**BACKGROUND OF THE STUDY**

**Introduction**

**HISTORY OF BLOCKCHAIN TECHNOLOGY**

Blockchain technology has revolutionized transactions and data management, garnering significant attention and impact in recent years. Its roots can be traced back to the late 1980s and early 1990s with the introduction of consensus models and electronic ledgers.

The concept was expanded upon by Satoshi Nakamoto in 2009 and was then used to create the cryptocurrency Bitcoin. Shortly after the Global Financial Crisis that happened in the same year, Bitcoin's introduction and the idea to utilize cryptocurrencies or digital cash efficiently addressed the problem of double-spending, opening up opportunities for the widespread adoption of blockchain technology.

Blockchain technology continuously evolves and demonstrates immense potential, with its fundamental properties of security, immutability, and decentralization proving valuable in various industries, particularly in cryptocurrencies like Bitcoin and Ethereum. It acts as the foundational framework for modern cryptocurrencies and a transformative force in the finance, supply chain, and healthcare sectors.

The impact of blockchain technology has reached the shores of the Philippines, driving remarkable growth, economic advancement, and innovation within the country. In 2017, Bitcoin, the first decentralized cryptocurrency, became popular in the Philippines (England, 2021).

The rise of blockchain, coupled with the COVID-19 pandemic, has intensified interest in Bitcoin as an investment. Additionally, Filipino individuals have discovered new income opportunities through games like Axie Infinity, where they can earn money through digital wallets and NFTs.

Investment opportunities and guilds have thrived within Axie Infinity to meet the growing demand. These guilds offer scholarships to players who cannot afford in-game creatures (Axies) in exchange for a portion of their earnings. This trend showcases the employment and economic potential of blockchain-based NFTs and games.

Moreover, Bitcoin trading and cryptocurrency transactions in the Philippines have exceeded previous records, indicating significant demand for digital assets and reflecting the rising interest in cryptocurrency. The country's central bank, the Bangko Sentral ng Pilipinas (BSP), recognizes cryptocurrencies as legitimate payment methods, issuing guidelines for virtual currency exchanges and embracing blockchain technology. The BSP plans to launch a wholesale central bank digital currency (CBDC) project to enhance domestic and cross-border payments and contribute to economic recovery.

The adoption of blockchain technology and cryptocurrencies are expected to grow in the Philippines as individuals explore their potential applications within the country's financial infrastructure (Ta-asan, 2022).

**WHAT IS BLOCKCHAIN?**

The blockchain serves as the underlying technology for trading cryptocurrencies and NFTs. It operates as a distributed database spread across interconnected computers, allowing the recording of different types of information like *cryptocurrency transactions*, *NFT ownership*, and *DeFi smart contracts.* It is a decentralized *digital ledger*, securely recording and verifying transactions across multiple computers or nodes (Ta-asan, 2022). Described as a collection of interconnected records, blockchain is highly resistant to alteration and protected using *cryptography.* It functions as a chain composed of individual blocks of data. Each transaction is recorded as a block, ensuring the integrity of the information.

1. **BLOCKCHAIN ARCHITECTURE**

**1.1 Decentralization**

In traditional centralized systems, transactions are validated by a central authority, which can be costly and lead to performance issues. However, in blockchain, no central authority is required. Instead, a decentralized network of participants uses consensus algorithms to maintain data integrity and stability.

**1.2 Persistency**

Valid transactions are swiftly verified and cannot be deleted or reversed once included in the blockchain. Invalid transactions are rejected, preventing them from propagating further within the network.

**1.3 Anonymity**

Blockchain allows users to interact using generated addresses, preserving their privacy by not revealing their real identities. However, it is essential to note that blockchain does not provide absolute privacy due to the permanent nature of the recorded transactions.

**1.4 Auditability**

Blockchain stores user data using the *Unspent Transaction Output (UTXO) model.* Each transaction references previous unspent transactions, and once a transaction is recorded, the referenced outputs transition from unspent to spent. This enables easy tracking and prevents double-spending.

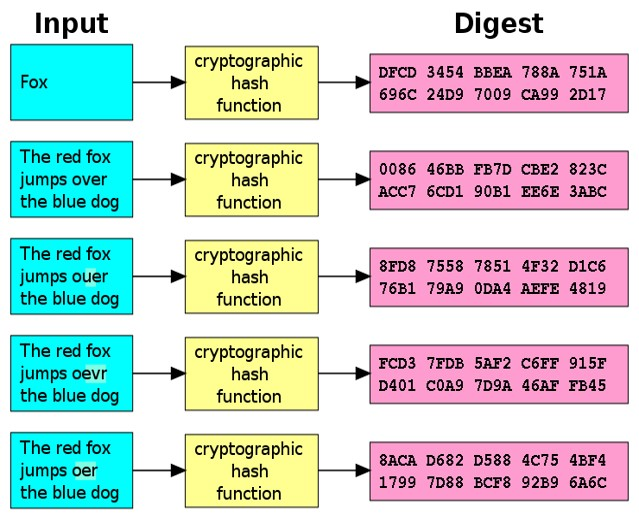
**1.5 Transparency**

Blockchain operates on a transparent system similar to cryptocurrencies like *Bitcoin*. Transactions are associated with addresses, ensuring transparency of the transaction history. While personal identities are hidden for security reasons, the owner of a block's address is responsible for the associated transactions.

**1.6 Cryptography**

Security is a fundamental aspect of blockchain, and it achieves this through *cryptography.* *Encryption* techniques, such as ciphers and cipher text, are employed to safeguard the data stored in blockchain blocks, ensuring the integrity and confidentiality of the information.

A *cryptographic hash function* is utilized to enhance the blockchain's security. This function is crucial in protecting the data stored within blockchain blocks. It converts the information into a fixed-length string of characters known as a *hash*, representing the input data. This distinct output is also called a message digest or simply digest.

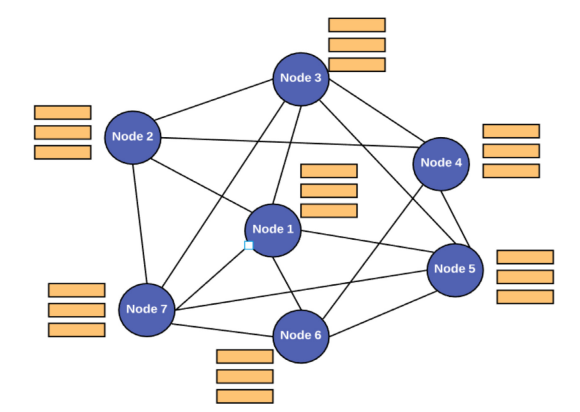


*Figure 1:  Illustrations of how cryptography works*

1. **CORE COMPONENTS OF BLOCKCHAIN ARCHITECTURE**

**2.1 Node**

Nodes are participants in the blockchain network, and their devices enable them to maintain and communicate with the distributed ledger. Nodes serve as communication hubs and share information with other nodes in the network. When a *miner* adds a new block to the blockchain, it is broadcasted to all network nodes.



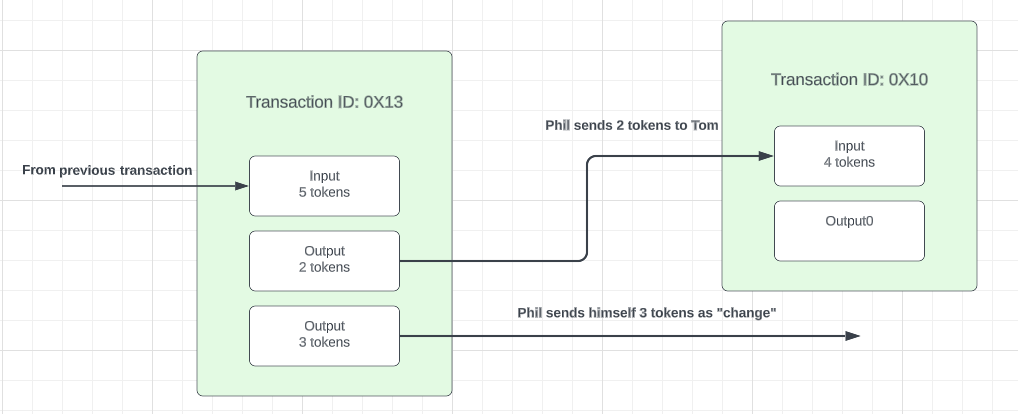
*Figure 2: Node Connection, as demonstrated by Mohanta et al.*

**2.2 Transactions**

Transactions represent agreements or contracts that involve the transfer of assets, such as cash or property, between parties. The blockchain network stores transactional data as copies in a digital ledger, ensuring transparency and immutability.

**Ledgers:** Ledgers in blockchain refer to the distributed and decentralized databases that store and maintain records of transactions. Ledgers provide transparency and immutability by ensuring all participants access the same information.

For instance, consider a group of friends gathering to eat at a restaurant. When it is time to pay the bill, one person volunteers to cover the entire amount. Afterward, the friends split the bill and used cryptocurrency to settle the expenses. In this scenario, the two friends who owe money send two tokens each to the person who paid the bill. In cryptocurrency transactions, the input consists of the cryptocurrencies owned by each participant, along with the specific amount they are sending to cover their share of the bill. The output of the transactions would be the updated cryptocurrency balances for each participant, reflecting the transfer of tokens from the friends who owed money to the person who paid the bill.



*Figure 3: P2P transaction between the two participants*

**2.3 Block**

Blocks are fundamental units in a blockchain network, functioning as links in a chain. In cryptocurrencies, blocks store transaction records, which are encrypted into a hash tree structure. With many daily transactions, the block structure allows users to track and organize these transactions efficiently.

A block in a blockchain consists of several components:

**Header:** The header is like an ID card for a block in the blockchain. It contains essential information about the block and is used to identify it uniquely. Miners periodically change a *nonce value* in the header and hash it to find a valid block.

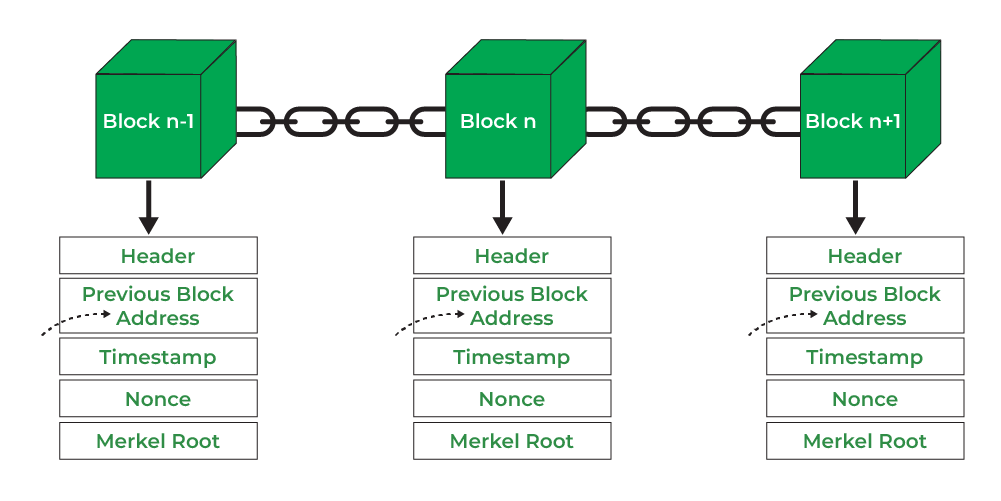
**Previous Block Address/Hash:** This is like a chain that connects blocks. Each block contains a reference to the previous block's hash in the chain. It helps maintain the order and integrity of the blockchain.

**Timestamp:** The timestamp is like a timestamp on a document. It indicates the exact time and date when a block is created. It helps ensure the chronological order of events in the blockchain.

**Nonce:** A nonce is a unique number that is used only once. It plays a role in the proof-of-work process of mining a block. When combined with other block data, miners test different nonce values to find one that produces a hash value that meets specific criteria.

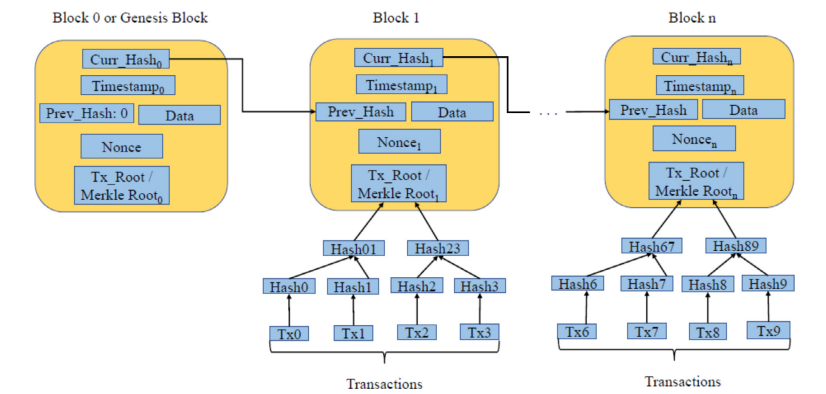
**Merkle Root:** The Merkle root summarizes all the transactions in a block. It is calculated by creating a digital fingerprint (block hash) of each transaction and combining them in a specific way. The Merkle root allows users to verify the integrity of transactions and determine if they belong to a particular block.

The block inherits the previous hash, and the blockchain system uses this previous hash to create new blocks. This makes the blockchain tamper-proof. Mining statistics is the various metrics and data. Mining statistics in blockchain provide data on the mining process. Miners create and validate blocks using complex algorithms, making them tamper-proof. The statistics include hash rate, difficulty, rewards, block time, and mining power distribution.



*Figure 4: Attributes of a Blockchain from GeeksforGeeks*

The Merkle Root generates the different block Hash within a blockchain. Modifying a transaction would require altering all subsequent block hashes. The level of difficulty in the mining algorithm determines the degree of tamper resistance in a blockchain block. A higher difficulty makes it more challenging to manipulate the block's contents, thereby enhancing the security of the blockchain.



*Figure 5: The Merkle Root, as demonstrated by Mohanta et al.*

**2.4 Chain**

The chain refers to the corresponding sequence of blocks in the blockchain network. Blocks are linked using the previous block's hash, creating a chain-like structure. This chaining mechanism ensures the integrity and chronological order of transactions in the blockchain.

**2.5 Miners**

Miners are individuals or entities involved in the process of blockchain mining. Mining involves validating transactions and adding them to the blockchain. Transactions typically need to be approved by miners before they are considered valid and added to the blockchain. The process of approving transactions is often referred to as transaction validation or consensus. Miners perform complex computational tasks to verify transactions and maintain the security and integrity of the blockchain network.

**2.6 Consensus**

Consensus mechanisms are fault-tolerant mechanisms used in computer and blockchain systems to achieve agreement on the network's state. In cryptocurrencies, consensus ensures agreement on transaction validity and the order of transactions across the distributed network. Miners or validators compete to solve complex mathematical puzzles or stake their coins to secure the network. This process ensures that only valid transactions are added to the blockchain.

1. **TYPES OF BLOCKCHAIN**

**3.1 Public Blockchain**

A public blockchain is an open network in which anyone can participate. It is decentralized and transparent, allowing anyone to read, write, and audit the blockchain's activities. It cannot be modified once data is validated on the public blockchain. It is accessible to everyone, and no permission is required to join or access the network.

**3.2 Private Blockchain**

A private blockchain requires permission to access. It operates based on controlled participation, limiting access to specific entities. Only authorized participants know transactions, and outsiders cannot access the blockchain. A single entity manages private blockchains, and the entity controls access rights. There may be restrictions on accessing the network of a private blockchain.

**3.3 Consortium Blockchain**

A consortium blockchain is a permission by a group of organizations or government entities rather than a single entity. It offers a balance between public and private blockchains. Consortium blockchains are more decentralized than private blockchains, enhancing privacy and security. Access to consortium blockchains is limited to the collaborating organizations within the consortium, and external access is not granted. Organizations within the consortium work together collaboratively.

1. **CONSENSUS ALGORITHM**

A consensus algorithm is a mechanism or protocol used in distributed systems to achieve agreement or consensus among multiple participants or nodes. In a distributed system, where multiple nodes need to work together and make collective decisions, consensus algorithms ensure that all nodes agree on a single, consistent state of the system.

**4.1 Proof of Work (PoW)**

Participants (stakeholder nodes) must prove that they have performed a certain amount of computational work to validate transactions and add them to the blockchain.  Miners need to invest computational power by performing numerous calculations until they find a solution (nonce) that satisfies the difficulty requirement. The miner who finds the solution first gets to propose the next block and is rewarded with newly minted cryptocurrency or transaction fees. The security of the blockchain is based on the majority of miners being honest and the overall computational power of the network.

**4.2 Proof of Stake (PoS)**

Participants are chosen to validate transactions and create new blocks based on their existing  “stake” or coins they hold, reducing the need for extensive computational work (mining).  The security of PoS blockchains depends on the economic incentives of validators, as they risk losing their stacked coins if they act maliciously.

**4.3 Proof of Capacity (PoC)**

Proof of Capacity involves sharing the available memory space of nodes in the blockchain network. Participants allocate storage space in advance to demonstrate their eligibility to validate transactions and create blocks. This approach reduces energy consumption compared to PoW.

**4.4 Proof of Elapsed Time (PoET)**

A consensus algorithm that uses cryptography to determine the time duration for each participant to take turns in validating transactions and adding them to the blockchain. It aims to achieve agreement and fairness among participants without requiring extensive computational resources.

**4.5 Delegated Proof of Stake (DPoS)**

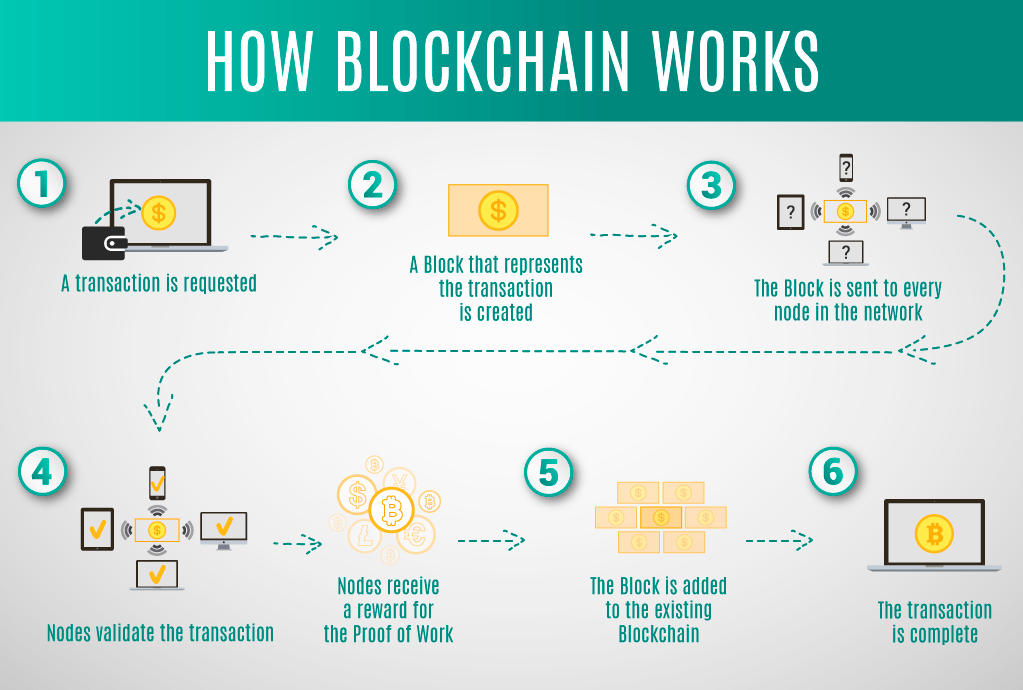
A consensus algorithm is used in blockchain networks where delegates are selected through a voting process to validate data blocks. These delegates, also known as block producers or witnesses, maintain the blockchain's integrity.

**4.6 Practical Byzantine Fault Tolerance (PBFT)**

A consensus algorithm ensures that computers in a network reach agreements, even in the presence of faulty or malicious computers. It allows the network to function correctly despite computers not working properly or attempting deception. PBFT employs a voting system where computers vote on decisions, and the majority's decision is accepted. This algorithm ensures reliable network operation and problem-handling capabilities.

**HOW BLOCKCHAIN WORKS?**

In Blockchain technology, when a transaction occurs, the record is created in the form of blocks, which permanently contain all the transaction details. These blocks form a chain of records called a ledger, shared among the participants, acting as a publicly distributed ledger. The information in each block is encrypted using an encryption algorithm, resulting in a unique hash. This hash is included in the following block, forming a chained block series.



*Figure 6: Blockchain Flow*

To better understand blockchain technology, envision a shared spreadsheet representing the blockchain itself. Participants can contribute transactions to the spreadsheet, which serves as recorded data within the blockchain. Each transaction undergoes transformation through cryptographic hash functions, ensuring integrity and authenticity.

Before adding a transaction, a participant supplies a nonce for security and attaches a digital signature using their private key to validate their identity. Other participants use public keys to verify the signature, and unique addresses derived from public keys identify senders and receivers in recorded transactions.

Private keys must be carefully safeguarded, similar to personal passwords or encryption keys, as losing them results in losing access to associated addresses and transactions.

The shared spreadsheet operates as a ledger, meticulously documenting all recorded transactions and serving as a distributed and synchronized database accessible to all participants.

Multiple transactions are consolidated into blocks to organize transactions, and each block references the preceding one, creating a chain-like structure. This chaining mechanism ensures the integrity and immutability of recorded transactions within the shared spreadsheet.

**Objectives**

Blockchain technology is a revolutionary concept that has grown in popularity in recent years. It is a decentralized and distributed digital ledger that records transactions in a safe and transparent manner. Our research goals include the following:

* To discuss the History of blockchain technology, how it works, its uses and its function.
* Determine its importance in different areas of Blockchain technology especially on Crypto and NFT.
* Observe the blockchain technology by discussing its current state in the Philippines,  popular cryptocurrency, rules and regulations, trends and emerging technologies.
* Analyze blockchain technology using various statistics and research.
* Evaluate blockchain technology through case reports, its effects and benefits.