**VIETNAM – KOREA UNIVERSITY OF INFORMATION AND**

**COMMUNICATION TECHNOLOGY**

**THE FACULTY OF COMPUTER SCIENCE**



**GRADUATE PROJECT**

**Applying Blockchain to build**

**computer business management system**

Student : **TRAN KHAC TUAN**

Lecturer : **PhD. NGUYEN QUANG VU**

Class : **17IT2**

***Da Nang, October 2021***

**VIETNAM – KOREA UNIVERSITY OF INFORMATION AND**

**COMMUNICATION TECHNOLOGY**

**THE FACULTY OF COMPUTER SCIENCE**

**GRADUATE PROJECT**

**Applying Blockchain to build**

**computer business management system**

***Da Nang, October 2021***

**INTRODUCTION**

Size 13

**ACKNOWLEDGEMENT**

Size 13

**MAKING RECOMMENDATIONS**

Size 13

**CONTENT**

Page

ACKNOWLEDGEMENT 1

[Chapter 1 Blockchain overview 1](#_Toc85911241)

[1.1 History of blockchain 1](#_Toc85911242)

[1.1.1 Blockchain overview 1](#_Toc85911243)

[1.1.2 Blockchain types 2](#_Toc85911244)

[1.2 Blockchain technology 4](#_Toc85911245)

[1.2.1 Blocks 4](#_Toc85911246)

[1.2.2 Hash algorithm 4](#_Toc85911247)

[1.2.3 Smart contracts 6](#_Toc85911248)

[1.2.4 Bitcoin 7](#_Toc85911249)

[1.2.5 Digital signatures in blockchain 8](#_Toc85911250)

[1.2.6 Consensus Mechanism 9](#_Toc85911251)

[1.3 Techniques applied in blockchain 13](#_Toc85911252)

[1.3.1 Decentralized consensus 13](#_Toc85911253)

[1.3.2 Distributed database 14](#_Toc85911254)

[1.3.3 Distributed ledger 16](#_Toc85911255)

[1.3.4 Data distributed 17](#_Toc85911256)

[Chapter 2 E-commerce problem analysis 19](#_Toc85911257)

[Chapter 3 Deploy and build the system 20](#_Toc85911258)

[Chapter 4 Conclusion and development direction 21](#_Toc85911259)

REFERENCES 130

**LIST OF TABLES**

Page

**LIST OF IMAGES**

Page

[Figure 1‑1. Hash function (source) 6](#_Toc84710793)

[Figure 1‑2. Linking between two blocks (source) 6](#_Toc84710794)

[Figure 1‑3. Blockchain structure (source) 7](#_Toc84710795)

**LIST OF ACRONYMS**

|  |  |  |
| --- | --- | --- |
| **#** | **Phrase** | **Abbreviation** |
| 1 | Bitcoin | BTC |
| 2 | The Elliptic Curve Digital Signature Algorithm | CNPM |
| 3 | Distributed database management system | DDBMS |
| 4 | Elliptic Curve Digital Signature Algorithm | ECDSA |
| 5 | Graphical user interface | GUI |
| 6 | Internet Protocol | IP |
| 7 | Personal computers | PCs |
| 8 | Proof of Activity | PoA |
| 9 | Proof of Burn | PoB |
| 10 | Proof of Capacity | PoC |
| 11 | Proof of Elapsed Time | PoET |
| 12 | Proof of Stake | PoS |
| 13 | Proof of Work | PoW |
| 14 | Revest-Shamir-Adleman | RSA |
| 15 | Secure hashing algorithm | SHA |
| 16 | Transmission Control Protocol | TCP |
|  |  |  |
|  |  |  |
|  |  |  |

# **Chapter 1** Blockchain overview

## History of blockchain

### **Blockchain overview**

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. It’s also described as a “trustless and fully decentralized peer-to-peer immutable data storage” [1][2][3][4] that is spread over a network of participants often referred to as nodes.

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation “Computer Systems Established, Maintained, and Trusted by mutually Suspicious Group.” Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stometta [4][6]. They wanted to implement a system wherein document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Markle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block [4][7].

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto importantly improved the design using the Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate with which blocks are added to the chain [4]. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.

Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to the protocol to communicate and validate new blocks. Although blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance [5].

Implementing a solution across multiple companies can be challenging because we need to trust data from a central database. Data is stored in a location as the source of truth. The company that maintains the database must be trusted as the central authority of the data.

Blockchain lets us implement a business process when we need to trust data and participants without using a central database.

Blockchain is a record-keeping and contract-enforcement technology that uses cryptography to make it extremely difficult to change the previous history. It allows participants to share workstreams by tracking changes on a shared ledger.

A block in the blockchain is a cluster of data that stores transaction information. The number of transactions in a block is usually time-based.

Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block reinforced the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchain uses consensus rules to ensure data is consistent across nodes. It also uses cryptography to enable participants to trust the data. Specifically, it prevents any individual participant or minority of participants from modifying history. Since blockchain is decentralized, solutions that can use a decentralized database work best. For example, you have a requirement to support multiple companies with no central authority due to cost, control, or being a single point of failure.

Blockchain uses a consensus mechanism to validate and agree on the data across all blockchain nodes. Consensus provides a way for all decentralized nodes to come to the same state. When transferring value or responsibility, order matters. For example, if we transfer ownership of a car to our friend, we cannot also transfer ownership to a colleague at work. This issue is known as the double-spend problem which consensus solves. Consensus ensures the correct order of transactions and the integrity of the blockchain. As part of the consensus, a group of transactions is validated as a block and the network must agree if the block should be included in the blockchain.

There are several blockchain consensus algorithms including proof of work, poof of stake, and proof of authority. Each algorithm solves consistency on a different way. In simple terms, consensus provides a way for the distributed ledger to come to a common state.

Through consensus, validated blocks are added to the blockchain at each node. Because all nodes have the same blocks in the chain, the ledger is consistent across the network. As a result, all nodes contain the same validated data in an agreed-upon order.

### **Blockchain types**

A blockchain can be public or private. That determines who can participate in the blockchain network.

Public blockchain

In a public blockchain, a user can become a member of the blockchain network. This means they can store, send, and receive data after downloading the required software on their device. Allowing anyone to read and write the data stored on the blockchain as it is accessible to everyone in the world.

A public blockchain is completely decentralized. The permissions to read and write data onto the blockchain are shared equally by all connected users, who come to a consensus before any data is stored on the database. All transactions in the blockchain are visible by any node on the network.

The first blockchain network was created for Bitcoin. The Bitcoin blockchain network is public. All transactions can be viewed by anyone. For example, we can view the latest Bitcoin blocks and transactions using a block explorer.

The consensus algorithms for public blockchain use cryptocurrency as a reward to validate blocks. Public blockchains may also charge a cryptocurrency fee for validating transactions. Public blockchain privacy is limited. If we want to keep our transaction private, we should only share our public key with the other participant in the transaction.

Private blockchain.

A private blockchain is also known as a consortium blockchain. The information stored in the blockchain would only be accessible to participants invited to the blockchain network. Private networks are semi-trusted networks. In a private network, there is an agreement between all participants about how they will leverage the blockchain. The blockchain is governed by a single entity. The participating parties require permission to read, write, or audit the blockchain. The blockchain can have multiple layers of data access to keep certain pieces of data confidential. Private blockchains, therefore, ensure a higher level of security, privacy, and performance. Due to their confidential nature, private blockchains can be designed for specific sectors such as finance and government services. The transactions and data are not publicly visible and can only be accessed by the participating parties.

Private blockchains usually can be adopted in the corporate sector where the details need to be shared only between certain nodes.

A consortium blockchain, also called permission blockchain can be considered as a hybrid model between the low trust offered by public blockchains and the single highly trusted entity model of private blockchains. Instead of allowing any user to participate in the verification of the transaction processor on the other side just allowing one single company to have full control, in a consortium blockchain a few selected parties are predetermined. It only allows a limited number of users the permission to participate in the consensus process.

Some of the benefits of a private blockchain are:

Permissioned blockchain – the consortium controls the resources and access to the blockchain.

Improved privacy – the transactions on the blockchain can only be accessed by permissioned parties.

Increased scalability – enterprises can add and remove nodes on demand.

## Blockchain technology

### **Blocks**

In the blockchain, a block records some or all the most recent transactions that have not yet entered any prior blocks. Thus, a block is like a page of a ledger or record book. Each time a block is ‘completed’, it gives way to the next block in the blockchain. Each block includes the cryptographic hash of the previous block in the blockchain, linking the two. This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks [8].

The current block of any block sequence has a timestamp and is connected to prior blocks by cryptographic hash values. Participating nodes cannot delete a block but can append new ones. The chaining of these blocks results in a shared, distributed database with an immensely growing record of transactions that are irreversible and immutable.

It is difficult for anyone to tamper with block information without other nodes detecting the changes. Unlike the days of centralized ledgers in the custody of a single point of authority, blockchains are essentially decentralized databases that are collaboratively managed by multiple participating entities [14].

Peers supporting the database are known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their database and retransmit the improvement to their peers.

Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks.

### **Hash algorithm**

A hash is a function that meets the encrypted demands needed to solve for a blockchain computation. A hash is developed based on the information present in the block header. It like a nonce or a solution, is the backbone of the blockchain network.

Blockchain uses a cryptographic hash to create link between blocks. By linking blocks, the orders of transactions can be agreed upon through the consensus algorithm. Hashes are fixed length since it makes it nearly impossible to guess the length of the hash if someone was trying to crack the blockchain. If we used a SHA-256 hash function on a 100 pages document, the function output is a 256-bit hash value. If just a character in the document changed and regenerated the hash, the output is a different 256-bit hash value.

Typical hash functions take inputs of variable lengths to return outputs of a fixed length. A cryptographic hash function combines the message-passing capabilities of hash functions with security properties. It is used in computing systems for tasks, such as checking the integrity of messages and authenticating information. While hash functions are considered cryptographically "weak" because they can be solved in polynomial time, but they are not easily decipherable.

Diagram, timeline

Description automatically generated

Figure 1‑1. Hash function ([source](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/3-how-blockchain-works?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development))

Blockchain uses hashes to detect if any changes have been made to the blocks. By including the previous block’s hash value when generating the next block’s hash, blocks are chained together through hashes.

A picture containing diagram

Description automatically generated

Figure 1‑2. Linking between two blocks ([source](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/3-how-blockchain-works?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development))

Blockchain provides trust by using hashes to prove data history hasn’t changed. By including the hash of the previous block when creating a new block, an immutable chain of transactions is created in order. If any block is modified in the chain, the hash of later blocks is different. As a result, validation discovers the discrepancy.

Timeline

Description automatically generated with medium confidence

Figure 1‑3. Blockchain structure ([source](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/3-how-blockchain-works?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development))

### **Smart contracts**

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without an intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

Blockchain-based smart contracts are proposed contracts that can be partially or fully executed or enforced without human interaction [11]. One of the main objectives of a smart contract is automated escrow. A key feature of the smart contract is that they do not need a trusted third party to act as an intermediary between contracting entities – the blockchain network executes the contract on its own.

This may reduce friction between entities when transferring value and could subsequently open the door to a higher level of transaction automation.

A smart contract is a digital program that automates the execution of business logic, obligations, and agreements. Smart contracts work by following simple “if/when...then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to other appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the result.

A smart contract can be used to represent almost anything: an electronic warehouse receipt, a bond, an invoice, a unit of electricity, a unit of currency, a futures contract, a share of risk, and much more. These cryptographically unique assets can be created, traded, and settled in real-time by users on the network

Each smart contract can be written to include almost any type of business logic. This business logic can be enforced automatically in accordance with the terms and conditions of the agreement.

The benefits of smart contracts.

Speed, efficiency, and accuracy – Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there’s no paperwork to process and no time spend reconciling errors that often result from manually filling in documents.

Trust and transparency – Because there’s no third party involved, and because encrypted records of transactions are shared across participants, there’s no need to question whether information has been altered for personal benefit.

Security – Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

Savings – Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays, and fees.

Applications of smart contract: verifying the integrity of messages and files, signature generation and verification, password verification, proof-of-work, file, or data identifier, etc.

### **Bitcoin**

Bitcoin (BTC) is a consensus network that enables a new payment system and completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet. Bitcoin can also be seen as the most prominent triple entry bookkeeping system in existence [14].

Bitcoin is the first implementation of a concept called “cryptocurrency”, which was first described in 1998 by Wei Dai on the cipher-punks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept were published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself.

Bitcoin is known as a type of cryptocurrency because it uses cryptography to keep it secure. There are no physical bitcoins, only balances kept on a public ledger that everyone has transparent access to. All bitcoin transactions are verified by a massive amount of computing power via a process known as “mining”. Bitcoin is not issued or back-end by any banks or governments, nor is an individual bitcoin valuable as a commodity. Despite it not being legal tender in most parts of the world, bitcoin is very popular and has triggered the launch of hundreds of other cryptocurrencies, collectively referred to as altcoins.

The bitcoin system is a collection of computers that all run bitcoin’s code and store its blockchain. Metaphorically, a blockchain can be thought of as a collection of blocks. In each block is a collection of transactions. Because all the computers running the blockchain has the same list of blocks and transactions and can transparently see these new blocks being filled with new bitcoin transactions, no one can cheat the system.

Balances of bitcoin tokens are kept using public and private “keys”, which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them. The public key serves as the address published to the world and to which others may send bitcoin.

The private key – like ATM PIN, that used to guard secret and only used to authorize Bitcoin transmissions. Bitcoin keys should not be confused with a bitcoin wallet, which is a physical or digital device that facilitates the trading of bitcoin and allows users to track ownership of coins. The term wallet is a bit misleading, as bitcoin’s decentralized nature means it is never stored in a wallet, bet rather distributed on a blockchain.

### **Digital signatures in blockchain**

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender and that the message was not altered in transit [13].

Digital signatures are a fundamental building block in blockchains. They are primarily used to verify the authenticity of transactions. When users submit transactions, they must prove to every node in the system that they are authorized to spend those funds while preventing other users from also spending those funds. Every node in the network will verify the conditions of the submitted transaction and check all other nodes' work to agree on a correct state.

Digital signatures are a standard element of most cryptographic, protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

A digital signature scheme typically consists of three algorithms.

A key generation algorithm – that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

A signing algorithm – that gives a message and a private key, produces a signature.

A signature verifying algorithm – that given the message, public key, and signature, either accepts or rejects the message’s claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party’s private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature. The Digital Signature Algorithm (DSA), developed by the Motional Institute of Standards and Technology, is one of many examples of signing algorithms.

For example, if Alice wants to send 1 BTC to Bob, she must sign a transaction spending 1 BTC of inputs using her private key and send it to nodes on the network. The miners, who have knowledge of her public key, will then check the conditions of the transaction, and validate the authenticity of the signature. Once validity is confirmed, the block containing that transaction will be then ready for finalization by a validator/miner.

The signature scheme currently used in Bitcoin is the Elliptic Curve Digital Signature Algorithm (ECDSA). Compared to Revest-Shamir-Adleman (RSA), ECDSA uses shorter keys and requires fewer computational requirements while still maintaining strong security. ECDSA also uses what is known as elliptic curves over finite fields.

### **Consensus Mechanism**

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies.

Public blockchains that operate as decentralized, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the blockchain, and on the block mining activities.

In such a dynamically changing status of the blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all-important task is performed by the consensus mechanism, which is a set of rules that decides on the legitimacy of contributions made by the various participants (i.e., nodes or transactors) of the blockchain.

There are different kinds of consensus mechanism algorithms, each of which works on different principles. In the context of blockchains and cryptocurrencies, proof-of-work (PoW) and proof-of-stake (PoS) are two of the most prevalent consensus mechanisms.

The proof of work (PoW).

The PoW is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin. In PoW, network actors or participants use computational power to win the right of adding new blocks to the blockchain. If a new block is detected and added to the network, the node that discovered the block is entitled to receive the predefined reward or transaction fees. Computational power is expended to solve a hash puzzle, the solution of which is included in the resulting block. The process of solving the puzzle is computationally intensive and stochastic in nature. Finding a solution is likened to a miner discovering gold; hence, the hashing process is referred to as mining and the node performing it is known as a miner. However, this consensus algorithm needs high energy consumption and a longer processing time.

The proof of stake (PoS).

The PoS is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it. The PoW algorithm is widely considered unsustainable, as the energy consumption required to mine Bitcoin leaves a significant carbon footprint in its wake. Additionally, Bitcoin miners generate large amounts of electrical waste because the ASIC machines used to mine Bitcoin only serve one function.

The PoS algorithm, however, seeks to solve this problem by effectively substituting staking for computational power, whereby an individual's mining power is limited to the percentage of ownership stake. This means a drastic reduction in energy consumption and the manufacture of single-purpose hardware, like the ASIC machines because they are no longer needed for their computing power. In PoW, miners are more likely to win additional blocks if they have more money. However, this comes with the drawback that it incentivizes crypto coin hoarding instead of spending.

With fewer miners than required mining for coins, the network becomes more vulnerable to a 51% attack. A 51% attack is when a miner or mining pool controls 51% of the computational power of the network and creates fraudulent blocks of transactions for themselves while invalidating the transactions of others in the network.

With a PoS, the attacker would need to obtain 51% of the cryptocurrency to carry out a 51% attack. The proof of stake avoids this ‘tragedy’ by making it disadvantageous for a miner with a 51% stake in a cryptocurrency to attack the network. Although it would be difficult and expensive to accumulate 51% of a reputable digital coin, a miner with a 51% stake in the coin would not have it in their best interest to attack a network that they hold a majority share.

The proof of capacity (PoC).

Proof of capacity (PoC) is a consensus mechanism algorithm used in blockchains that allow mining devices in the network to use their available hard drive space to decide mining rights and validate transactions. This contrasts with using the mining device’s computational power (as in the proof of work algorithm) or the miner’s stake in the cryptocurrencies (as in the proof of stake algorithm).

Pros of PoC are:

PoC can use any regular hard drive including those with Android-based systems.

It is reportedly up to 30-times more energy efficient than the ASIC-based mining of the bitcoin cryptocurrency.

There is no need for dedicated hardware or constant upgrading of hard drives.

Mining data can be easily wiped off and the drive can be reused for any other data storage purpose.

Cons of PoC are:

Not many developers have adopted the system.

It is possible for malware to affect mining activities.

Widespread adoption of PoC could start an "arms race" to produce higher-capacity hard drives.

The proof of activity (PoA).

Proof-of-activity (PoA) is a blockchain consensus algorithm used in cryptocurrencies and similar systems. It is used to ensure that all transactions occurring on the blockchain are genuine, as well as to ensure that all miners arrive at a consensus. PoA is a combination of two other blockchain consensus algorithms: proof-of-work (PoW) and proof-of-stake (PoS).

The PoA system is an attempt to combine the best aspects of both the PoW and the PoS systems. In PoA, the mining process begins the same way as in a PoW process, with various miners trying to outpace each other with higher computing power to find a new block. When a new block is found (or mined), the system switches to PoS, with the newly found block containing only a header and the miner's reward address.

The proof of burn (PoB).

Proof of burn (PoB) is an alternative consensus algorithm that tries to address the high energy consumption issue of a PoW system.

PoB is often called a PoW system without energy waste. It operates on the principle of allowing miners to burn virtual currency tokens. They are then granted the right to write blocks in proportion to the coins burnt.

Proof of burn is one of the several consensus mechanism algorithms implemented by a blockchain network to ensure that all participating nodes come to an agreement about the true and valid state of the blockchain network. This algorithm is implemented to avoid the possibility of any cryptocurrency coin double-spending.

The proof of elapsed time (PoET).

Proof of elapsed time (PoET) is a consensus mechanism algorithm that is often used on the permissioned blockchain networks to decide the mining rights or the block winners on the network. Permissioned blockchain networks are those which require any prospective participant to identify themselves before they are allowed to join. Based on the principle of a fair lottery system where every single node is equally likely to be a winner, the PoET mechanism is based on spreading the chances of winning fairly across the largest possible number of network participants.

Proof of elapsed time (PoET) is a blockchain network consensus mechanism algorithm that prevents high resource utilization and high energy consumption and keeps the process more efficient by following a fair lottery system. The algorithm uses a randomly generated elapsed time to decide mining rights and block winners on a blockchain network. By running a trusted code within a secure environment, the PoET algorithm also enhances transparency by ensuring lottery results are verifiable by external participants.

The benefits of PoET are:

Essentially, the workflow is similar to the consensus mechanism followed by Bitcoin's proof of work (PoW) algorithm, but without its high-power consumption.

The mechanism of running trusted code within a secure environment also takes care of many other necessities of the network.

PoET controls the cost of the consensus process and keeps it nimble so that the cost remains proportional to the value derived from the process, a key requirement for the cryptocurrency economy to continue flourishing.

## Techniques applied in blockchain

### **Decentralized consensus**

The term “decentralized consensus” refers to a set of principles and techniques that allow participants on a distributed network to arrive at a perfect agreement on a shared document or database. Systems built upon decentralized consensus methods are inherently tamper-proof, censorship-resistant, and permissionless.

Decentralized systems are distributed systems where a group of independent but equally privileged nodes operate on local information to accomplish global goals. These systems lack a central controller that exercises governance, supervision, and control over the system, thus allowing power to be distributed over the network in a more uniform and fair manner. Distributed systems are not new, with applications such as Napster driving the peer-to-peer boom of the early 2000s.

Consensus is a shared view of reality that is agreed upon between different parts of a system. Whereas decentralized systems are easy to build without consensus and consensus is easy to achieve in centralized systems, maintaining both properties in the same system proves difficult. This is the underlying innovation in the field of decentralized consensus. The ability to build decentralized systems where a group of independent but equally privileged nodes can reach a shared view of reality. Cryptocurrencies are an excellent example of an application that requires such a system, where agreement upon the ledger of transactions and balances can be reached without a governing body.

Decentralized networks like Bitcoin, Litecoin, Ethereum, or Bitcoin Cash have no central authority that would validate their crypto transactions or safeguard their records.

Such peer-to-peer networks consist of thousands of computers or nodes, which are distributed all around the world. But how do nodes, which work as independent units and do not trust any higher authority, manage to agree on the right state of the blockchain? It’s all thanks to the implementation of a consensus mechanism, which allows nodes to reach an agreement on the validity of transactions.

Nodes go through these processes independently but must follow the same set of blockchain consensus rules to stay compatible. Decentralized consensus emerges from four specific processes.

Full nodes independently check each transaction against pre-specified criteria.

Mining node then collect verified transactions and add them to a new block alongside the solution to the computational puzzle required for proof of work.

Every node verifies the new blocks and connects them to the chain.

It is then up to full nodes to determine which of the chains exhibits the most cumulative computation demonstrated by proof of work, making that branch of the chain the main chain.

### **Distributed database**

A distributed database is a database that is not limited to one system, it is spread over different sites, on multiple computers, or over a network of computers. A distributed database system is located on various sites that don’t share physical components. This may be required when a particular database needs to be accessed by various users globally. It needs to be managed such that for the users it looks like one single database.

Distributed databases are divided into two types are: Homogeneous Database and Heterogeneous Database.

In the Homogeneous Database, all the physical locations have the same underlying hardware and run the same operating systems and database applications. Homogeneously distributed database systems appear to the user as a single system, and they can be much easier to design and manage. For a distributed database system to be homogeneous, the data structures at each location must be either identical or compatible. The database application used at each location must also be either identical or compatible.

In Heterogeneous Database, the hardware, operating systems, or database applications may be different at each location. Different sites may use different schemas and software, although a difference in schema can make query and transaction processing difficult. Heterogeneous distributed databases are often difficult to use, making them economically infeasible for many businesses.

There are two ways in which data can be store on different sites.

Replicated data is used to create instances of data in different parts of the database. If the entire data base is available at all sites, it is a fully redundant database. Hence, in replication, systems maintain copies of data.

Replicated data can be divided into two categories: read-only and writable data. Read-only allow revisions only to the first instance, subsequent enterprise data replications are then adjusted. Writable data can be altered, but the first instance is immediately changed.

The advantages of replicated data are increasing the availability of data at different sites. However, it has certain disadvantages are data needs to be constantly updated.

Data are located near the greatest demand site. The data in a distributed database system are dispersed to match business requirements which reduces the cost of data access.

Faster data access. End users often work with only a locally stored subset of the company’s data.

Faster data processing. A distributed database system spreads out the workload of the system by processing data at several sites.

Growth facilitation. New sites can be added to the network without affecting the operations of other sites.

Improved communications. Because local sites are smaller and located closer to customers, local sites foster better communication among departments and between customers and company staff.

Reduced operating costs. It is more cost-effective to add workstations to a network than to update a mainframe system. Development work is done more cheaply and more quickly on low-cost PCs than on mainframes.

User-friendly interface. PCs and workstations are usually equipped with an easy-to-use graphical user interface (GUI). The GUI simplifies training and uses for end-users.

Less danger of a single-point failure. When one of the computers fails, the workload is picked up by other workstations. Data are also distributed at multiple sites.

Processor independence. The end-user can access any available copy of the data, and an end user's request is processed by any processor at the data location.

In addition to the advantages that distributed databases bring, there are also many disadvantages that encounter:

The complexity of management and control. Applications must recognize data location, and they must be able to stitch together data from various sites. Database administrators must have the ability to coordinate database activities to prevent database degradation due to data anomalies.

Technological difficulty. Data integrity, transaction management, concurrency control, security, backup, recovery, query optimization, access path selection, and so on, must all be addressed and resolved.

Security. The probability of security lapses increases when data are located at multiple sites. The responsibility of data management will be shared by different people at several sites.

Lack of standards. There are no standard communication protocols at the database level. (Although TCP/IP is the de facto standard at the network level, there is no standard at the application level.) For example, different database vendors employ different—and often incompatible—techniques to manage the distribution of data and processing in a DDBMS environment.

Increased storage and infrastructure requirements. Multiple copies of data are required at different sites, thus requiring additional disk storage space.

Increased training cost. Training costs are generally higher in a distributed model than they would be in a centralized model, sometimes even to the extent of offsetting operational and hardware savings.

Costs. Distributed databases require duplicated infrastructure to operate (physical location, environment, personnel, software, licensing, etc.).

The relations are fragmented and each of the fragments is stored in different sites where they are required. Fragmentation is advantageous as it does not create copies of data, consistency is not a problem.

Fragmentation of relations can be divided into two ways: Horizontal fragmentation – Splitting by rows and Vertical fragmentation – Slitting by columns.

With Horizontal fragmentation, it is fragmented into groups of tuples so that each tuple is assigned to at least one fragment. In Vertical fragmentation, the schema of the relations is divided into smaller schemas. Each fragment must contain a common candidate key to ensure a lossless join.

### **Distributed ledger**

A distributed ledger is a database shared by multiple participants in which each participant maintains and updates a synchronized copy of the data. Distributed ledgers allow members to securely verify, execute, and record their transactions without relying on an intermediary, such as a bank, broker, or auditor. It allows transactions to have public "witnesses." The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

A centralized ledger is more prone to cyber-attacks and fraud, as it has a single point of failure. The distributed ledger is different from that, it is inherently harder to attack because all the distributed copies need to be attacked simultaneously for an attack to be successful.

Furthermore, these records are resistant to malicious changes by a single party. By being difficult to manipulate and attack, distributed ledgers allow for extensive transparency.

Distributed ledgers also reduce operational inefficiencies, speed up the amount of time a transaction takes to complete, and are automated. All of that reduce overall costs for the entities that use them and helps remove the possibility of fraud occurring on the financial books of a company.

The distributed ledger is usually used for: Finance, music and entertainment, diamond and precious assets, artwork, and supply chain of various commodities.

Distributed ledgers are held, reorganized, and controlled by individuals called nodes. The database is constructed independently by each node.

Every transaction occurring on the network is processed, and a conclusion on the development of the database is created by each node. Voting is carried out on the changes completed on the database.

All nodes participate in the voting, and if at least 51% of them agree, the new transaction is accepted on the database. Afterward, the nodes update the versions of the ledger so that all the devices or nodes will be of the same version. The new transaction is written onto a block on the blockchain.

Nodes in the Proof-of-Work blockchain are also called miners. When a miner successfully puts a new transaction into a block, they receive a reward. It requires dedicated computing power.

It is the responsibility of miners to compute the cryptographic hash for new blocks. Whoever, among the miners, successfully finds the hash first, gets the reward. Miners dedicating more computational power to find the hash will be more successful. However, as blocks keep generating, it becomes more difficult to find subsequent hash scales. The goal is to keep a constant speed of generating the blocks.

Benefits of Distributed Ledger.

Highly transparent, secure, tamper-proof, and immutable – In distributed ledgers, the entries happen in the database without third-party involvement. After records are written into distributed ledgers, they cannot be altered by any other party. Hence, until the ledgers are distributed, the records cannot be tampered with.

The need for a third party is eliminated – Although it is not necessary to always operate the distributed ledgers without a third party, it can save a lot of money and time in some cases. In the supply chain business, results can be written directly by sensors to the blockchain without the need for a third party. It saves a considerable amount of money, effort, and time.

Inherently decentralized – The distributed ledgers’ inherently decentralized nature adds another layer of security. As the database is spread globally, it is difficult to attack.

Highly transparent – Distributed ledgers present with a high level of transparency. They allow all the stored information to be freely and easily viewable. It provides a significant amount of transparency desired by many industries.

### **Data distributed**

Data distribution is a function that specifies all possible values for a variable and quantifies the relative frequency. Distributions are considered any population that has a scattering of data. It’s important to determine the kind of distribution that population has so we can apply the correct statistical methods when analyzing it Data distributions are widely used in statistics.

Data distributions are basically classified based on the type of data.

A discrete distribution resulting from countable data that has a finite number of possible values. Furthermore, discrete distribution can be reported in tables and the respective values of the random variable are countable.

A continuous distribution containing infinite data points that may be displayed on a continuous measurement scale. A continuous random variable is a random variable with a set of possible values that is infinite and uncountable.

By storing data across its peer-to-peer network, the blockchain eliminates several risks that come with data being held centrally [3]. The decentralized blockchain may use ad hoc message passing and distributed networking. One risk of a lack of a decentralization is a so-called “51 attack” where a central entity can gain control of more than half of a network and can manipulate that specific blockchain record at will, allowing double-spending [9].

Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography [10]. A public key is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible [3].

# Chapter 2 E-commerce problem analysis

# Chapter 3 Deploy and build the system

# Chapter 4 Conclusion and development direction

**Appendix**

**References**

1. Morris, David Z. (15 May 2016) – “Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting”
2. Popper, Nathan (21 May 2016) – “A Venture Fund with Plenty of Virtual Capital, but No Capitalist”
3. “The great chain of being sure about things” (The Economist, October 31, 2015) – [The great chain of being sure about things | The Economist](https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things) – (Accessed 2:21 PM, October 8, 2021)
4. Narayanan, Arvind; Bonneau Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016) – “Bitcoin and cryptocurrency technologies: a comprehensive introduction”
5. “The Truth About Blockchain” (Harvard Business Review, Jan-Feb 2017) - [The Truth About Blockchain (hbr.org)](https://hbr.org/2017/01/the-truth-about-blockchain) – (2:52 PM, October 8, 2021)
6. Haber, Stuart; Stornetta, W. Scott (January 1991) – “How to time-stamp a digital document”
7. Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992) – “Improving the Efficiency and Reliability of Digital Time-Stamping.”
8. Bhaskar, Nirupama Devi; Chuen, David LEE Kuo (2015) – “Bitcoin Mining Technology”
9. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’” (Fortune, May 29, 2018) – (Accessed 3:13 PM, October 8, 2021)
10. Brito, Jerry; Castillo, Andrea (2013) – “Bitcoin: A Primer for Policymakers” - [Brito\_BitcoinPrimer.pdf (mercatus.org)](https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf)
11. Franco, Pedro (2014) – “Understanding Bitcoin: Cryptography, Engineering and Economics”
12. Size of the Bitcoin blockchain from January 2009 to September 13, 2021 (Statista) - [• Bitcoin blockchain size 2009-2021 | Statista](https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/) – (Accessed 4:15 PM, October 8, 2021)
13. Paul, Eliza (September 12, 2017) – “What is Digital Signature – How it works, Benefits, Objectives, Concept”
14. Damilare Peter Oyinloye, Je Sen Teh, Norziana Jamil, and Moatsum Alawida – “Blockchain consensus: An Overview of Alternative Protocols”
15. [FAQ - Bitcoin](https://bitcoin.org/en/faq#who-controls-the-bitcoin-network) – (Accessed 10:57 PM, October 9, 2021)
16. [Blockchain - Wikipedia](https://en.wikipedia.org/wiki/Blockchain#:~:text=The%20first%20blockchain%20was%20conceptualized,as%20Satoshi%20Nakamoto%20in%202008.&text=The%20design%20was%20implemented%20the,all%20transactions%20on%20the%20network.) – (Accessed 2:01 PM, October 8, 2021)
17. [What is blockchain? - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/2-what-is-blockchain?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development) – (Accessed 8:10 PM, October 7, 2021)
18. [How blockchain works - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/3-how-blockchain-works?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development) – (Accessed 8:21 PM, October 7, 2021)
19. [Blockchain types - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/intro-to-blockchain/4-blockchain-types?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.ethereum-blockchain-development) – (Accessed 3:39 PM, October 8, 2021)
20. [What are smart contracts on blockchain? | IBM](https://www.ibm.com/topics/smart-contracts) – (Accessed 4:09 PM, October 8, 2021)
21. [Digital Signatures in Blockchains: The Present and Future — Bison Trails](https://bisontrails.co/digital-signatures/) – (Accessed 5:10 PM, October 8, 2021)
22. [Blockchain and Decentralized Consensus (orbs.com)](https://www.orbs.com/blockchain-and-decentralized-consensus/) – (Accessed 5:20 PM, October 8, 2021)
23. [What is distributed database? - Definition from WhatIs.com (techtarget.com)](https://searchoracle.techtarget.com/definition/distributed-database) – (Accessed 10:20 PM, October 21, 2021)
24. [What are distributed ledger technologies? | Hedera](https://hedera.com/learning/what-are-distributed-ledger-technologies-dlts?gclid=CjwKCAjwn8SLBhAyEiwAHNTJbenhUVF4czl8fOF9S-JcRwk1KTw6MJl158cDIrHxXLZFsyW6hzKLZxoCg_AQAvD_BwE) – (Accessed 10:30 PM, October 21, 2021)
25. [Data Distributions - What you need to know for a Six Sigma certification exam. (sixsigmastudyguide.com)](https://sixsigmastudyguide.com/data-distributions/) – (Accessed 4:00 PM October 23, 2021)
26. [Public vs private blockchain: Who wins? | public blockchain | (allerin.com)](https://www.allerin.com/blog/public-vs-private-blockchain-who-wins) – (Accessed 4:15 PM October 23, 2021)
27. [Hash Definition (investopedia.com)](https://www.investopedia.com/terms/h/hash.asp) – (Accessed 5:00 PM October 23, 2021)
28. [Distributed Ledgers - Overview, How It Works, Benefits (corporatefinanceinstitute.com)](https://corporatefinanceinstitute.com/resources/knowledge/other/distributed-ledgers/) – (Accessed 6:30 PM October 23, 2021)
29. [Proof of Activity Definition (investopedia.com)](https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp) – (Accessed 7:00 PM October 23, 2021)
30. [Proof of Burn (Cryptocurrency) Definition (investopedia.com)](https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp) – (Accessed 7:10 PM October 23, 2021)
31. [Proof of Elapsed Time (PoET) (Cryptocurrency) Definition (investopedia.com)](https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp) – (Accessed 7:15 PM October 23, 2021)
32. [Proof of Capacity (Cryptocurrency) Definition (investopedia.com)](https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp) – (Accessed 7:20 PM October 23, 2021)