital forensics [1].

2.2. Blockchain Network Security Challenges

The number of data breaches affecting financial networks and resulting in the loss or compromise of personal data more than doubled between 2015 and 2017 only. Security issues such as the growing number of attacks and its impact make network security a critical subject for already certified and potential IT professionals. Network security, which is an important area in the field of cybersecurity, is the process of restricting access of devices and networks to unauthorized users. It covers physically protecting network servers and devices to limit external access to them and taking measures that ensure digital networks are secure. Today, in an era where cyberattacks are growing more frequent and advanced, the matter of network security takes more importance than ever before. To successfully deploy and operate secure networks, it is crucial to know the key vulnerabilities, threats, and problems in the current IT sector. Whilst some problems can be sorted out quite easily, others need more complicated solutions. Almost every computer network is vulnerable to attacks from outside the system; besides, the devices and networks are exposed even if no one actively threatens or targets them. Vulnerability is the state of the network or its physical components, not because of external interference [8]. Table 1. enlists some common network vulnerabilities:

 doi:10.20944/preprints202510.1488.v1

Table 1. Vulnerabilities and Description.

Vulnerability Type	Description
Unpatched Systems	Failure to update OS or software introduces exploits
Weak Authentication	Use of insecure or default passwords
Improper Configurations	Poorly installed nodes or components
Design Flaws	Architectural gaps within the OS or blockchain software
Lack of Encryption	Absence of proper cryptographic protections

Vulnerabilities are not the only reason for an attacker or hacker to target a network. Nevertheless, they can make the task of penetrating the network easier, and possible.

2.3. Security Analysis of Blockchain Technology

2.3.1. Blockchain and CIA Triad:

The CIA security model facilitates the understanding of the impact of technology on the Confidentiality, Integrity and Availability of data or digital information. As network security breaches and attacks have been on the rise, it has become imperative to explore other forms of network systems that can mitigate the security issues and incidents to the barest minimum. This review will look at the blockchain network and how it conforms with the CIA Triad to provide better security in the blockchain's network and infrastructure. Approaching blockchain from this perspective provides a better comprehensive understanding of the way data stored on a blockchain is protected when it comes to these three security principles.

a) Confidentiality: The National Institute of Standards and Technology, (NIST) enumerated that preserving the authorization restrictions on information access and disclosure is the main aim of confidentiality which involves protecting personal privacy and proprietary information. The undeniable fact that all data storages in a public blockchain are accessible to all participants who act as nodes does not undermine the confidentiality principle because the encryption of data would make it impossible for any potential attacker to carry out any attack, thanks to the implementation of private keys, where no one else can access information deposited on a blockchain except the true owners [9]. If a private key gets stolen, a hacker can open everything that is behind the private key. Therefore, perform backups of your private keys using secure devices to safeguard them. However, the advent of quantum computing would lead to cyber security issues for blockchain platforms that are based on cryptographic private and public keys. This technology has a prospect of unraveling the private key, which is currently unachievable utilizing the available computing power. This can be resolved using more sophisticated hashing algorithms that are based on the SHA-384, 512 algorithms among others.

Further study also shows that NTRU-based cryptographic mechanism proves to be one of the most effective security measures for post-quantum cryptography considering its speed and energy efficiency outperforming traditional cryptographic techniques [10].

 doi:10.20944/preprints202510.1488.v1

b) Integrity: NIST [9] defines integrity as the property of unaltered data in an unauthorized manner on both storage, processing, and during transit over a network. This is made possible by using blockchain technology to create tamper-evident logs through hash codes that change with the slightest alteration of any detail whatsoever, the integrity of data can hence be made certain. In addition to this, blockchain technology provides a transparent verification procedure which allows for the identification of any data modification done by an attacker from the point of attack or breach. The blockchain feature ensures storage records of transactions for data reliability and integrity has not been violated on a trusted network. Further, data operations and computational transactions required could be added to the blockchain signed with a private key to achieve traceability [9].

c) Availability: NIST 2013, stated that availability is "an assured access to and use of the data without constraints." The blockchain here stores this data by utilizing a network of nodes which are distributed. This implies that if an attacker seeks to breach the network or destroy the whole network or just a small part of its functions, that will not affect the rest of the network [9]. A node under attack is easily excluded from the network as it forms a decentralized system and ensures the network remains extremely resilient, when attackers try to disable the network by sending many transactions at the same time. Decentralization of blockchain network ascertains that there is no single point of failure that can break down the entire network. An example is in a case where a country faces a total blackout, all their networked stations will cease to communicate. However, with the decentralization of their infrastructure and adequate networks, their data and information in other locations of the blockchains will be available for access [9].

2.4. Cryptography Algorithms in Data and Networks

Data and networks have been secured by cryptographic algorithms and different transposition systems for the security of points of sales systems, including electronic commerce, chip-based payment systems, digital currency systems, passwords [11]. Cryptography is the use of sophisticated computing techniques to protect information which is valuable and sensitive to prevent unauthorized access either when in storage or during network transmission. The word 'kryptos' was adopted from the Greek lexicon which means 'hidden' [12]. Encryption and obfuscation are two key elements of cryptography. The process of scrambling or rearranging data into a cipher and back to original form on arrival to its destination is known as Encryption while hiding data or information within other data using techniques like microdots or merging is called Obfuscation.

Cryptography has different encryption techniques, but the most popular ones are symmetric, asymmetric, and hashing. For the blockchain, the cryptographic hashing technique was adopted as the most efficient, secure, and reliable solution for decentralized network protection and distributed computing requirements of the blockchain's underlying security mechanism.

2.5. Hashing Functions in Cryptography Algorithm

The H in a hashing function takes an input of any size and then maps it into a size that is fixed as output [13]. Additionally, they have the following functions which include collision resistance, preimage resistance, and second preimage resistance. For Collision resistance, values *a* and *b* will be decoded with difficulty per the following illustration:

$$H(a) = H(b) \quad (1)$$

Equation (1) ensures secure advantages for the system. In Preimage resistance, the difficulty is to discover input '*a*' when output '*y*' is given per the following expression:

$$H(a) = y \quad (2)$$

For Second Preimage resistance, given in (2), difficulty in finding second level input '*b*' will be doubled as follows:

$$H(b) = y \quad (3)$$

 doi:10.20944/preprints202510.1488.v1

Cryptographic hash functions are necessary in blockchains as cryptographic puzzles rely on them for their solutions (eg Bitcoin's Proof of Work (PoW)), addresses generation (for public and private keys), reduction of public address length, and signature of message descriptions. The most used hash function for blockchain technology is SHA-256 in the cryptocurrency industry. It is employed in Bitcoin with a double application of the technique which is known as SHA-256d as illustrated in the following expression:

$$\text{SHA256d(message)} = \text{SHA256(SHA256(message))} \quad (4)$$

2.6. RSA Encryption

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) introduced a cryptographic algorithm in 1978, which replaced the National Bureau of Standards (NBS) algorithm as it was less secure [14]. The RSA encryption system is based on the mathematical enumerations of modular arithmetic with prime numbers, making provision for a way of securing data through a public key for encryption and a private key for decryption. RSA security depends on the difficulty in the factorization of a large number into its prime factors [15,16]. RSA Key generation Components:

- Prime Numbers p and q: - These are any secret prime numbers which are used for key generation.
- Modulus n - The product of p and q. This forms part of the public key used in encryption and decryption.
- Public Exponent e: A choice of number such that:

$$1 < e < a\ \phi(n) \quad (5)$$

Where the equation (5) does not share a factor with $\phi(n)$. This also forms part of the public key.

- Private Key d: The modular multiplicative inverse of e *modulo* $\phi(n)$.

1) Calculating the private key 'd': The calculation of the private key d is fundamentally about finding a number to decrypt a message encrypted with the public key component e, adhering to the RSA algorithm. This is done by calculating the modular multiplicative inverse of the expression:

$$e \text{ modulo } \phi(n) \quad (6)$$

Where $\phi(n)$ is Euler's totient function, representing the number of integers coprime to n, with

$$n = p \times q \quad (7)$$

2) The Modular Multiplicative Inverse: The modular multiplicative inverse of *(6)* is a number d such that the following congruence relation is satisfied:

$$e \times d \equiv 1 \bmod \phi(n) \quad (8)$$

Equation (8) signifies that when e is multiplied by d, and the product is divided by $\phi(n)$, the remainder (or modulus) is 1. Finding d is critical because it ensures that whatever is encrypted with e can only be decrypted with d, and vice versa, fulfilling the requirement for asymmetric encryption [17].

3) Why use p-1 and q-1?: Using *p-1* and *q-1* in the formula is related to Euler's totient function (ϕ) and its properties with prime numbers. Since p and q are prime, each has precisely *p-1* and *q-1* numbers, respectively, that are prime to them. The product of these two numbers gives us the total number of integers less than n that are coprime to n, which is essential in the RSA algorithm for ensuring that the encryption and decryption operations are inverses of each other [18]. In practice, d is calculated using efficient algorithms like the Extended Euclidean algorithm, which can find the modular inverse without exhaustively trying every possible value. While computationally intensive, this calculation is feasible with modern computers and forms the backbone of the security provided by RSA encryption.

 doi:10.20944/preprints202510.1488.v1

2.7. Addressing Gaps in Literature

Existing research on blockchain security often emphasizes quantitative metrics, technical assessments, or performance evaluations. However, there are significant gaps in the literature related to the practical implementation of the security mechanisms, especially from a human and organizational perspective. A qualitative approach enables the researcher to explore these less tangible but critically important dimensions of network security, such as decision-making processes, stakeholder collaboration, and organizational strategies.

The blockchain implementation process considers choosing a MasterChain development platform that involves identification, selection, evaluation and validation [19]. Further, the implementation process adopted similar techniques from the information in the reviewed literature from existing work.

3. Approach

This section discusses the proposed approach for the study and methods of implementation and the justification of the approach. The choice of qualitative research approach for this paper can be justified based on some important factors which especially depend on the complex and evolving nature of both network security and blockchain technology. It will also help in great lengths to answer the research questions of 'how' and 'why' this work is being conducted and implemented [18]. This research approach which aims for more in-depth exploration of the intricate and context-specific difficulties can be seen in the implementation of the CIA Triad (Confidentiality, Integrity, and Availability) in blockchain systems. The following points were considered during the selection process of the approach used for this implementation.

Figure 2 shows the implementation process as proposed by the Central Blockchain Council of America (CBCA) [19]. From Use case identification, proof of concept, choice of the blockchain platform, choice of right consensus protocol, to building of the ecosystem and definition of operational rules.

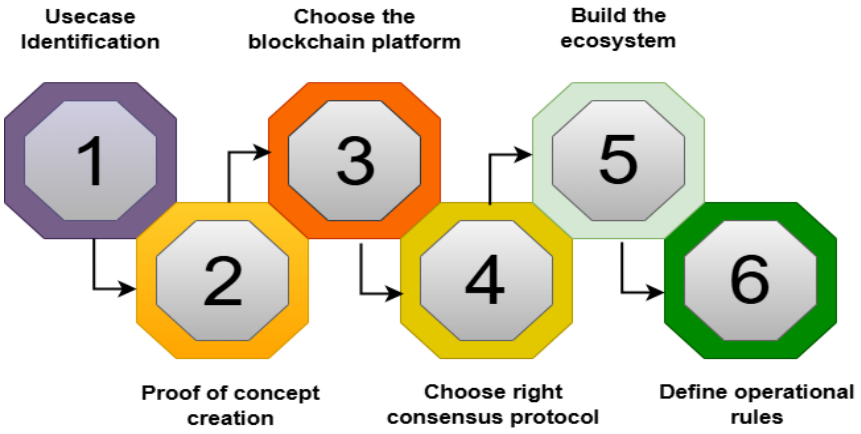

Figure 2. Blockchain Implementation Steps.

Table 2 considers the (CBCA) approach [19] and provides a brief description of the method for the implementation steps as follows:

Table 2. Implementation Process.

Step	Description
1) Identification of the use case	Aim and Objectives on how the solution will be proffered

 doi:10.20944/preprints202510.1488.v1

2) Creation of proof of concept	Proof of concept created through detailed analysis of existing work
3) Choosing the blockchain platform	Choice based on requirements of the implementation and desired results
4) Choose the right consensus protocol	Proof of Work (PoW) as discussed in concept background and literature reviews
5) Build an ecosystem	Main practical work for this exploration
6) Determine rules of operation	Part of Section V. Results and Discussions

The justification of our approach considers issues relating to the challenges of finding vulnerabilities in the Blockchain smart contract and how it is crucial to prevent attackers from deploying malicious exploits during transactions [20].

4. Implementation

This implementation will show a step-by-step demonstration of the proposed topic using the approach described in Section 3. As proof of concept is already established and the platform is to be developed from scratch, necessary requirements will next be elucidated for setting up a working environment like software and hardware. It will then discuss the work setup and show the detailed process of coding the MasterChain system with relevant screenshots of the working software.

4.1. Software Requirements:

The software needed for implementation is as follows:

- Visual Studio Code: This is the primary Integrated Development Environment (IDE) where the MasterChain system will be coded. The IDE provides a coding platform for many programming languages and packages.
- Anaconda Python: Python is an all-purpose programming language that can be used to code across different platforms. It comes with suitable libraries which are ideal for the development of the MasterChain blockchain system. For this paper, the Anaconda distribution of python will be used.
- Flask: This is a python framework used to develop web applications. It will be used to program the distributed computing features of the MasterChain system to give it the functionality of constant availability.
- Postman: It is a web client that will be used to interact with the MasterChain blockchain system.
- VirtualBox: This is a virtualization software used to set up and run one or multiple complete or pre-packaged operating system known as guest OS inside another operating system running on a local computer.
- Ubuntu Linux OS: Ubuntu is a type of Linux Operating System distribution which is open-source, stable, and user-friendly.

4.2. Hardware Requirements and Lab Set up

The hardware system used for this implementation was HP Laptop Computer (16gb RAM, 2TB HDD, Intel Core i7).

Setting up the lab for this implementation basically involved the use of two nodes where the HP Laptop computer serves as the first node and a virtual machine running Ubuntu Linux will serve at the second. On the first node, installation of the VS Code IDE and some relevant python extensions like pylance, language support, and debugger to facilitate the coding experience will be done.

 doi:10.20944/preprints202510.1488.v1

Two dependencies will also be installed on both nodes. They are the python **flask** library and requests library. Packages like RSA Python and pycryptodom encryption are added to the development computer's VSCode development environment which will enable implementation of data privacy by making any stored information on the MasterChain blockchain hidden.

4.3. Coding Process of the MasterChain System

The Coding process of the MasterChain system starts with importation of relevant libraries and modules to be used in the entire coding process. Figure 3 and the steps below provides a brief explanation of the imported libraries:

- RSA Algorithm: Used for encrypting the information
- Hashlib: Used to call the SHA 256 or 512 hash functions
- JSON: Used for JavaScript Object Serialisation. It helps to show the python code data in human readable format.
- Base64: Used to encode byte data into JSON string
- Crypto.publickey: Used in combination with RSA to create encryption keys
- Crypto.cipher: Used in combination with RSA to create encryption keys
- Requests: Used to make JSON object requests for JSON data within an application or from across applications
- Time: Used for creating timestamps for mined blocks
- UUID4: This is used to create a unique identifier for an object, in our case, a computing node.
- Flask: A light python package or module use for web content programming.
- Jsonify: Used to manipulate and display data in human redable format in python and flask applications.
- Flask request: used to make web object requests in flask applications.
- URLparse: use for sending and pulling url requests and data.

The Blockchain class defines the main structure of the MasterChain system along with its properties like functions and variable definitions. Figure 3 below also shows the imported libraries and beginning of the Blockchain class.

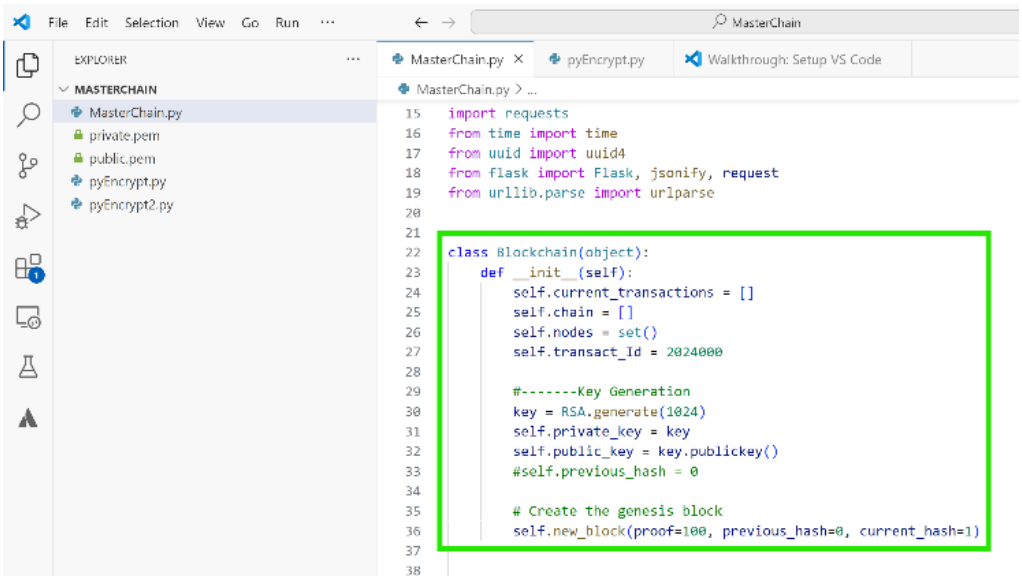

Figure 3. The Libraries Importation and Blockchain Class Definition.

The Blockchain class starts with initialization of relevant variables, then proceeds with definition of useful functions. All of which will make up the properties of the blockchain that we are building. These properties will eventually be accessed or called by instantiating an object of the blockchain

 doi:10.20944/preprints202510.1488.v1

class. Figure 4 shows how the two functions new_transaction and new_transaction_encrypted are coded. The first one is to create new transaction when a user makes the request, and second is to create an encrypted version of the first if confidentiality is required.

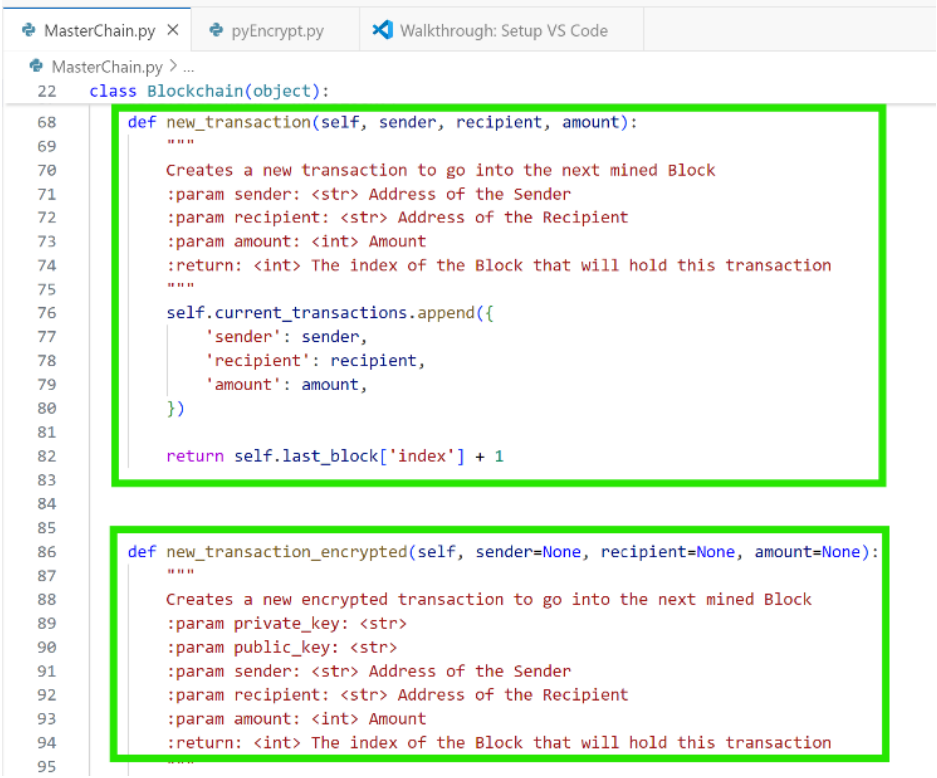

Figure 4. New_Transaction and New_Transaction_Encrypted functions.

Figure 5 depicts how the chosen consensus protocol which is proof of work function is defined along with a validation function to verify the proof. The function for registering nodes is created. These nodes are the system that form the distributed computing future which gives the assurance of Availability in the CIA Triad. It is followed by the function to verify the chains of a block which ensures their authenticity.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 October 2025 doi:10.20944/preprints202510.1488.v1


```python
MasterChain.py > ...
class Blockchain(object):
    def valid_proof(last_proof, proof):
        guess_hash = hashlib.sha512(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def register_node(self, address):
        """
        Add a new node to the list of nodes
        :param address: <str> Address of node. Eg. 'http://192.168.0.5:5000'
        :return: None
        """

        parsed_url = urlparse(address)
        self.nodes.add(parsed_url.netloc)

    def valid_chain(self, chain):
        """
        Determine if a given blockchain is valid
        :param chain: <list> A blockchain
        :return: <bool> True if valid, False if not
        """

        last_block = chain[0]
        current_index = 1

        while current_index < len(chain):
            block = chain[current_index]
            print(f'This is the First Block ---- \n{last_block}')
            print(f'These are the Subsequent Blocks ---- \n{block}')
            print("\n-----------\n")
            # Check that the hash of the block is correct
            print ("Current Block  Previous Hash ", block['previous_hash'])
```

Figure 5. Chain Functions Created for Registering the Nodes.

Figure 6 shows the coding of the flask application that presents the visuals and communication with the blockchain through 'endpoints' mechanism.

```python
MasterChain.py > ...

# Instantiate our Node
app = Flask(__name__,)

# Generate a globally unique address for this node
node_identifier = str(uuid4()).replace('-', '')

# Global Variable for Transaction ID
#tID = 2024000

# Instantiate the Blockchain
blockchain = Blockchain()
previous_hash = blockchain.last_block['current_hash']

@app.route('/mine', methods=['GET'])
def mine():
    # We run the proof of work algorithm to get the next proof...
    last_block = blockchain.last_block
    last_proof = last_block['proof']

    proof = blockchain.proof_of_work(last_proof)

    # We must receive a reward for finding the proof.
    # The sender is "0" to signify that this node has mined a new coin.
    blockchain.new_transaction(
        sender="0",
        recipient=node_identifier,
        amount=1,
    )
```

Figure 6. Flask App Initialization through 'Endpoints' Mechanism.

 doi:10.20944/preprints202510.1488.v1

These endpoints are where the normal web browser connects to human interactions and visualization of the blockchain behaviors, activities, and responses. The flask application will be accessed at a specified IP address and port number being 0.0.0.0 and 5000 respectively.

5. Results and Discussion

The result of the above implementation is centered on the achievement of improving security by aligning the Confidentiality, Integrity, and Availability factors of the CIA Triad to conform to the business goals of the MasterChain blockchain system which are data encryption, cryptographic hashing, and distributed functionality. The results show that the CIA triad can be used to prevent possible Blockchain attacks during the exploitation of blockchain vulnerabilities. Figure 7, box 2 proves that when a user sends in a message as transaction to the blockchain using the Postman client, the contents of the message are encrypted and added to the blockchain. Further, Figure 7, box 3 shows the block that mined the user's transaction to the MasterChain system and is denoted as 'Block 3'. Box 2 has the user's transaction with the entire message encrypted. An attacker who tries to sniff the transmitted data with a sniffing tool will only see encrypted data.

Figure 7. User's transaction with the message encrypted.

The same transaction can be seen in box 2 of Figure 8 which was captured in the other node running the Ubuntu VM as the second node of the MasterChain blockchain system.

 doi:10.20944/preprints202510.1488.v1

Figure 8. Ubuntu nodes resolved to sync with Windows nodes.

The findings indicate that the Confidentiality aspect of the Triad was ensured through the MasterChain system's capability to encrypt messages within transactions, utilizing the RSA encryption mechanism. In a traditional blockchain system, transaction hash, identifier, or number can easily reveal the contents of a transaction for public consumption, but the MasterChain system keeps transactions private and only accessible to the holder of the private key. Further, better integrity was achieved by employing SHA512 cryptographic hashing and linking of the mined blocks that appear as a chain which makes the system immutable. This enables the preservation of the system's integrity.

Furthermore, the Availability future was achieved by the operation of the distributive nature of the system where the host node (Windows) could interact and synchronize with the guest node (the Ubuntu VM) to validate and store identical information generated on the blockchain system running concurrently. The significance of the distributed functionality is to ensure that if one node goes down, the system will still be up and running and therefore remains available for use.

Figure 9 below buttresses these outcomes as can be seen where the user's protected message is transmitted using Postman client in addition to the Secured Socket Layer (SSL) protocol through the internet. This helps prevent any form of packet sniffing or man in the middle attacks. When fed into the blockchain infrastructure, the message is received as a transaction, secured with RSA encryption, and attached to a block for mining. The block once mined is further secured with cryptographic hashing function to strengthen the security through immutability as it is being added to the existing chain of blocks for storage. The transaction once stored becomes tamper-proof owing to the immutable nature of the MasterChain blockchain system.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 October 2025 doi:10.20944/preprints202510.1488.v1

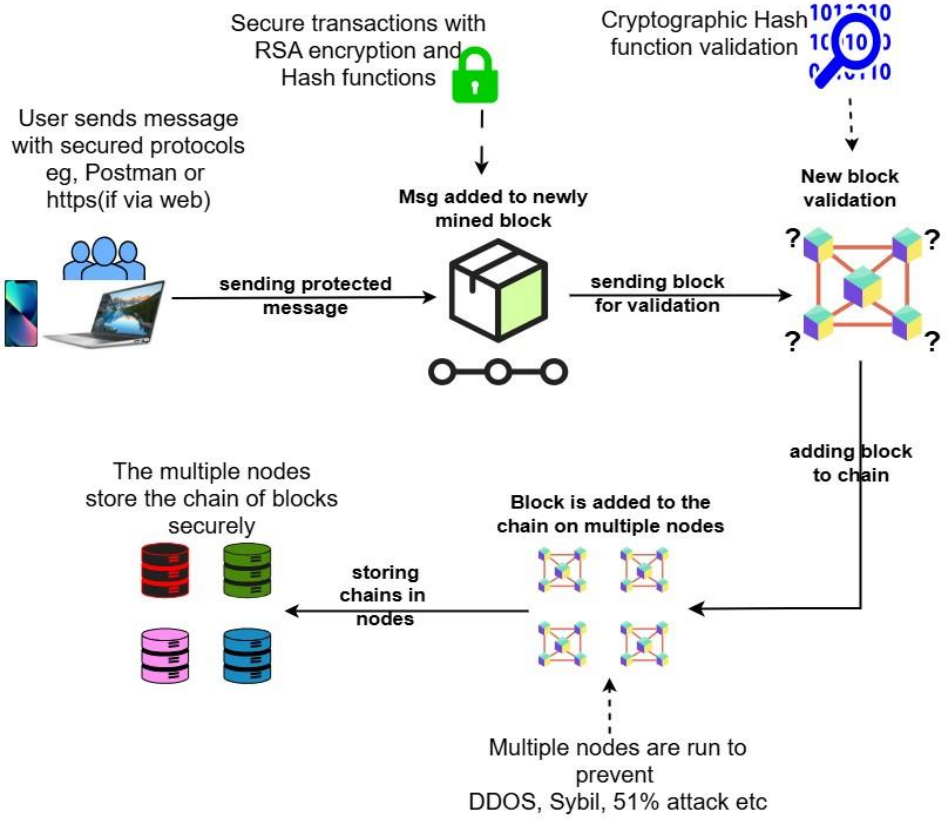

Figure 9. Blockchain Attack Prevention Mechanism Model.

A. Blockchain Prevention Mechanisms

Table 3. discusses the Blockchain prevention mechanisms using the CIA triad to improve security in a network transaction process:

Table 3. Blockchain Prevention Mechanisms.

CIA Principle	Attack Types	Prevention Mechanisms
Confidentiality	Eavesdropping Attacks	Application of End-to-end encryption to secure data in transit.
	Deanonymization Attack	Apply Zero-knowledge Proofs (ZKPs) and privacy-preserving techniques such as ring signatures.
	Metadata Leakage	Mixing services, coin tumblers, and onion routing (e.g., TOR).
Integrity	Double Spending	Cryptographic consensus protocols (PoW, PoS), transaction finality mechanisms.
	51% Attack	Decentralization, checkpointing, hybrid consensus models.
	Smart Contract Exploits	Formal verification, rigorous auditing, and use of secure contract patterns.

 doi:10.20944/preprints202510.1488.v1

Availability	Denial of Service (DoS)	Rate limiting, minimum gas thresholds, and DDoS protection measures.
	Sybil Attack	Identity validation, stake-based participation, and node reputation systems.
	Routing Attacks (e.g., BGP Hijacking)	Use of redundant nodes, encrypted communication, and real-time routing monitoring.

6. Conclusions

This work has shown the effectiveness of modern security technology tools like RSA encryption mechanism and cryptographic hash functions using blockchain technology. It looked at how the CIA principles can be incorporated to boost the security of networks, especially for financial related operations. First, the introductory section gave a broad look at security trends and their impact on modern day society. It discussed the challenges that organizations are facing which have been on the rise and then identified some of these challenges along with how to tackle them.

A review of several literatures was conducted to facilitate the proposed technique chosen to tackle the identified security challenges, which is using a blockchain system to model the CIA Triad. It extensively discussed blockchain technologies, cryptographic hashing, and RSA encryption mechanism. The qualitative approach method was chosen and justified extensively. Also, an implementation procedure was chosen and discussed.

The implementation section is the core of this development work. It started with the identification of requirements and artefacts needed. Then it discussed the platform and lab environment setup for software development. It discussed the use of VSCode IDE and Oracle Virtual Box as virtualization software to run a guest OS, Ubuntu Linux. It then went through the detailed coding process with explanation of the blockchain class, functions, and applications. Section V enumerated the outcomes of the functionalities of the software. It gave insights into how the developed application will benefit organizations in real world use by protecting their systems through conformity with the CIA Triad security principles.

Future work will consider the adoption of blockchain technology security mechanisms for critical infrastructure use cases such as the protection of financial transactions in cloud-based systems which are more exposed to threats.

Acknowledgments: We thank immensely our respective families for their support during the study and research process, design, development, and implementation of this work. The authors have reviewed and edited the output and take full responsibility for the content of this publication."

Conflicts of Interest: Declare conflicts of interest or state "The authors declare no conflicts of interest." Authors must identify and declare any personal circumstances or interest that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results must be declared in this section. If there is no role, please state "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results".

 doi:10.20944/preprints202510.1488.v1

Abbreviations

The following abbreviations are used in this manuscript:

CIA	Confidentiality, Integrity, and Availability
SHA	Secure Hash Algorithm
RSA	Rivest, Shamir, and Adleman
NIST	National Institute of Standards and Technology
PoW	Proof of Work
NBS	National Bureau of Standards
CBCA	Central Blockchain Council of America
IDE	Integrated Development Environment
NTRU	N^{th} Truncated polynomial Ring Units
NFT	Non-Fungible Token
P2E	Play to Earn

References

1. Yeboah-Ofori, A.; Sadat, S. K.; Darvishi, I. "Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment," 2023 10th (FiCloud), Morocco, 2023, pp. 344-351, doi: 10.1109/FiCloud58648.2023.00057.
2. De Miranda, P. L.; Kerrigan, C. Cybersecurity amd Blockchain. In: Finteck. s.l.:Edward Elgar Publishing, pp. 242-266.
3. Wylde, V.; Rawindaran, N.; Lawrence, J.; Balasubramanian, R.; Prakash, E.; Jayal, A.; Khan, I.; Hewage, C.; Platts, J. Cybersecurity, Data Privacy and Blockchain: A Review. SN COMPUT. SCI. **3**(127). https://doi.org/10.1007/s42979-022-01020-4.
4. Taherdoost, H. Blockchain Innovations, Applications, and Future Prospects. Electronics 2024, 13, 422. https://doi.org/10.3390/electronics13020422
5. Singh, G.; Garg, V.; Tiwari, P. Introduction to Blockchain Technology. In: R. Agrawal & N. Gupta, eds. Transforming Cybersecurity Solutions using Blockchain. Agrawal, Rashmi ed. Singapore: Springer, Singapore, pp. 1-18.
6. Antonopoulos, A. Chapter 7: The Bitcoin. https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html
7. Wang, Y.; Singgih, M.; Wang, J.; Rit, M. Making sense of blockchain technology: How will it transform supply chains?. Innsbruck, s.n.
8. CompTIA. (N.D) Network Security: What Is It, Why Does It Matter and What Can You Do to Make Networks More Secure?. https://www.comptia.org/content/guides/network-security-basics-definition-threats-and-solutions.
9. Bult, T. Security Analysis of Blockchain Technology, s.l.: Oulu University of Applied Sciences.
10. Karpinski, M.; Kuznetsov, O.; Oliynykov, R. Security, Privacy, Confidentiality, and Trust in the Blockchain: From Theory to Applications. Electronics. 2025 Feb 1;14(3):581, https://doi.org/10.3390/books978-3-7258-3308-5
11. Yeboah-Ofori, A.; Agbodza, C. K.; Opoku-Boateng, F. A.; Darvishi, I.; Sbai, F. "Applied Cryptography in Network Systems Security for Cyberattack Prevention," 2021 (ICSIoT), France, 2021, pp. 43-48, doi: 10.1109/ICSIoT55070.2021.00017.
12. Kaspersky, What is Cryptography? https://www.kaspersky.com/resource-center/definitions/what-is-cryptography.

 doi:10.20944/preprints202510.1488.v1

13. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. IEEE Access, 7(no issue), pp. 148550 – 148575. https://ieeexplore.ieee.org/document/8865045.
14. Milanov, E. The RSA Algorithm. RSA Laboratories. pp 1-11. http://susanka.org/MathPhysics2/RSA_Algorithm_Yevgeny.pdf.
15. Mahalakshmi, B. ; Deshmukh, G.; Murthy, V. N. L. N. Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm. IEEE Xplore, (online) pp.363–366. doi:https: //doi.org/10.1109/ICIIP47207.2019.8985665.
16. Cobb, M.; What Is the RSA algorithm? https://www.techtarget.com/searchsecurity/definition/RSA
17. Yakymenko, I. Z.; Kasianchuk, M. M.; Ivasiev, S. V.; Melnyk, A. M.; Nykolaichuk, Y. M. Realization of RSA Cryptographic Algorithm Based on vector-module Method of Modular Exponention. IEEE Xplore, pp.550–554. //doi.org/10.1109/tcset.2018.8336262.
18. StackExchange, RSA Key generation: Why Use lcm(p-1, q-1) Instead of the Totient ϕ(n)? Cryptography Stack Exchange. https://crypto.stackexchange.com/questions/95556/rsa-key-generation-why-use-lcmp-1-q-1-instead-of-the-totient-%cf%95n/95557#95557.
19. Nanayakkara, S.; Rodrigo, M. N. N.; Perera, S.; Weerasuriya, G. T.; Hijazi, A. A. A methodology for selection of a Blockchain platform to develop an enterprise system. Journal of Industrial Information Integration, https://doi.org/10.1016/j.jii.2021.100215.
20. Darvishi, I.; Asare, B. T.; Musa, A.; Yeboah-Ofori, A.; Oseni, W.; Ganiyu, A. "Blockchain Technology and Vulnerability Exploits on Smart Contracts," 2024 11th (FiCloud), Vienna, Austria, 2024, pp. 160-167, doi: 10.1109/FiCloud62933.2024.00032.