Application of Number Theory in Blockchain Using Cryptography and Hashing

Ariel Jovananda– 13521086
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13521086@std.stei.itb.ac.id

***Abstract*— A key component of blockchain technology is cryptography, which enables safe data transmission and storage over the network. Data is encrypted and decrypted using mathematical techniques, guaranteeing that only people with the proper permissions can access it. Cryptography is employed in the context of blockchain to protect the transactions that take place on the network and to confirm the parties' identities. This guarantees that transactions are carried out securely and transparently and that the integrity of the data on the blockchain is maintained. So how exactly are cryptography and hashing employed in blockchain?**

***Key words*—Blockchain, cryptography, hashing, number theory.**

I. INTRODUCTION

Using codes to safeguard the validity, integrity, and confidentiality of data is known as cryptography. In the realm of blockchain technology, the use of cryptography has grown in significance during the past several years.

The generation of hashes is a crucial use of cryptography in blockchain. A hash is a distinctive, predetermined string of characters that is created from the data contained in a transaction. Each new block of transactions in a blockchain contains a hash that is obtained from the one before it. Because every effort to change a previous transaction would result in a different hash being generated, this establishes a tamper-proof, chronological record of all transactions on the blockchain.

Many blockchain networks use consensus procedures, and these mechanisms incorporate cryptography. Consensus mechanisms are methods that enable the network to agree on the state of the blockchain at any given time, guaranteeing that each node has the same information.

In order to confirm the validity of transactions and stop hostile parties from tampering with the blockchain, these systems frequently rely on cryptographic techniques like proof-of-work or proof-of-stake.

Therefore, cryptography is an essential part of blockchain technology. Cryptography enables the secure and open movement of digital assets on a decentralized, distributed ledger through the use of digital signatures, hashes, and consensus procedures. The significance of cryptography in maintaining the integrity of this system will only rise as the use of blockchain technology expands. We will examine the function of cryptography in blockchain technology and go over some of its many uses in this essay.

II. BASIC THEORY

A. Modulo Arithmetic

The mathematical process known as modulo arithmetic is used to determine the remaining amount in a division issue. For instance, the outcome of the formula "5 mod 3" would be 2, as 2 is the leftover when 5 is divided by 3. Calculations and comparisons are frequently done in computer programming using modulo arithmetic. It is a fundamental mathematical procedure that is utilized in a wide range of disciplines, such as computer science and cryptography. The definition of modulo arithmetic is as follows:

"If a, q, r, and m are integers, with $m > 0$, the operation a mod m (read: a modulo m) gives the remainder r. So that $a = mq + r$, with $0 \leq r < m$." [2]

Both of these integers are referred to as "congruent" if they both have the same amount of remainder. Congruence is denoted by the symbol (≡) and has the following meaning.

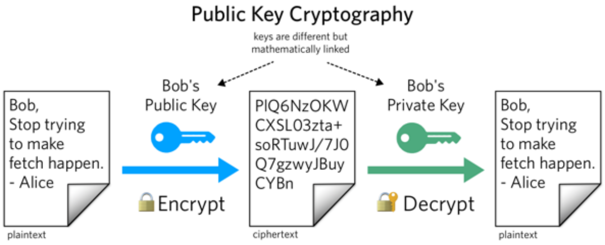
"If a, b, and m are integers, with $m>0$. a is said to be congruent with b ($a \equiv b \pmod{m}$), if and only if m is divisible by a-b ($m|a-b$)". [2]

We also need to comprehend the concepts of prime numbers and "relatively prime." In order to create a public key and a private key in a security system, these two ideas will be crucial. A prime number is one that can only be divided by one (1) and by itself, while a relative prime number is one that meets the following criteria.

"Two numbers can be said to be relatively prime, that is, if a and b are integers and if GCD(a, b) = 1 (GCD is Greatest Common Divider)". [2]

B. Cryptography

Information is encrypted and decrypted using mathematical methods in the art of cryptography to prevent unauthorized access. These methods encrypt messages using mathematical formulas so that only a person with the right key can decipher them. To prevent sensitive information from being accessed by unauthorized people or groups, cryptography is utilized in a variety of domains, including computer science, engineering, and national defense.


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Encrypt
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

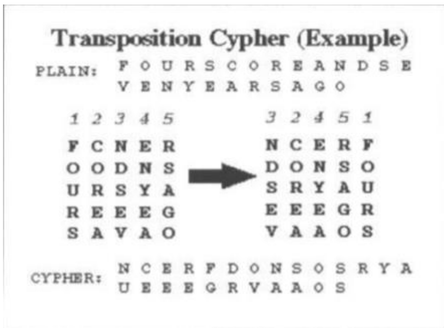
Picture 1. Illustration of encryption and decryption
https://www.twilio.com/blog/what-is-public-key-cryptography

Numerous cryptographic techniques have been used since Julius Caesar was still alive. Caesar developed a straightforward cryptographic technique in which each letter of the alphabet is moved n times to the right, where n is a number. Consider the following as an illustration if n equals 5.

Plain text : SEJARAH KRIPTOGRAFI
ciphertext : XJOFWFM PWNUYTLWFJN

"Transposition Cipher" and "XOR Cipher" are two other fundamental cryptography techniques. Transposition ciphers are a type of encryption where the ciphertext is produced by rearranging the letters of the plaintext message. There are several ways to accomplish this, such as putting the message in a grid and then reading the ciphertext off in a different order, or by employing a secret keyword to jumble the message's letters.

While The XOR cipher is a straightforward symmetric-key cipher that creates the ciphertext by combining the plaintext with a secret key using the XOR (exclusive OR) operator. Although it can offer a moderate level of protection and is reasonably simple to deploy, it is not thought to be extremely secure.



Transposition Cypher (Example)

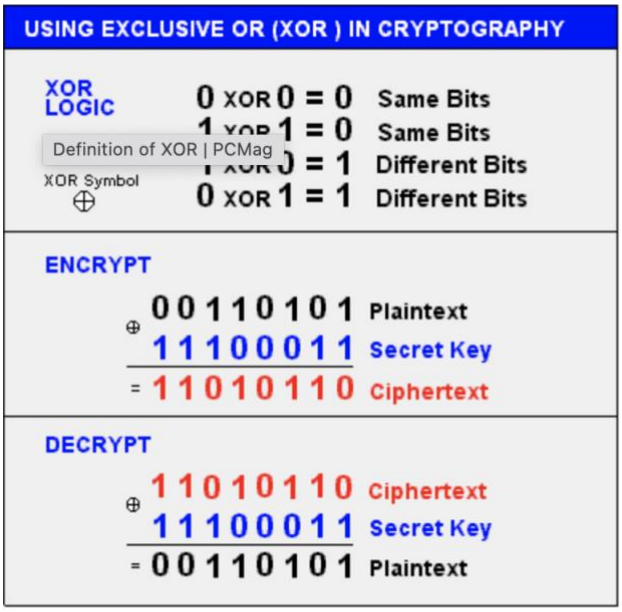
PLAIN: F O U R S C O R E A N D S E
V E N Y E A R S A G O

1	2	3	4	5
F	C	N	E	R
O	O	D	N	S
U	R	S	Y	A
R	E	E	E	G
S	A	V	A	O

3	2	4	5	1
N	C	E	R	F
D	O	N	S	O
S	R	Y	A	U
E	E	E	G	R
V	A	A	O	S

CYPHER: N C E R F D O N S O S R Y A
U E E E G R V A A O S

Picture 2. Transposition Ciphers
http://bestcodes.weebly.com/transposition-cipher.html



USING EXCLUSIVE OR (XOR) IN CRYPTOGRAPHY

XOR LOGIC

0 XOR 0 = 0 Same Bits
1 XOR 1 = 0 Same Bits
1 XOR 0 = 1 Different Bits
0 XOR 1 = 1 Different Bits

Definition of XOR | PCMag

XOR Symbol ⊕

ENCRYPT

```
  00110101 Plaintext
⊕ 11100011 Secret Key
= 11010110 Ciphertext
```

DECRYPT

```
  11010110 Ciphertext
⊕ 11100011 Secret Key
= 00110101 Plaintext
```

Picture 3. XOR Cipher
https://www.pcmag.com/encyclopedia/term/xor

As time goes by, computer-based cryptography techniques get increasingly complex. Writing algorithms and protocols in a programming language, then utilizing computers to execute tests and simulations to ensure the security and effectiveness of the procedures, is what this entails. The approaches can be used in the nodes, consensus algorithm, and smart contracts, among other parts of the blockchain network, once they have been developed and tested. As a result, the network can operate safely and effectively.

Although the cryptography techniques employed in blockchain aren't particularly complicated in and of itself, the context in which they are used can be. This is due to the fact that blockchain technology includes a wide range of diverse elements and procedures, including distributed ledger technology, consensus mechanisms, and smart contracts, all of which depend on cryptography to operate safely. As a result, a blockchain network's overall cryptographic design may be highly intricate and advanced. Among the primary cryptography techniques employed in blockchain are:

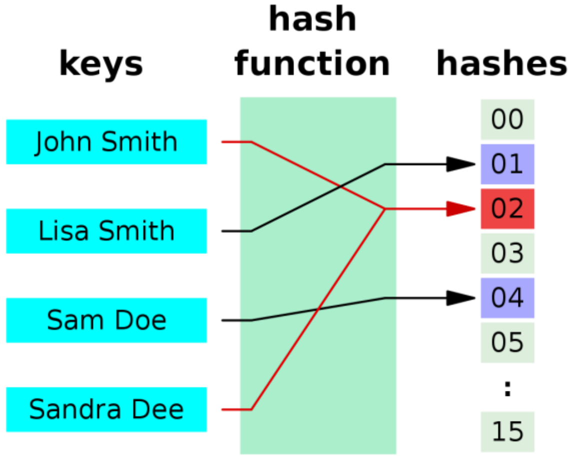
- Public-key cryptography: This method of encryption encrypts and decrypts data using a set of two keys, a public key and a private key.
- Hashing: Hashing is a cryptographic method for converting data of any size into an output of a specific size. Each block of data on the network is given a distinct fingerprint via hashing in the context of blockchain.
- Proof of work (PoW): Proof of work is a consensus-building technique that involves asking users to solve challenging arithmetic problems in order to validate transactions and add new blocks to the network.
- Zero-knowledge proofs: A sort of cryptographic protocol called zero-knowledge proofs enables one party to demonstrate to another that they are aware of

a piece of information without disclosing the information itself. Zero-knowledge proofs are used in the context of blockchain to enable private transactions on the network without disclosing the specifics of the transaction to the public.

The data on the network is secured and protected using encryption, which is a crucial part of blockchain technology.

C. Hashing

Hashing is a common method used in blockchain technology for transaction security and data integrity protection. Applying a mathematical function on a piece of data, such as a transaction, results in a "hash," a fixed-size output. Since the generated hash is specific to the original data, any changes to the input will affect the generated hash.



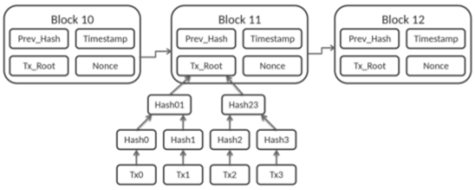
Picture 4. How hashing works in general
https://en.wikipedia.org/wiki/Hash_function

There are numerous hashing techniques; the following are a few examples:

- CryptoNight: a hash function used in several cryptocurrencies as proof-of-work (PoW).
- Equihash: a PoW hashing algorithm made to withstand mining with specialist equipment.
- SHA-256: This algorithm, a member of the SHA family, is a mainstay of blockchain technology.
- Scrypt: This password-based key derivation function is made to be challenging to compute, protecting it from brute-force assaults.

D. Blockchain

A blockchain is a type of distributed database that allows for the secure, transparent and decentralized storage and transfer of data. It is a digital ledger of transactions that is maintained by a network of computers, rather than a single central authority.



Picture 5. A Visualization of whats inside a blockchain
https://id.wikipedia.org/wiki/Rantai_blok#/media/Berkas:Bitcoin_Block_Data.svg

Each member of the network has a unique copy of the ledger, which is continuously updated when transactions are completed. Strong cryptography is used to protect the ledger, and a consensus method is used by the network to verify transactions. This guarantees the accuracy, immutability, and auditability of the data stored on the blockchain.

III. BLOCKCHAIN MECHANISM

A. Creating a Blockchain

The first stage in creating a new blockchain is deciding on the objectives and aims of the blockchain as well as the particular policies and protocols that will control it.

The technical architecture of the blockchain, which includes the data structure, consensus algorithm, and other important elements, must then be designed and put into practice.

The blockchain has to be filled with initial data and transactions once the technological architecture is in place. Pre-mining some blocks and adding them to the blockchain may be included in this, as well as enabling users to start conducting transactions on the network.

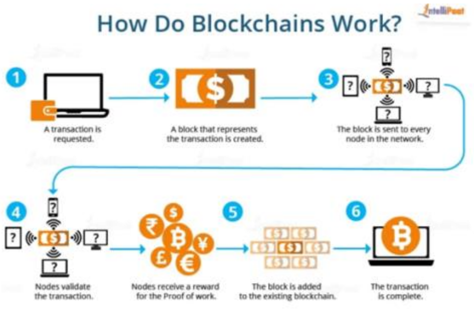
After then, users must be able to access the blockchain, either by having it deployed on a public network or by having access to a private network.

To preserve its usefulness and security, the blockchain needs to be continually updated and maintained.

This can entail introducing new features, updating the program, and fixing any emerging technical problems.

B. How Blockchain works

Blockchain is a distributed database system that enables safe and open transaction recording. Here is a step-by-step breakdown of the procedure.



How Do Blockchains Work?
IntelliPaat
1
A transaction is requested.
2
A block that represents the transaction is created.
3
The block is sent to every node in the network.
4
Nodes validate the transaction.
Nodes receive a reward for the Proof of work.
5
The block is added to the existing blockchain.
6
The transaction is complete.

Picture 6. How blockchains work
https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/

A user who wishes to send money to another user on the network starts a transaction.

Several nodes across the network verify the transaction after it is broadcast to the entire network (computers on the network). The user's digital signature, which is generated using the user's private key, is examined by the nodes to confirm the transaction. By doing this, it is ensured that the transaction is genuine and unaltered.

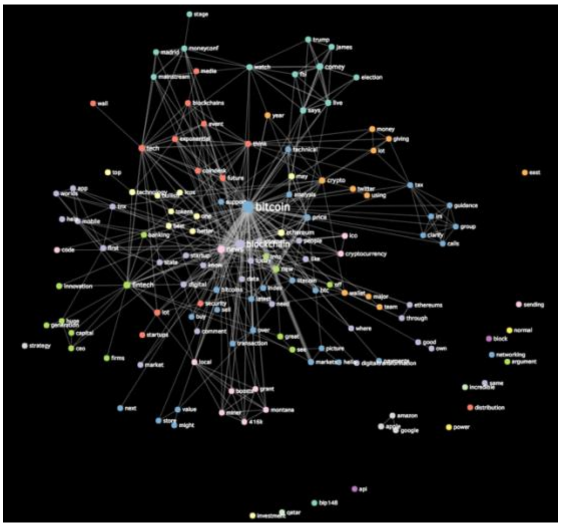
The transaction is added to a block of transactions after it has been validated, along with a special hash (a combination of numbers and letters) that uniquely identifies the block and the transactions it holds.

The block is subsequently included in the blockchain, a distributed database that keeps track of all network transactions.

The blockchain produces a secure and unchangeable chain of blocks because each block has a distinct hash and the hash of the one before it. As a result, it is impossible to change a block's contents without also breaking the chain, which the network would quickly notice.

The blockchain's use of encryption maintains the network's security and integrity and permits the secure exchange of information between parties without the need for a central authority or middleman.

In general, the use of blockchain technology enables the establishment of decentralized and trust-free networks by allowing for the secure and transparent recording of transactions.



Picture 7. A visual representation of a blockchain
https://datalion.com/blockchain-bitcoin-visualizations/

C. How Cryptography is used in blockchain

The process of adding a transaction to the blockchain involves the usage of encryption at several points. Here is how each step uses it:

A user's private key is used to generate a digital signature for a transaction when they start it. The transaction's signature is attached to it and is used to confirm the transaction's legitimacy.

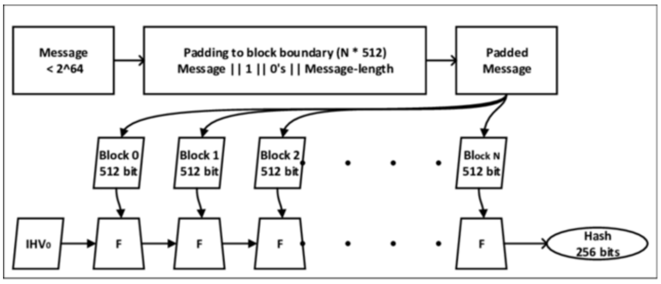
The nodes employ the user's digital signature to validate the transaction when it is broadcast to the network. This makes it easier to verify that the transaction is real and unaltered.

When a transaction is included in a block, a special hash is generated for the block using cryptographic algorithms.

The block and the transactions it contains are identified by this hash. The hash of the block before it on the chain is included when the block is added to the blockchain. With no way to break the chain, this results in a safe and immutable chain of blocks.

D. How the SHA-256 hashing method works

We'll use the hashing algorithm SHA-256 as an illustration. A SHA-256 cryptographic hash function is frequently employed to check the accuracy of data. It is a mathematical process that converts data of any size into a hash, which is a fixed-length bit string. A 256-bit (32-byte) hash value is what the SHA-256 algorithm produces as its result. We'll first go over how SHA-256 functions step by step before explaining how hashing is employed on the blockchain.



Picture 8. SHA-256 Scheme
https://www.researchgate.net/figure/General-architecture-to-compute-the-SHA-256-hash-function_fig1_335095939

A message is used as the input for the SHA-256 algorithm, which then applies a series of mathematical operations to create a fixed-size output known as a hash. The precise steps in this method are listed below.

The length of the input message is padded to be a multiple of a given value (usually a power of 2). This guarantees that the algorithm processes the complete message.

After then, blocks of a predetermined size are created from the padded message (usually 512 bits).

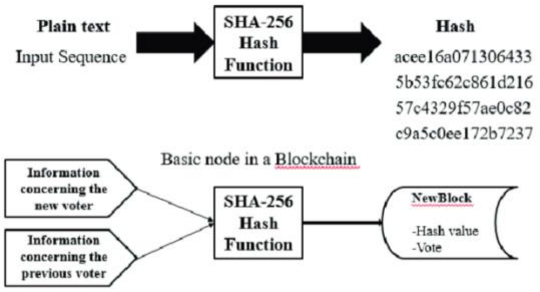
A sequence of logical and mathematical operations are used to process each block, each of which is intended to yield a distinct output for any potential input.

A mathematical formula known as a compression function is then used to combine the output of each block with the output of the preceding block.

Every block in the message goes through this process again. The hash value is the algorithm's ultimate output after all of the blocks have been processed.

This number has a fixed length of 256 bits and is commonly represented as a series of hexadecimal digits (32 bytes).

E. How the SHA-256 hashing method works in blockchain



Picture 9. SHA-256 in blockchain
https://www.researchgate.net/figure/SHA-256-Algorithm-Working_fig1_343285210

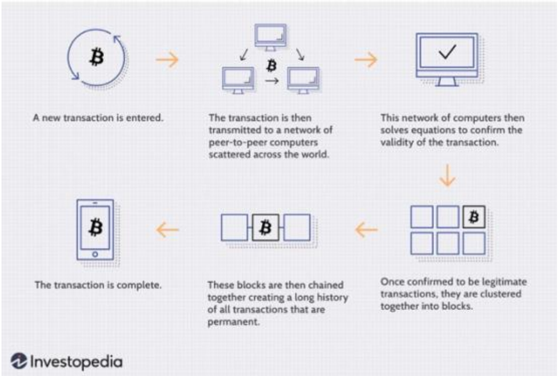
The SHA-256 method is used to hash the data included in a newly formed block. The block and the transactions it contains are identified by this distinctive and irreversible representation of the data.

The SHA-256 hash of the block's data and the hash of the preceding block in the chain are both included in the block when it is added to the blockchain. With no way to break the chain, this results in a safe and immutable chain of blocks.

The blockchain uses the SHA-256 hashing algorithm, which makes it difficult to change the data in a block without disrupting the chain, to help ensure the security and integrity of the network.

E. Applications of blockchain

One of the most well-known uses of blockchain technology is for the creation and use of digital currencies, such as Bitcoin.



A new transaction is entered.

The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.

This network of computers then solves equations to confirm the validity of the transaction.

Once confirmed to be legitimate transactions, they are clustered together into blocks.

These blocks are then chained together creating a long history of all transactions that are permanent.

The transaction is complete.

Picture 10. Infographic about blockchain in bitcoin
https://www.investopedia.com/terms/b/blockchain.asp

Here are some other ways that blockchain technology is being used:

- Digital currencies: The technology behind many digital currencies, including Bitcoin, Litecoin, and Ethereum, is called blockchain.
- Financial transactions: Using blockchain, financial transactions may be made faster and more securely.
- Healthcare: Blockchain has potential applications in the healthcare sector, including the safe storage and exchange of patient data.
- Real estate: Blockchain could be used in the real estate industry to track property ownership and transactions.
- Voting systems: The usage of blockchain in voting systems could result in a more transparent and secure voting procedure.
- Identity management: A decentralized system for managing digital identities might be developed using blockchain technology.
- File storage: Blockchain technology offers the possibility of a decentralized, secure method of file storage.

In conclusion, blockchain has numerous potential applications across numerous industries. It is utilized for supply chain management and digital currencies, and it may also be applied to voting systems, real estate, and the healthcare industry. There will probably be even more applications for blockchain as the technology develops..

IV. CONCLUSION

Hashing and cryptography are crucial ideas in the world of blockchain technology. Hashing is the technique of giving data a unique digital fingerprint, whereas cryptography is the discipline of utilizing mathematical procedures to encrypt and safeguard data. These technologies are applied to blockchain in order to secure transactions and safeguard the accuracy of the ledger.

Digital signatures are made possible by cryptography and are used to verify the parties to a transaction and thwart fraud. Data is represented uniquely and irreversibly via hashing, which is then saved in blocks on the blockchain. This guarantees that the data on the blockchain is safe and cannot be altered.

Overall, the usage of encryption and hashing helps to secure the security and integrity of the blockchain. They are crucial parts of blockchain technology.

V. THANK-YOU NOTE

I want to thank Allah SWT, his grace and guidance has helped me throughout the process of writing this paper, and thankfully complete it on time. I want to also thank all of the lecturers, Mr Rinaldi, Ms. Fariska, Ms. Nur Ulfa, for teaching the course, thus helping me to be able to write this paper. I want to finally thank all of my family and friends for all of their support all this time.

REFERENCE

[1] *Rosen, Kenneth H. Discrete Mathematics andIts Applications, 7th Edition.*

[2] Munir, Rinaldi. *Teori Bilangan* (2022). Accessed in 9th of December 2022, from https://informatika.stei.itb.ac.id/~rinaldi.munir/Mat dis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf

[3] Raj, Roshan. How Does Blockchain Work? (2022). Accessed in 9th of December 2022, from https://intellipaat.com/blog/tutorial/blockchain- tutorial/how-does-blockchain-work/

[4] *Simplilearn. Blockchain In 7 Minutes* (2019). Accessed in 9th of December 2022, from https://www.youtube.com/watch?v=yubzJw0uiE4

[5] guptavivek0503. Cryptography in Blockchain (2022). Accessed in 9th of December 2022, from https://www.geeksforgeeks.org/cryptography-in-blockchain/#:~:text=Cryptography%20is%20a%20method%20of,main%20concepts%20cryptography%20and%20hashing.

[6] *Bitstamp. How Does Hashing Work?* (2022). Accessed in 9th of December 2022, from https://www.bitstamp.net/learn/blockchain/how- does-hashing-work/

[7] *BybitLearn. Explained: What is Hashing in Blockchain?* (2020). Accessed in 9th of December 2022,from https://learn.bybit.com/blockchain/what- is-hashing-in-blockchain/

STATEMENT

I hereby declare that the paper I am writing is my own writing, not an adaptation or translation of someone else's paper, and not plagiarism.

Bandung, 10th of December 2022

Ariel Jovananda 13521086