Chapter 2
BLOCKCHAIN CONCEPTS

2.1. CONCEPT

2.1.1. Concept

Blockchain is a distributed database technology that acts as a cryptographically secured digital ledger, allowing information to be stored in a transparent, secure, and immutable manner. This information is organized into blocks, linked together in chronological order through hash functions, forming a chain. Let's learn the basic concepts of this technology.

Blockchain is not yet a household word, like the cloud or the Internet of Things. It's not yet an innovation that you can see and touch as easily as a smartphone or a package from Amazon. But in a world where anyone can edit an entry on Wikipedia, or information on social networks,... blockchain is the answer to a question we have been asking since the dawn of time. The invention of the internet age: How can we come together to trust what happens online?

Every year, we handle more of our work than our lives – many of the core functions of government, the economy and society – on the internet. We do a lot of our banking online. We shop online. We log into applications and services that create a digital record of our information and send information back and forth across the internet. Think of blockchain as an underlying historical structure that records everything that happens - every digital transaction; exchange of value, goods and services; or private data - exactly as it happens.

Blockchain is like a distributed database that maintains a list of records and is shared across the internet environment. These records are called blocks and each encrypted block of code contains the history of every block before it with transaction data timestamped down to the second, the chain of blocks linked together is called the blockchain (blockchain) and then they are distributed across a global network of computers creating a complete blockchain where third parties cannot change the data.

Blockchain is made up of two main components: a decentralized network that facilitates and verifies transactions, and an immutable ledger that this network maintains. Everyone on the network can see this shared ledger of transactions, but there is no single point of failure from which a record or digital asset could be hacked or corrupted. Because of that decentralized trust, there's also no one organization that controls that data, whether it's a big bank or a tech giant like Facebook or Google. No third party acts as a controller of the internet. The power of distributed ledger technology has applications across all types of digital records and transactions, and we are starting to see major industries transition to this trend.

First comes the big banks and technology giants. Big business has always been at the forefront of innovation, the development of blockchain-based smart contracts has made blockchain an intermediary for complex business transactions, legal agreements and automated data exchange. . Companies like Microsoft or IBM are leveraging their cloud infrastructure to build custom blockchains for customers and test their own applications, such as developing a global food safety network connecting connecting manufacturers and

retailers. On the academic side, researchers are exploring blockchain applications in projects ranging from digital identities to medical and insurance records, etc.

At the same time, dozens of startups are using this technology for everything from global payments to music sharing, from tracking sales to tracking supply chains and more. That's why. Why is blockchain's potential so great? When it comes to digital assets and transactions, you can put anything on the blockchain. A series of economic, legal, regulatory and technological hurdles must clear before we see widespread adoption of blockchain technology, but the frontrunners are making incredible strides. Over the next few years, much of your digital life could start running on a blockchain platform - and you might not even realize it.

Blockchain is the data structure that allows Bitcoin (BTC) and new generation cryptocurrencies such as Ether (ETH), Cardano (ADA),... to develop strongly through a combination of decentralized encryption, computing anonymity, immutability, and global scale. This is the not-so-secret weapon behind the rise of cryptocurrencies, and to explain how blockchain came to be, we must begin briefly with the legacy of Bitcoin introduced in the next section of the chapter. This.

People often get bogged down in the complexity of the technology when trying to understand blockchain, but the basic concept is a simple and universal one. We have facts and information that we do not want to be accessed, copied or tampered with, but on the internet there is a possibility that they can be hacked or modified. Blockchain gives us a principle - a platform that we know will not change once we put something on the platform, where a transaction will only be verified if it follows the rules of this platform.

White paper Nakamoto explains the basics about "mining" data into a block, then using a hash function (time-stamped link) to chain those blocks together on a decentralized network of "nodes" that verify each transaction pandemic. Another key innovation in the white paper is the use of what is called a proof-of-work (PoW) model to create distributed "trustless" consensus and solve the double-spending problem (ensuring ensure that cryptocurrency cannot be spent more than once).

"The system does not need to be trusted" doesn't mean you can't trust the system. Quite the contrary, because the blockchain verifies each transaction through PoW, this means there is no need for trust between those involved in the transaction. Where does proof of work come from? Miners. A P2P network of Bitcoin "miners" create PoW when they hash blocks together, verifying transactions that are then included in the ledger.

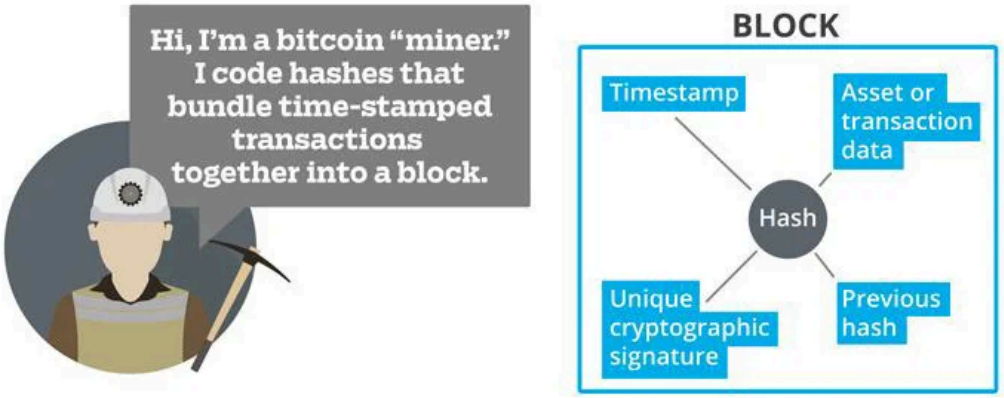

Figure 2.1. Block

In the 2016 book Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, authors Don and Alex Tapscott explained Nakamoto's Bitcoin model as concisely as possible:

> *"Bitcoin or other digital currencies are not stored in a file somewhere; they are represented by transactions recorded in a blockchain - like a global spreadsheet or ledger, leveraging resources of a large P2P network to verify and approve each Bitcoin transaction. Each blockchain, like the [Bitcoin blockchain] is distributed: it runs on computers provided by volunteers around the world Which central database to hack? public: anyone can view it at any time because it is on the network… and the blockchain is encrypted… it uses public and private keys (like a two-key system to access a safe deposit box) security) to maintain virtual security."*

Please note that nothing is completely unhackable, especially when you do not use it for its intended purpose. Blockchain's security is not only effective because it is encrypted but also because it is decentralized. Victims of the largest blockchain breaches and cryptocurrency thefts (**Mt. Gox** 2014 and **Bitfinex** 2016) were targeted and stolen because they tried to centralize a decentralized system. **Ethereum** has also seen a number of hacks and security incidents. The 2016 DAO hack was one of the standout events in blockchain history. Specifically, it concerns vulnerabilities in smart contracts written on the Ethereum blockchain. Recently, the largest Ethereum exchange in South Korea was hacked, and an initial coin offering (ICO) by an Israeli startup ran into trouble when its website was compromised.

All of these problems stem from vulnerabilities in the systems connected to the blockchain, not from the blockchain itself. The underlying encryption and security model of blockchain is still considered sound, but how to enforce that security is another matter.

We've explained how the network works and how security is implemented, but how do the blocks actually connect to each other? Why is the stronger the blockchain, the slower the processing speed? Where does immutability appear? Tapscotts' explanation continues as follows:

"Every ten minutes, like the heartbeat of the Bitcoin network, all transactions made are verified, removed from the queue and stored in a block linked to the previous block, thereby forming a blockchain .To be valid, each block must reference the previous block, not only does it permanently time-stamp it, but it also stores value transactions, preventing anyone from altering the ledger. Blockchain is a distributed ledger, representing consensus network of every transaction that has taken place. Just as the World Wide Web is a global network of information, blockchain is the 'World Wide Ledger' of this new digital ledger that can be programmed to record almost everything that is important and valuable to humanity: from birth certificates, death certificates, marriage licenses, deeds and property rights, educational qualifications, financial accounts, medical procedures health, insurance claims, votes, to food origins or anything that can be expressed in code."

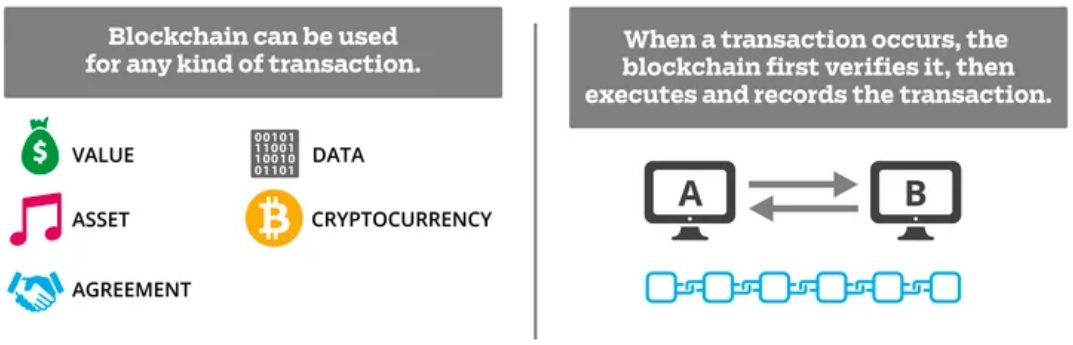

Figure 2.2. *World Wide Ledger*

Immutability is perhaps the most important concept to understand about blockchain and why it is valuable. In the digital world, creating an object that cannot be changed after its creation brings infinite value, because it ensures data integrity and reliability.

Going back to the 'power in numbers' principle, the more nodes a blockchain is distributed across, the stronger and more reliable it is. This is a process of verification upon verification, which lasts indefinitely. A blog post by Garzik highlights that the network effect of blockchain is the key to its immutability, and is also the reason why Bitcoin's public blockchain remains the most popular and trusted system today.

Garzik explains: Immutability depends heavily on network effects. This is clearly shown with Bitcoin. The cost of creating a new digital asset is almost zero. So to convince anyone To leave the Bitcoin blockchain, you need to demonstrate superior value to overcome the inherent network effect. Not only is it a reliable track record, Bitcoin also has high security value from a technical perspective The immutability of a blockchain is a direct result of its economics behind it – including the level of investment in the ecosystem and the number of people using the system."

2.1.2. Some important characteristics of blockchain

Blockchain is a prominent technology in the cryptocurrency space, but it also has many other applications beyond currency. Here are some important characteristics of blockchain:

1. Immutability: Data in the blockchain cannot be changed or deleted once recorded, ensuring the integrity of the ledger.

2. Decentralization: Blockchain does not depend on a central authority or organization for management, but transactions are distributed and confirmed through many network nodes, ensuring transparency and reducing the risk of abuse of power.

3. Transparent and immutable: Every transaction on the blockchain is recorded and made public to all network participants, and once information is recorded on the blockchain, it cannot be altered or deleted.

4. High security: Blockchain uses strong encryption to protect data and ensure that only those with access can change the information. This makes blockchain an extremely secure platform.

5. Smart Contracts: Blockchain can support the implementation of smart contracts, which are contracts that automatically execute when certain conditions are met. This helps save time and costs related to intermediaries and procedures.

6. Scalability and wide application: While blockchain is best known for its cryptocurrency applications, the technology is also applied in a variety of fields, from supply chain management and e-voting to insurance and healthcare. .

7. Dispersion: Each blockchain participant (network nodes) has a copy of the entire ledger, which helps disperse information and protect the system from attacks.

8. Cost savings: Blockchain can help reduce transaction and payment processing costs by eliminating intermediaries and using automated processes, thereby improving efficiency and minimizing dependence on third parties.

2.1.3. Basic components of blockchain

Blockchain is made up of a number of basic components, each of which plays an important role in ensuring the security, transparency and efficient operation of the system. Here are the basic components of blockchain:

1. Blocks:

Blockchain is divided into blocks, each block contains a group of transactions. Each block includes information such as:

- Transaction data: Transactions are recorded in blocks, including information about the sender, recipient, and transaction amount.

- Digital Signature: Used to confirm the validity of transactions.

- Hash code of the previous block: Each block stores the hash code of the previous block, forming a linked chain.

- Hash code of the current block: Each block has a separate hash code, used to identify and confirm the integrity of the data.

2. Distributed Ledger:

Blockchain is a distributed ledger, which means copies of data are stored on multiple nodes across the network.

This ensures transparency and reduces the risk of a node or part of the system being attacked.

3. Network node (Node):

Nodes in the blockchain can be computers, devices, or organizations participating in the network. They are responsible for storing and processing information.

Nodes can be full nodes, which store the entire copy of the blockchain, or light nodes, which store only a portion of the necessary data.

4. Mã hash (Hash):

Hash is an arithmetic value generated by the hash algorithm, used to represent the block's data.

Each block in the blockchain has a unique hash code, which helps ensure that any changes in the block will change the hash code and make tampering easier to detect.

5. Consensus Algorithm:

The consensus algorithm is the mechanism for nodes in the blockchain network to agree on valid transactions and add them to the chain.

Popular algorithms include:

- Proof of Work (PoW): Requires nodes to perform complex calculations to verify and add transactions to the blockchain (used in Bitcoin).

- Proof of Stake (PoS): Nodes are selected based on the amount of currency they own and are willing to participate in the validation process (used in Ethereum 2.0).

- Delegated Proof of Stake (DPoS): The blockchain network can delegate authority to a number of representative nodes to process transactions (commonly seen in EOS).

6. Smart Contract:

Smart contracts are programs that automatically execute conditions when a transaction occurs without the intervention of a third party.

They help automate agreements and enforce the rules that participating parties have agreed to.

7. Communication channel (P2P Network):

Blockchain uses a peer-to-peer network so nodes can exchange information directly with each other without going through an intermediary server. This increases the dispersion and security of the system.

8. Cryptography mechanism:

Encryption plays an important role in protecting data integrity and authenticating transactions.

Transactions and information on the blockchain are encrypted using algorithms such as SHA-256, RSA, or elliptic curve cryptography (ECC).

These components work together to form a complete blockchain system, ensuring security, transparency and stability.

2.1.4. Blockchain's operating process

The blockchain process can be summarized as a series of steps, from the time a transaction is created until it is confirmed and added to the permanent ledger. Below is the basic working process of blockchain:

1. Create transaction

The process begins when users (or systems) create a transaction. Transactions can be money transfers, asset ownership transfers, or other actions depending on the application of the blockchain.

This transaction will be encrypted and includes information such as sender, recipient, amount, and related information.

2. Confirm the transaction

Transactions, after being created, will be distributed to the network of nodes in the blockchain.

Nodes in the network will check the validity of the transaction (for example, verify that the sender has enough balance to make the transaction).

Some blockchains use consensus algorithms (like Proof of Work, Proof of Stake) to confirm transactions.

3. Create a new block (Block)

Once a transaction is confirmed, it will be grouped with other transactions into a block.

Each block will have the following main components:

- Transaction data: Confirmed transactions.
- Hash of previous block: Links this block to the previous block in the chain.
- Hash code of the current block: Guarantees the integrity of the block.
- Timestamp: Time when the block was created.
- Execute smart contract (if any).

4. Block validation via consensus algorithm

Once the block is created, it is sent to the nodes in the network for confirmation.

This validation process typically uses consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) to ensure that nodes agree to the block and the transactions within it.

For example, in a Proof of Work system, nodes (miners) compete to solve complex mathematical problems (finding a valid hash value), and when they succeed, the block is accepted and added. into the chain.

5. Add block to blockchain

Once a block is confirmed, it is added to the blockchain chain permanently.

The new block will contain the hash of the previous block, forming an irreversible chain. This ensures that once information has been recorded on the blockchain, it cannot be altered or deleted without altering all subsequent blocks, which is difficult and expensive.

6. Distribute copies of the ledger

Once the new block is added to the blockchain, its copy is distributed to all nodes in the network.

This ensures that every node has the latest copy of the blockchain and helps maintain the system's decentralization and transparency.

7. Transaction completed

Once the block has been confirmed and added to the blockchain, the transactions in the block are considered complete and cannot be changed.

Recipients can confirm that they received the transaction through the system, and all parties involved can access a copy of the ledger to check the validity of the transaction.

8. The process continues

After each transaction is added to the blockchain, the process will continue from step 1 for subsequent transactions.

New blocks will be created and confirmed continuously, maintaining the development of the blockchain chain.

With the above process, blockchain ensures that each transaction is recorded transparently and securely without the intervention of an intermediary organization.

2.2. HISTORY OF BLOCKCHAIN

2.2.1. A brief history of blockchain technology

The core idea of blockchain technology began to emerge in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol; and in 1990 he submitted the paper *The Part-Time Parliament* for magazine *ACM Transactions on Computer Systems*. This paper, eventually published in 1998, describes a consensus model that helps achieve unity within a computer network, even when the computers or network may not be completely trustworthy.

In 1991, a digitally signed string of information was used as an electronic ledger to digitally sign documents, helping to prove that no documents in the ledger had been altered. These ideas are then combined and applied to cryptocurrencies; in 2008, they are described in the paper *Bitcoin: A Peer-to-Peer Electronic Cash System*, published under the pseudonym Satoshi Nakamoto. By 2009, Bitcoin's blockchain network was officially established. Nakamoto's paper laid out the fundamental design on which most modern cryptocurrency systems are based, albeit with variations and improvements. Bitcoin was the first blockchain application, paving the way for many other applications based on blockchain technology.

Before Bitcoin, there were many other cryptocurrency systems such as **ecash** and **NetCash**, but neither system achieved widespread popularity. Blockchain allows Bitcoin to operate in a distributed form, with no one in complete control of the system and no centralized point of failure, which has fueled its adoption. The main benefit of Bitcoin is that it allows direct transactions between users without the need for a trusted intermediary. Furthermore, blockchain supports the issuance of new cryptocurrencies in a predetermined manner for the participants who maintain the network and update the ledger, known as *'miner'* in Bitcoins. Automated payments to miners help manage the system in a distributed fashion without the need for complex organization. Blockchain and consensus mechanisms have created a self-operating system, ensuring that only valid transactions and blocks are added to the blockchain.

In Bitcoin, blockchain allows users to be partially anonymous. This means that users are not directly identified, but their account identifiers can be tracked. Furthermore, all transactions are public on the blockchain. This anonymity helps Bitcoin provide a fair level of security, as accounts can be created without going through the verification or authorization process that is typically required by law. *Know-Your-Customer (KYC)*.

Because Bitcoin is partially anonymous, creating trust in an environment where users are not easily identifiable is important. Before the advent of blockchain technology, this trust was typically provided through trusted intermediaries on both sides of the transaction. In blockchain, trust is built on four key characteristics of blockchain technology:

- **Ledger**: This technology uses a write-only ledger, providing a full transaction history. Unlike traditional databases, transactions and values on the blockchain are not overwritten.
- **Secure (Secure**): Blockchain is secured using cryptographic methods, ensuring that the data in the ledger cannot be tampered with and is always verifiable.
- **Shared**: The ledger is shared among multiple participants, providing transparency across all nodes in the blockchain network.
- **Distributed:** Blockchain can be distributed, allowing the number of nodes in the network to expand, thereby increasing resistance to attacks from bad actors. As the number of nodes increases, the likelihood of a bad actor influencing the blockchain's consensus protocol decreases.

Blockchain was officially introduced in 2009 with the launch of its first application, the cryptocurrency Bitcoin. However, the origins of this technology date back decades. Many of the technologies underlying today's blockchain were developed long before Bitcoin appeared.

However, blockchain is often associated with Bitcoin, whether in a positive or negative way. In the chaotic and tumultuous years that followed Bitcoin's launch, blockchain became a technology with a reputation akin to the Wild West. Its distributed peer-to-peer (P2P) architecture allows virtually anyone to participate in the process, making it too risky for business adoption. However, this began to change in 2016, when a growing open source community began building complete enterprise platforms.

Since then, blockchain technology has taken on a life of its own, attracting interest from many quarters, despite the sometimes scary headlines associated with cryptocurrencies. Governments, businesses, and other organizations are researching and implementing blockchain technology to serve needs unrelated to digital currencies. Amid rising cyber threats and government data privacy regulations, blockchain provides security, immutability, traceability, and transparency across the entire distributed network. distributed, helping to solve problems that traditional infrastructure can hardly support and protect.

Although blockchain has a relatively short history, its influence today is widespread and its applications are expanding and evolving. Over the decades, the development and evolution of blockchain has witnessed some of the following notable advances:

- Pioneers like Merkle with his tree model, Chaum with digital currency, Haber with timestamps, Dwork with proof of work (PoW), Black with hashcash, and Finney with reusable PoW have contributions from the early years in the development landscape of cryptocurrency and blockchain.

- The pseudonym Satoshi Nakamoto was used to introduce the concept of cryptocurrency and blockchain. Soon after, the cryptocurrency was launched, and Nakamoto made the transaction *bitcoin* First, a bitcoin exchange was established, and a programmer spent *10.000 bitcoin* to buy two pizzas.

- Bitcoin prices have skyrocketed from a few cents to tens of thousands of dollars, accompanied by controversies, shutdowns, crackdowns, bankruptcies, scams, scandals and arrests.

- Blockchain began to separate from Bitcoin when the blockchain platform became decentralized *Ethereum* becoming one of the largest applications of blockchain technology, opening up opportunities for many business applications beyond the cryptocurrency sector.

- Powered by AI, IoT, non-fungible tokens (NFTs), decentralized finance (DeFi), smart contracts, and initiatives from companies like Walmart and Amazon, blockchain has become a legal, safe and viable alternative to traditional methods of conducting business and personal transactions.

2.2.2. The formation and development process of blockchain technology

In 1979, one of the first pre-blockchain technologies, the Merkle tree, was named after computer scientist and mathematician Ralph Merkle. He described a method of distributing public keys and digital signatures called tree authentication in his doctoral thesis at Stanford University. Merkle then patented this idea as a method of providing digital signatures. Merkle trees provide a data structure for verifying individual records.

In 1992, in his PhD thesis at the University of California, Berkeley, David Chaum described a safe system for establishing, maintaining, and building trust between the computer systems of mutually suspicious groups. each other. This system includes many elements that make up a blockchain. Chaum is also credited with inventing digital currency, and in 1989 he founded the company DigiCash.

In 1991, Stuart Haber and W. Scott Stornetta published an article describing how to time-stamp digital documents to prevent users from changing the dates of electronic documents. The goal is to maintain complete document privacy without the need to keep records of a time stamping service. Haber and Stornetta later updated their design to incorporate a Merkle tree, allowing multiple document certificates to exist on a single block.

In 1993, the original concept of **PoW** (Proof of Work) was published in an article by Cynthia Dwork and Moni Naor, aiming to provide "*a computational technique for fighting spam in particular and controlling access to shared resources in general.*"

In 1997, Adam Black introduced **hashcash**, a PoW algorithm that aims to provide countermeasures against denial of service (DoS) conditions.

In 1999, Markus Jakobsson and Ari Juels published the term **proof of work** (Proof of Work). Same year, network **P2P** was popularized by peer-to-peer file sharing applications **Napster**, although this application no longer exists. Some people argue that Napster is not a true P2P network because it uses centralized servers. However, the service helped highlight the concept of P2P networks, helping to build distributed systems that can leverage computing power and storage capacity from thousands of computers.

In 2000, Stefan Konst introduced the concept of *The string is cryptographically secured* in the article "Secure Log Files Based on Cryptographically Concatenated Entries." His model showed that entries in the chain could be traced back to the Genesis block to prove authenticity, and this became the basis for today's blockchain models.

In 2004, Hal Finney introduced reusable PoW, a mechanism for receiving a non-exchangeable - or non-fungible - hashcash token in exchange for a token signed with RSA. The PoW method plays an important role in Bitcoin mining today. Cryptocurrencies like Bitcoin and Litecoin use PoW, while Ethereum has moved to a proof of stake protocol to secure the network with a fraction of the energy that PoW uses.

In 2008, Satoshi Nakamoto, believed to be the pseudonym of an individual or group of individuals, published a white paper introducing the concept of cryptocurrency and blockchain, and developed the first Bitcoin software. According to the white paper, the blockchain infrastructure will support secure P2P transactions without the need for a trusted third party such as banks or governments. Nakamoto's true identity remains a mystery, but there is no shortage of theories.

The Bitcoin/blockchain architecture was introduced and built upon technologies and concepts developed three decades ago. Nakamoto's design also presents the concept of a "blockchain", which allows blocks to be added without the need for confirmation by a trusted third party. Nakamoto defines a cryptocurrency as a "chain of digital signatures", where each owner passes the coin to the next owner by "digitally signing the hash of the previous transaction and the public key of next owner, then add them to the end of the coin".

In 2009, Bitcoin was launched during the Great Recession, when governments were pumping large amounts of money into the economy. At that time, the value of Bitcoin was less than a penny. Nakamoto mined the first Bitcoin block, validating the blockchain concept. This block contains 50 bitcoins and is called the Genesis block, also known as block 0.

Nakamoto released Bitcoin v0.1 to the SourceForge web service as open source software. Currently, Bitcoin is available on GitHub.

The first Bitcoin transaction occurred when Nakamoto sent Hal Finney 10 bitcoins in block 170. The Bitcoin-dev channel was created on the text-based instant messaging system Internet Relay Chat (IRC) for Bitcoin developers . The first Bitcoin exchange - Bitcoin Market - was established, allowing people to exchange paper money for bitcoin. Nakamoto launched the Bitcoin Talk forum to share news and information related to Bitcoin.

In the spirit of cryptocurrency as money with a fixed supply, Nakamoto established a system to ensure that the number of bitcoins mined would never exceed 21 million.

On May 22, 2010, Bitcoin made history when a programmer Laszlo Hanyecz paid 10,000 bitcoins for two Papa John's pizzas to be delivered. The two pizzas were then worth about $40, but if calculated at today's Bitcoin price, this transaction would be worth more than $260 million.

A short time later, Jed McCaleb, a programmer, launched Mt. Gox, a Bitcoin exchange headquartered in Tokyo. Mt. Gox stands for Magic: The Gathering Online eXchange, inspired by a fantasy card game. At its peak, Mt. Gox handles more than 70% of all Bitcoin transactions. However, in August, a hacker exploited a vulnerability in the blockchain's code, creating more than 184 billion bitcoins in block 74,638, severely damaging Bitcoin's reputation. Nakamoto released a new version of Bitcoin software to fix the problem, but by the end of the year, he had completely disappeared from the Bitcoin scene.

In 2011, a quarter of the total 21 million bitcoins were mined. By early February, the value of one bitcoin was equal to the US dollar. Shortly thereafter, McCaleb sold Mt. Gox to Mark Karpelès. Bitcoin also reached parity with the euro and British pound. WikiLeaks begins accepting bitcoin donations. However, Mt. Gox was hacked and bitcoins were stolen, causing an artificial drop in value and resulting trading suspensions. Litecoin was released in October as a spin-off of Bitcoin and is considered the first alternative cryptocurrency.

In 2012, interest in cryptocurrencies became solid. Bitcoin price hovered around $5 for most of the year with some fluctuations. Earlier that year, Mihai Alisie and Ethereum founder Vitalik Buterin launched Bitcoin Magazine and published the first issue in May. A few months later, the Bitcoin Foundation was established to promote Bitcoin and restore public awareness. them about cryptocurrencies after several scandals. McCaleb and Chris Larsen founded OpenCoin, which led to the development of the Ripple trading protocol for real-time currency transactions and payments. Coinbase has raised over $600,000 in its first round of funding and is crowd-funded on its way to becoming one of the leading Bitcoin exchanges.

In 2013, Bitcoin's upward trajectory continued. In February, Coinbase reported selling $1 million in bitcoin in just one month, for more than $22 per bitcoin. By the end of March, with 11 million bitcoins in circulation, the total value of the coin exceeded $1 billion. And in October, the first bitcoin ATM reportedly launched in a coffee shop in Vancouver, BC.

However, it's not all good news for digital currencies. Both Thailand and China ban cryptocurrencies. The United States Federal Court confiscated funds from Mt. Gox in the United States for transferring money without a license. The FBI also shut down the Silk Road black market, confiscating about 144,000 bitcoins worth more than $1 billion, and as a result, owner Ross Ulbricht was sentenced to life in prison for a series of crimes, including drug trafficking , computer hacking and money laundering.

In 2014, despite the obstacles, one of the important milestones in blockchain history took place when Bitcoin Magazine co-founder Vitalik Buterin published a report proposing a

decentralized application platform . This report led to the creation of Ethereum and the Ethereum Foundation. Ethereum has paved the way for blockchain technology to be used for applications beyond cryptocurrencies. It introduces smart contracts and provides developers with a platform to build decentralized applications (dApps). Ethereum provides a major boost to blockchain development, opening up many application opportunities in fields such as finance, supply chain management, and many others.

Financial institutions and other industries have begun to recognize and exploit the potential of blockchain technology, shifting focus from digital currencies to developing blockchain applications. However, Bitcoin remains the center of attention, both positive and negative. Bitcoin exchange Mt. Gox filed for bankruptcy, and the Vice President of the Bitcoin Foundation was arrested for money laundering. At the same time, the British tax authorities classify Bitcoin as private money. Still, several major companies such as the Chicago Sun-Times, Overstock.com, Microsoft, PayPal, and Expedia have begun accepting Bitcoin as of late. This adoption further increases the heat for blockchain.

In 2015, the Ethereum Frontier network officially launched, opening up the possibility for developers to write smart contracts and build decentralized applications on a live network. Ethereum quickly became one of the most prominent applications of blockchain technology, attracting an active developer community and continues to maintain this status today. The same year, Nasdaq began testing the technology blockchain technology, while the Linux Foundation initiated the Hyperledger project to promote enterprise blockchain applications. Notably, nine major investment banks have collaborated to form the R3 alliance to research how blockchain can optimize their operations. In just six months, this alliance has expanded to more than 40 financial institutions globally.

The year 2016 marked a turning point when the term "blockchain" was officially recognized as a single word, instead of being split into two separate concepts as in Nakamoto's original paper. This year, the Chamber of Digital Commerce and the Hyperledger project established a partnership to promote advocacy and education about blockchain technology. Besides progress, 2016 also recorded many notable and challenging events. A vulnerability in the code of the decentralized autonomous organization Ethereum was exploited, forcing the Ethereum network to perform a "hard fork" to resolve the issue. At the same time, the Bitfinex cryptocurrency exchange suffered a serious attack, resulting in the theft of nearly 120,000 bitcoins, equivalent to about 66 million USD at the time.

In 2017, Bitcoin reached a record high of nearly $20,000, marking an important milestone in the history of cryptocurrency. In the same year, Japan officially recognized Bitcoin as a legal currency, creating a great impetus for the development of this market.

Seven European banks have joined forces to form the Digital Trade Chain Consortium, with the goal of developing a blockchain-based trade finance platform. At the same time, software company Block.one launched the EOS blockchain operating system, built on the EOS cryptocurrency and designed to support decentralized applications for commercial purposes.

According to the report, about 15% of global banks have applied blockchain technology to some extent, demonstrating the rapid expansion of this technology in the financial sector.

2018 marked 10 years since Bitcoin was born, but its value dropped sharply, closing the year at about 3,800 USD. In this context, online payment company Stripe stopped accepting payments in Bitcoin, and Google, Twitter and Facebook all banned cryptocurrency advertising, putting more pressure on the market. However, the development of blockchain

technology continues to move forward. South Korea, despite banning anonymous cryptocurrency trading, has pledged to invest millions in blockchain initiatives. The European Commission also launched a Blockchain Observatory and Forum to promote the development of this technology. In China, Baidu – the search engine giant – introduced the BaaS (Blockchain as a Service) open platform, affirming the importance of blockchain in the fields of technology and business.

2019 saw a significant increase in the application of blockchain technology in practical fields. Walmart deploys a supply chain system based on the Hyperledger platform, significantly improving transparency and efficiency in supply chain management.

Amazon also strongly entered the blockchain space with the launch of the Amazon Managed Blockchain service on the AWS platform. This service helps users build resilient Web 3.0 applications on both public and private blockchains, opening up new possibilities for businesses.

At the same time, the Ethereum network recorded a record of more than one million transactions per day, reflecting the rapid growth of decentralized applications (dApps). In this context, blockchain research and development has become a top priority as organizations globally actively apply this technology for a variety of use cases, from finance, healthcare to financial management. products and supply chains.

In 2020, blockchain continues to play an important strategic role, with 40% of businesses implementing it in production and 55% considering it a top priority, according to a survey by Deloitte. Ethereum launches Beacon Chain, preparing for Ethereum 2.0 to improve scalability and security. Stablecoins thrive thanks to their stability compared to traditional cryptocurrencies. At the same time, the combination of blockchain and AI attracts attention, focusing on business process optimization and decentralized data mining.

In 2021, blockchain and cryptocurrency reach important milestones. Bitcoin hit a record high of $68,789.63, with a market capitalization exceeding $3 trillion. Coinbase makes a major listing on the US stock exchange, while the DeFi market grows 600%, reaching a value of 200 billion USD. NFT artwork sold for $69 million, confirming the boom of this field.

Many celebrities, such as Elon Musk and Aaron Rogers, entered the market, with Musk allowing Bitcoin payments for Tesla cars (though later rescinded) and Rogers receiving his NFL salary in Bitcoin.

Blockchain is not only associated with cryptocurrencies but is also widely applied in areas such as voting, real estate, health monitoring, intellectual property, IoT and vaccine distribution during the COVID pandemic. -19. Cloud service providers expand blockchain services, and demand for blockchain developers increases.

According to Statista, the global blockchain market is valued at nearly 6 billion USD in 2021 and is forecast to surpass 1 trillion USD by 2030, showing the strong growth potential of this technology in the future.

In 2022, NFTs continue to grow, eco-friendly blockchain networks emerge, and blockchain applications increase among companies. Bitcoin mining activities getting closer to Nakamoto's limit of 21 million coins, reaching 19 million with less than 10% of the bitcoins left to mine.

The prices of Bitcoin and other cryptocurrencies plummeted in the spring after reaching all-time highs, due to concerns from investors about inflation and the emergence of the Omicron variant of COVID-19. Several cryptocurrency exchanges have declared bankruptcy.

The collapse of the FTX exchange and the arrest of CEO Sam Bankman-Fried have raised concerns about risks in the cryptocurrency industry. Open source blockchain platform Terra has also collapsed. Speculation about new US government regulations on cryptocurrencies has increased uncertainty, but is also expected to help legitimize the industry.

Globally, Danish shipping company Maersk announced the closure of its blockchain-based digital ledger TradeLens, which it co-developed with IBM, due to lack of participation from participating parties. At the same time, the Australian Stock Exchange canceled a seven-year plan to move its trading platform to blockchain. According to Statista, more than 100 countries have participated in the development of central bank digital currencies (CBDC). CBDCs are digital versions of real-world fiat currencies, intended to speed up cross-border retail transactions on the blockchain, in contrast to the slow speed and price volatility of cryptocurrencies.

Claims about the inviolability of blockchain have come under attack, and not just figuratively. Blockchain analytics firm Chainalysis has identified nearly 200 cryptocurrency or blockchain hacks, causing losses of up to $3.8 billion. The most notable incident occurred when video game blockchain Ronin Network reported the theft of $625 million in Ether and stablecoin USDC. The US Treasury Department blamed a group of hackers from North Korea for the attack.

In 2023, the cryptocurrency industry continues to face major challenges as the US Securities and Exchange Commission (SEC) indicts the executives of two major exchanges, Coinbase and Binance. At the same time, the SEC also filed a lawsuit against businessman Justin Sun and three companies he wholly owned for allegedly conducting unregistered offerings and sales of cryptocurrency securities.

Businesses continue to deploy blockchain technology, but with more caution than before. Currently, blockchain is mainly applied in the financial and banking sectors, but other potential fields are also gradually being explored, including games, media and entertainment, real estate, health care. health, cybersecurity, smart contracts, NFTs, IoT, transportation, supply chain management, and public administration. In particular, Web 3.0 - the latest version of the internet - with its ability to provide decentralization and data security, is being considered the biggest driving force promoting the development of blockchain technology.

Bitcoin has now stabilized at a relatively solid price range between $25,000 and $30,000. According to Satoshi Nakamoto's original design, Bitcoin mining will gradually approach a maximum limit of 21 million coins, expected to be reached around the year 2140.

After 2023, several trends are expected to contribute significantly towards achieving a trillion-dollar valuation of blockchain technology, including:

- Expanding DeFi (Decentralized Finance) Applications: DeFi protocols continue to grow, bringing transparent and decentralized financial solutions to global users.

- The rise of Web 3.0: The decentralized Internet, with blockchain-based applications, will open up huge potential for data security and privacy.

- Integrating blockchain into supply chain management: Ensuring transparency and traceability in global supply chains.

- NFTs and digital assets: The evolution of NFTs continues to shape the way digital assets are owned and traded in sectors such as art, entertainment, and sports.

- Applications in the field of IoT: Combining blockchain with the Internet of Things (IoT) to improve security and device management.

- Advanced smart contracts: Use of self-executing contracts is increasingly common in the legal, real estate, and healthcare sectors.

- Digital transformation in government: Blockchain has the potential to revolutionize data management, elections and public services in many countries.

2.3. TYPES OF BLOCKCHAIN NETWORKS

There are four main types of blockchain networks: public blockchain, private blockchain, consortium blockchain, and hybrid blockchain. Each of these network types has its own characteristics, with different benefits, drawbacks, and ideal applications. We will explore each platform in detail.

2.3.1. Public blockchain

How it works: Public blockchain is where cryptocurrencies like Bitcoin were born, helping to popularize distributed ledger technology (Distributed Ledger Technology - DLT). This technology solves the problems of centralization, including poor security and transparency. DLT does not store information in a single location, but distributes information across a peer-to-peer network. The decentralized nature of blockchain requires the use of methods to verify the authenticity of data. One of these methods is the consensus algorithm, which helps members of the blockchain network reach agreement on the current state of the ledger. The two most popular consensus methods are Proof of Work (PoW) and Proof of Stake (PoS).

Advantage: One of the advantages of public blockchain is its complete independence from institutions. This means that, even if the organization that initiated the blockchain no longer exists, the public blockchain network can still operate as long as there are still computers connected to it. According to James Godefroy, principal and vice president of enforcement at Rouse, an intellectual property services provider, "Some blockchains incentivize users to commit their computing power to network security by providing award."

Another advantage of public blockchain is network transparency. As long as the user Strict adherence to security protocols and methods, public blockchains are mostly secure.

Disadvantages: Public blockchain networks may experience speed issues, and companies cannot restrict access or usage. One of the potential risks is that if hackers capture 51% or more of the network's computing power, they could unilaterally change data in the blockchain. James Godefroy said this is one of the risks facing public blockchain networks.

Use case: The most popular use case of public blockchain is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be applied to create permanent records with an auditable chain of custody, for example to electronically notarize affidavits or create public records of asset ownership .

This type of blockchain is especially suitable for organizations that rely on transparency and trust, such as social support groups or NGOs. However, due to the public nature of the network, private businesses will likely want to avoid using public blockchains.

2.3.2. Private blockchain

How it works: A private blockchain operates in a limited environment, such as a closed network or under the control of a single entity. Although it uses the same decentralized

and peer-to-peer connections as public blockchains, private blockchains are much smaller in scale. Instead of allowing anyone to participate and provide computing power, private blockchains are typically operated on a small network within a company or organization. This type of blockchain is also known as permissioned blockchain or enterprise blockchain.

Advantage: The entity that controls the private blockchain will establish permissions, security, authorization, and accessibility levels. For example, an organization setting up a private blockchain network can determine which nodes have permission to view, add, or change data, and can also prevent third parties from accessing certain information.

“You can think of private blockchains as intranets, while public blockchains are more like the internet,” said James Godefroy.

Because of their smaller scale, private blockchains can be very fast and process transactions much more efficiently than public blockchains.

Disadvantages: Disadvantages of private blockchains include the controversial claim that they are not "real" blockchains, as the core philosophy of blockchain is decentralization. Furthermore, achieving complete trust in the information becomes more difficult, as centralized nodes decide which information is valid. A low number of nodes can also mean poorer security. If a few nodes operate illegally, the consensus method may be compromised.

Additionally, the source code of private blockchains is often proprietary and closed, making it impossible for users to independently inspect or verify. This can lead to a lower level of security. Additionally, private blockchains do not support anonymity, which reduces the ability to protect user privacy.

Use cases: The speed of private blockchains makes them an ideal choice in situations where the blockchain needs to be cryptographically secured but the controlling entity does not want the information to be accessible to the public.

“For example, companies can choose to leverage blockchain technology without giving up their competitive advantage to a third party,” said James Godefroy. “They can use private blockchain to manage trade secrets.” , audit."

Other use cases for private blockchain include supply chain management, asset ownership, and internal voting, where security and access control are important.

2.3.3. Blockchain

How it works: Hybrid blockchain combines elements of both private and public blockchain. It allows organizations to set up a private, permission-based system alongside a permissionless public system, allowing them to control who can access Specific data is stored in the blockchain and what data will be made publicly available.

Typically, transactions and records in a hybrid blockchain are not public but can be verified when needed, such as by allowing access through smart contracts . Confidential information is kept inside the network but can still be verified. Although a private entity can own the hybrid blockchain, it cannot change the transactions.

When users join a hybrid blockchain, they have full access to the network. The user's identity is protected from other users, unless they participate in a transaction. Their identities are then revealed to the other party.

Advantage: One of the big advantages of hybrid blockchain is that because it operates in a closed ecosystem, outside hackers cannot carry out a 51% attack on the network. It also

protects privacy but allows communication with third parties. Transactions are cheap and fast, and it offers better scalability than public blockchain networks.

Disadvantages: This type of blockchain is not completely transparent because information can be hidden. Upgrading can also be a challenge, and there is no incentive for users to join or contribute to the network.

Use cases: Hybrid blockchain has several strong use cases, including real estate. Companies can use hybrid blockchain to run private systems but expose certain information, such as listings, to the public. Retail can also streamline its processes with hybrid blockchain and highly regulated marketplaces such as Financial services may also see benefits in using it .

According to Godefroy, medical records can be stored in a hybrid blockchain. Profiles cannot be viewed by random third parties, but users can access their information through smart contracts. Governments can also use it to store citizen data privately but share information securely between organizations.

2.3.4. Linked Blockchain

How it works: The fourth type of blockchain, confederation blockchain, also known as federation blockchain, combines the features of public blockchain and private blockchain. However, the difference is that multiple organizations cooperate on a decentralized network. Essentially, a consortium blockchain is a private blockchain with limited access, allowing only a specific group to participate, which eliminates the risks associated with just one entity controlling the network as in private blockchains. .

In the consortium blockchain, consensus procedures are controlled by pre-established nodes. It has a validator node that initiates, receives, and verifies transactions. Member nodes can receive or initiate transactions within the network, facilitating collaboration between organizations in a secure and controlled environment.

Advantage: Federated blockchains tend to be more secure, scalable, and efficient than public blockchain networks. Like private blockchain and hybrid blockchain, it also provides access control.

Disadvantages: Federated blockchains are less transparent than public blockchains. It can still be compromised if a member node is breached, and the blockchain's own regulations can weaken the network's functionality.

Use cases: Banking and payments are two applications of this type of blockchain. Different banks can join together and form a consortium, deciding which node will validate transactions. Research organizations could create a similar model. Alliance blockchain is ideal for supply chains, especially food and medicine applications.

2.4. CRYPTOCURRENCY AND TOKENOMICS

2.4.1. Cryptocurrency

2.4.1.1. Concept

Cryptocurrency or electronic money is a digital currency designed to operate through a computer network, independent of any central authority, such as a government or bank...

Cryptocurrency is a form of digital currency that uses cryptography to secure the processes involved in creating units, conducting transactions, and verifying the exchange of ownership of the currency.

Most modern currencies are commonly referred to as "currencies"**fiat**", managed and produced by a government entity. For example, the US dollar is a fiat currency. In contrast, cryptocurrencies are not issued by any government agency. It is usually is not directly managed by a single authority but operates under a distributed consensus approach.

Cryptocurrency gets its name from the combination of "cryptography" and "currency". At the heart of all cryptocurrencies is a cryptographic algorithm encryption complicated . Cryptocurrencies are created by solving part of an algorithm hash password in a long string. It is not a physical unit, like a penny or a dollar bill, but a mathematical calculation. Crypto assets are typically stored in one digital wallet to track cryptocurrencies.

One Distributed, decentralized ledger monitors all cryptocurrency transactions worldwide. One of the most famous cryptocurrencies is Bitcoin, introduced in 2009. Since then, cryptocurrencies have become extremely popular. According to some estimates, there are more than 10,000 digital currencies in circulation worldwide.

Unlike traditional currencies, which are approved by a country as legal tender and regulated by the national government and central bank, cryptocurrencies are largely unregulated and do not have a financial entity. Which overarching government oversees its use?

What is cryptocurrency?

Cryptocurrencies are cryptographically protected digital currencies that help ensure the security and authenticity of transactions. This is a digital asset commonly used as a medium of exchange in transactions. Cryptocurrencies operate globally, are not limited by time zones, and operate 24/7. In particular, cryptocurrencies are independent of intermediaries such as banks and payment processors, helping to reduce transaction costs and processing times.

The decentralized nature of cryptocurrencies supports direct person-to-person transactions (P2P). So instead of using hardware wallets and bank accounts, people access cryptocurrencies through these cryptocurrency wallet or unique cryptocurrency exchanges like Binance, Remitano, BitMart, …

First cryptocurrency?

Bitcoin is the first and most famous cryptocurrency. Bitcoin is named by a person or group of people as “Satoshi Nakamoto” created in 2009. Since then, thousands of cryptocurrencies have emerged, each with its own characteristics and purposes.

Like traditional fiat currencies, cryptocurrencies can be used as a medium of exchange. However, the uses of cryptocurrencies have evolved significantly over the years and now include many applications in many industries such as decentralized finance (DeFi), artificial intelligence, gaming, management, healthcare, digital collectibles, and many other industries.

2.4.1.2. What are the main characteristics of cryptocurrencies?

- Cryptocurrencies are digital currencies protected by cryptography. Cryptocurrencies are powered by blockchain technology, allowing users to send and receive assets through a decentralized peer-to-peer (P2P) network.
- Bitcoin, ETH, BNB, USDT and SOL are examples of the top cryptocurrencies by market capitalization.

- Users access cryptocurrencies through cryptocurrency wallets or exchanges. Although people often say that cryptocurrencies are "stored" in wallets, balances are actually recorded on the blockchain.

How does cryptocurrency work?

Blockchain network

Most cryptocurrencies are decentralized, meaning they use a distributed network of computers (node) to manage and record transactions in a public ledger called blockchain.

So, whenever you send bitcoin to a friend, your transaction must be jointly verified and authenticated by the network's nodes.

Each computer node must maintain a local copy of the blockchain and update that copy every time new data is added to the ledger. Once authenticated and confirmed, cryptocurrency transactions are permanently recorded in the blockchain database.

This distributed architecture increases network security because there is no single point of failure for bad actors to exploit. If a node attempts to validate invalid transactions or behaves improperly, that node will be promptly expelled from the network.

Cryptography

Cryptocurrencies used code to secure transactions, maintain data integrity, and control the creation of additional units. When you open a wallet and make a cryptocurrency transaction, you are essentially using private key yours to create digital signature. The network will then check your signature. If everything is fine, your transaction will be added to one block new.

Blockchain is a series of linked blocks, so you can think of each block as one of many pages on the blockchain ledger. Each block contains a unique list of cryptocurrency transactions, along with other information.

2.4.1.3 Classification of cryptocurrencies?

To date, there are many different types of cryptocurrencies, just as there are many different types of fiat currencies issued by global governments. While Bitcoin Arguably the most famous cryptocurrency, many other cryptocurrencies have emerged over the years. Including Dogecoin and Ethereum popular on the internet. Here is a breakdown of popular cryptocurrencies:

Bitcoin

Bitcoin, the first cryptocurrency, was launched in 2009 and created by a person named Satoshi Nakamoto, BTC is the first and most famous cryptocurrency. Bitcoin is widely used as a store of value and medium of exchange.

Bitcoin uses a consensus mechanism called **proof-of-work (PoW)**, in which miners compete with each other to validate transactions and receive rewards in the form of blocks. This process requires computing power to solve complex problems, helping to ensure network security.

Also, with limited supply only **21 million coins**, Bitcoin became relatively scarce and is often considered "digital gold", because this scarcity increases its value and appeal as a long-term investment asset.

Not all cryptocurrencies ***Bitcoin*** commonly called ***altcoin***.

Some popular altcoin cryptocurrencies:

Ether (ETH)

Ether (ETH) is the native coin of the blockchain Ethereum. Created by Vitalik Buterin, Ethereum provides a decentralized network where developers can build DApps using smart contracts.

Initially, Ethereum used a proof-of-work consensus mechanism but has since switched proof-of-stake (PoS) to increase efficiency and reduce energy consumption. This change allows users to authenticate transactions and secure the network by stake ETH instead through nodes using computing power.

Cardano (ADA)

Cardano (ADA) launched on September 29, 2017. This was the moment when the Cardano network officially went live, and the ADA coin began to be traded on cryptocurrency exchanges. Cardano is developed by IOHK (Input Output Hong Kong), with the goal of creating a secure, sustainable and highly scalable blockchain platform.

Cardano (ADA) is an open source blockchain platform founded by Charles Hoskinson, aiming to provide a secure and sustainable system for distributed applications and smart contracts. Cardano uses a Proof of Stake (PoS) consensus mechanism called Ouroboros, which saves energy and increases scalability. It has an architecture separated into two layers: Settlement Layer (SL) for transactions and Computation Layer (CL) for smart contracts. Cardano supports smart contracts through the Plutus language, with the goal of providing interoperability between different blockchains and sustainable development. ADA token is the main currency, used in transactions and staking.

BNB

BNB launched in 2017 as token ERC-20 on the Ethereum blockchain. In 2019, BNB migrated to its own blockchain and is now the ecosystem's native cryptocurrency BNB Chain.

Similar to Ethereum, BNB Chain provides an environment for smart contracts and DApps, with lower transaction fees and faster processing times than other blockchains.

BNB has many uses, including staking, paying transaction fees on BNB Chain and Binance, as well as participating in token sales on Launchpool. In addition, the BNB automatic burning mechanism helps reduce supply and create scarcity, contributing to maintaining the value of this coin.

Tether (USDT)

USDT is a USD-pegged stablecoin developed by Tether Limited Inc. launched in 2014. Stablecoins is a cryptocurrency designed to always maintain value with a reserve asset, such as the US dollar or another fiat currency.

In the case of USDT, each token is backed by an equivalent amount of assets held in the company's reserves. Stablecoins like USDT eliminate the additional costs and delays that are common when switching back and forth between crypto and fiat.

Litecoin

As an altcoin or original Bitcoin alternative, Litecoin initially emerged thanks to its use of the Scrypt hashing algorithm, which proponents say is easier to manage than the SHA-256 encryption used by Bitcoin. Litecoin, codenamed LTC, was first released in 2011 by author Charlie Lee; Market capitalization is estimated at approximately 12 billion USD.

Solana (SUN)

SUN is the native cryptocurrency of the Solana blockchain. Solana is a third generation PoS blockchain launched in 2020. Solana has made many unique improvements to deliver high throughput, fast transaction speeds, and low fees.

2.4.1.4. Applications of cryptocurrency in the economy

Cryptocurrency is increasingly accepted and widely used by many different industries and sectors in the economy in many different countries. The application of cryptocurrency in the economy is concentrated in three main areas. Weaknesses include: Payment, money transfer, and investment.

Money transfer service

One of the biggest uses of cryptocurrencies (especially Litecoin-LTC, Stellar Lumen-XLM and Bitcoin Cash-BCH) is the ability to conduct large-scale transactions in real time. short and low cost based on the blockchain technology platform of cryptocurrencies. For example, a $99 million LTC transfer was performed within 2.5 minutes and cost the sender only $0.40 in transaction fees (Lielacher, 2018). The money transfer process, including time and cost, is considered superior compared to the cost of money transfer services at financial institutions.

Pay

Cryptocurrency is also accepted by some organizations and units to pay for transactions or reward employees and participating members. For example, the world's leading blogging and social networking platform, Steemit (https:// steemit.com/) rewards members with cryptocurrency for posts on the site and for their contributions. Members are responsible for managing the content posted on the site to encourage site members to increase the quality of content posted on the site (Lielacher, 2018). Statistics from Statista (2020) also show that the number of Blockchain e-wallet accounts in the world increased nearly 5 times, from 8.95 million wallets in the third quarter of 2016 to nearly 44.7 million wallets by the end of the fourth quarter/ 2019 (Figure 4).

Some travel companies such as CheapAir and Destinia also accept Bitcoin in payment for air tickets, vehicle rental services, and hotel services (Lielacher, 2018). Payments while traveling are also becoming easier for individuals and organizations that own cryptocurrency as the Bitcoin ATM market is becoming more and more popular around the world, meaning users can exchange money. encrypted into local fiat currency in many major tourist cities around the world. The coinmap statistics shown in Figure 1 above also show the level of widespread application and acceptance by economic participants of Bitcoin in particular and cryptocurrencies in general in the field of payment.

Capital mobilization and Investment

Raising capital through initial coin offerings (ICOs) is becoming increasingly popular and has important implications for startups operating in the field of blockchain technology, especially Especially small-scale businesses that have difficulty accessing traditional sources of capital funding from financial institutions or through capital mobilization on the stock market.

In terms of terminology, “cryptocurrency” in the name ICOs – refers to tokens issued by specific projects or issuers, not cryptocurrencies created with separate blockchain technology such as Bitcoin, Eutherem... Types of digital assets such as "tokens" and

"cryptocurrencies" ("coins") are often used interchangeably in terms of terminology, although In terms of nature and characteristics, they are completely different.

To raise capital through cryptocurrency issuances, issuers (blockchain startups) often have to have their own currency systems (which are cryptocurrencies - private digital assets, often called cryptographic “tokens”). These tokens will be priced by the issuer and sold to investors in cryptocurrency. Investors can then hold the tokens or sell the tokens on the secondary market in exchange for cryptocurrency. However, the secondary market for tokens is relatively illiquid (Lipush, 2018).

Unlike the issuance of securities, which must comply with strict regulations of the Ministry of Finance, the issuance of cryptocurrency to mobilize capital is largely not subject to the management of authorities. Issuing organizations only need to have a business idea and white paper (report of issuance information and capital use purposes), instead of having to have a Prospectus in the issuance dossier as required by an issuance plan. securities) is possible to organize capital mobilization in cryptocurrency.

2.4.2. Tokenomics

2.4.2.1. Concept

In traditional economics, the production, distribution, and consumption of goods are often accompanied by means of exchange such as currencies and commodities. Currency is the most popular medium of exchange, helping to simplify the buying, selling and pricing of goods and services. Before the advent of money, direct barter (barter) was a common form, in which one commodity was exchanged for another of equal value. Similarly, in the blockchain ecosystem, the method of exchange, management and circulation is digital tokens (also known as tokenomics). Tokenomics refers to the economic factors related to the development, distribution and use of tokens in the blockchain, which play a similar role to currencies in the traditional economy.

Understanding tokenomics is paramount for anyone involved or interested in the world of cryptocurrency, as it directly affects the value, utility, and potential of a digital asset. Let's dig deeper to grasp the fundamental concepts and discover why tokenomics is pivotal to the future of decentralized finance, and the future digital economy.

What is Tokenomics?

*“**Tokenomics** is a term combining "token" and "economics", used to refer to economic factors related to the creation, distribution, use and management **token** in blockchain ecosystems. Tokenomics is key to ensuring the growth and stability of a cryptocurrency project, as it directly affects the value, utility, and potential of the token.”*

Let's take a look What is crypto token? . This is a digital currency built by crypto projects on existing blockchains. Like any regular currency, crypto tokens hold a certain value and are exchangeable.

In terms of economics, it is important to understand how the token economy differs from the traditional economy. Regardless of the era in history, governments create more money without any basis in reality. From conflict to war or dealing with drought can be very costly. To solve this problem, raising revenue was not always an option, and the authorities found that minting coins was a simpler alternative. Creating more money will eventually reduce the value of the existing currency.

However, cryptocurrency projects pre-determine and algorithmically create release schedules for tokens. We can accurately predict the number of coins in circulation at a

particular time. The distribution of coins among different stakeholders is also considered in advance. While it is technically possible to change release schedules and distribution plans, the process is difficult to do.

For example, Bitcoin shows how the tokenomics design of a token is quite simple and ingenious. The total supply of Bitcoin is pre-programmed with a maximum amount of 21 million tokens. Bitcoins are created and released through a mining process, in which miners are rewarded with a set amount of Bitcoins when blocks are mined approximately every 10 minutes.

This reward, also known as the block subsidy, will be halved every time 210,000 blocks are mined. According to this schedule, each halving will occur every four years. Based on these rules, we can easily calculate the number of Bitcoins mined annually and predict that the last Bitcoin will be mined around the year 2140.

Bitcoin's tokenomics also includes the design of transaction fees, which miners receive when a new block is confirmed. This fee is designed to increase as transaction size and network congestion increase. It helps prevent spam transactions and incentivizes miners to continue validating transactions even when the block subsidy gradually decreases.

In short, Bitcoin's tokenomics is simple and ingenious, all transparent and predictable. The incentives surrounding Bitcoin reward participating members for keeping the network strong and contributing to its value as a token.

2.4.2.2. Classify

Tokenomics (token economics) refers to the design, management and analysis of token ecosystems in blockchain projects. Tokenomics classification is often based on aspects related to the purpose, function, and how the token operates. Here is a common classification:

a) Classification according to intended use

Utility Token (Utility Token):

Utility Token, also known as Utility Token, is a cryptocurrency created and used for specific purposes within the ecosystem of a blockchain project. Utility Token does not represent ownership or shares in the business.

Utility Tokens are designed to provide access to a product, service, or blockchain platform.

For example: Ethereum (ETH) to pay transaction fees, Binance Coin (BNB) to reduce transaction fees on Binance exchange.

Security Tokens:

Token represents a real asset or investment interest (e.g. stock, bond). They are often governed by financial regulations.

Security Token, also known as Securities Token, is a type of cryptocurrency that represents ownership or economic interest in an asset or project. It is issued on a blockchain platform and complies with securities legal regulations.

Security Token represents ownership of assets (stocks, bonds, real estate...), traded on centralized or decentralized exchanges that support security token trading but must be legally regulated. securities management.

For example: Tokens issued under STO (Security Token Offering); Securitize; tZERO.

Governance Token (Governance Token):

Provides voting rights to holders in decisions related to project development or management.

Governance tokens are tokens that developers create to allow token holders to help shape the future of a protocol. Governance token holders can influence project-related decisions such as proposing or deciding on new feature proposals and even changing the governance system itself.

In many cases, changes are proposed, vetted, and then voted on through on-chain governance accessed using governance tokens applied automatically by smart contracts. In other cases, the project maintenance team is tasked with applying the changes or hiring people who will do so.

Proponents of systems that use governance tokens believe they give users control, which is true to cryptocurrency's original ideals of decentralization and democratization. In most cases, organizations that allow users to control the development of their systems are called decentralized autonomous organizations (KNIFE).

A famous example of a governance token is Maker (MSEK). This token allows holders to vote on decisions related to decentralized finance protocols (DeFi) which decentralized stablecoins COME ON run on it.

Each governance token a person holds is typically equivalent to a vote on upcoming proposals, but there are other methods. Those with governance tokens can use them to accept or reject changes to a decentralized application (dApp) or blockchain during scheduled voting periods. Many dApps also allow people to use their governance tokens to create initiatives and put them up for voting.

Payment Tokens:

Payment tokens are used as an alternative means of payment and exchange. Unlike fiat currencies such as the US Dollar, Euro or Japanese Yen, payment tokens such as Bitcoin are not legal tender and are not backed by governments. Instead, their main goal is to be a decentralized tool for buying and selling goods and services without the need for a traditional intermediary and with no other functionality (or only limited functionality). .

For example, in one consultation article announced in January 2019, the UK's FCA has confirmed that Payments or Exchange tokens - as the FCA calls them - "are currently outside the scope of regulation. This means that the transfer, purchase and the sale of these tokens, including the trading by cryptocurrency exchanges for exchange tokens, are activities that are not currently regulated by the FCA."

Muscle Swiss regulator FINMA also does not consider payment tokens as securities but emphasizes that if they are classified as securities through new legislation or legal documents, FINMA will amend its operations.

Furthermore, it is worth noting that with the upcoming amendments to the EU money laundering directive (“AMLD 5”) needs to be implemented in each member state by 10 January 2020, stricter AML rules will apply to entities carrying out activities such as exchanges between assets cryptocurrencies and fiat currencies, between one or more other forms of crypto assets, transfer of crypto assets, custody or management of crypto assets, or instruments allowing control of crypto assets encode, join and provide the financial services related to the issuer's offer or sale of cryptocurrency assets.

Stablecoin (Price Stable Token):

Stablecoins value attached to a stable asset such as fiat currency (USD, EUR) or gold; For example: Tether (USDT), USD Coin (USDC).

Stablecoins are a type of cryptocurrency that seek to maintain a stable value by tying their market value to an external reference. This reference can be a fiat currency like the US dollar, a commodity like gold, or another financial instrument. The main goal of stablecoins is to provide an alternative to the high volatility of popular cryptocurrencies like Bitcoin (BTC), which can make these digital assets less suitable for regular transactions.

Stablecoins play an important role in the cryptocurrency ecosystem due to their stability. Cryptocurrencies like Bitcoin and Ether offer many benefits, such as not needing to trust an intermediary to send payments anywhere and to anyone. However, their prices are unpredictable and can fluctuate wildly, making them difficult to use on a daily basis. Stablecoins aim to address these price fluctuations by tying the value of cryptocurrencies to more stable assets, typically fiat currencies. This stability is intended to maintain their value over time and encourage their adoption in frequent transactions.

b) Classification according to issuance and management mechanism

Inflationary Token:

Token inflation is the increase in the number of tokens in circulation over time. When token inflation occurs, the value of each token will decrease and the value of investors' assets will also be affected if supply exceeds demand.

Several factors can lead to token inflation:

- Increase the number of tokens in circulation due to unlocking activities to unlock tokens according to the roadmap.
- The project was attacked, hackers created many tokens to put into circulation.
- The project's activities encourage users to lock and stake, helping to temporarily reduce the amount of tokens in circulation. If these policies are unattractive, the amount of new tokens put into circulation is greater than the amount of locked tokens, which will also result inflationary.

In summary, the main factors leading to token inflation include increasing the number of tokens, lack of demand, changes in issuance policies, market impacts, being attacked and being out of sync with market demand. school. In summary, the main factors leading to token inflation include increasing the number of tokens, lack of demand, changes in issuance policies, market impacts, being attacked and being out of sync with market demand. school.

Deflationary Token (Deflationary Token):

Deflationary tokens are increases in the intrinsic value of a cryptocurrency over time as supply decreases or remains constant.

Token Deflations take a different approach, as they are designed to reduce token supply. While demand is steady, reducing the number of new coins will at least maintain their value.

The design of a deflationary cryptocurrency aims to achieve token scarcity by reducing supply and increasing the value of tokens over time. This process hopes to gradually reduce the number of tokens and maintain real-world usefulness without disturbing balance or causing market volatility.

Deflationary tokens, unlike inflationary tokens, do not have a fixed deflation rate in their protocol. Instead, the protocol stipulates the conditions for removing tokens from

circulation, usually through a token burning process. This mechanism reduces supply over time, but the rate of reduction is not set for a specific period of time but varies depending on network activity. For example, a token with a 2% deflation rate will reduce its total token supply by 2% per year. A deflationary token can have a fixed or variable supply limit, limiting the number of tokens issued.

Creators of deflationary tokens can use direct or indirect mechanisms to destroy coins in circulation. A popular way to reduce supply is to use a token burn mechanism, a process that permanently removes a portion of tokens from circulation. Additionally, they can also burn some tokens as gas fees for transactions on the blockchain.

An example of a deflationary cryptocurrency is Binance Coin (BNB). Every quarter, Binance holds a coin burning event to eliminate excess BNB. In addition, Binance also burns a portion of BNB as transaction fees. Binance pledges to burn 50% of the total supply of BNB.

Fixed Supply Token (Token with fixed supply):

Some cryptocurrencies, like Bitcoin, follow a fixed token supply model. This means that the total number of tokens that will exist is predetermined and cannot be changed. For example, Bitcoin has a fixed supply of 21 million coins, and when they are all mined, no new Bitcoins will be created. A fixed token supply creates scarcity, as the number of available tokens is limited, leading to a potential value increase over time as demand increases.

This scarcity is often cited as one of the reasons behind Bitcoin's value, as it mirrors the properties of precious metals such as gold, which also have a limited supply. Investors and enthusiasts believe this scarcity contributes to Bitcoin's potential as a store of value and a hedge against inflation in traditional fiat currencies.

c) Classification by release method

Pre-Mined Token:

All tokens are issued before the project launches; for example Ripple (XRP), ADA,...

While Bitcoin releases new coins into circulation through mining, some cryptocurrencies, such as Ripple, Cardano, and Stellar, are "pre-mined," meaning a portion of the coins have already been mined and distributed in advance. The project's official launch date.

When a cryptocurrency is pre-released, it simply means that a portion of that currency's coins or tokens were created - and in some cases, distributed - before its official launch. that cryptocurrency. In contrast to Bitcoin, which releases new coins when exploit takes place, some cryptocurrency projects pre-create their currencies before the official launch.

For pre-mined cryptocurrencies, a portion of the coin supply is created immediately upon launch in the first block of the protocol and distributed to ICO investors, developers and group members. For example, Ripple (XRP) was created as a cryptocurrency for a centralized payment system, allowing for quick and cost-effective money transfers in partnership with banks. However, the majority of XRP coins are still held by Ripple and this company centrally controls the issuance of the coin. Unlike mineable cryptocurrencies like Bitcoin or Litecoin, pre-mined coins or tokens are usually issued by a centralized organization.

Before switching to Proof-of-Stake (PoS), Ethereum was both a pre-mined and a mined token at the same time. Ether was first offered as a pre-mining reward to those who funded the Ethereum project during its initial coin offering (ICO) in July and August 2014.

Pros and cons of pre-mining cryptocurrencies:

At present, pre-mining has generally been widely accepted by the cryptocurrency community, as many coins and tokens are distributed this way through ICOs and other forms of offering other tokens. Some people argue that pre-mining cryptocurrencies is justified in order to reward the developers who participated in its creation and did the work required to give the initial impetus to the coin. cryptocurrency. Pre-mined coins and distributed to development team members can serve as an incentive for employees and early adopters.

A pre-mine is also a proof to investors that the coin or token that has been created actually works. A pre-released coin can be used as a prototype to present to interested parties.

On the other hand, critics say that pre-mining mainly serves ICO startups to pump and dump their cryptocurrency. “Pump and dump” is a form of investment fraud in which the value of an asset purchased at a low price is artificially inflated in order to sell it at a higher price.

Minted Token:

Tokens are released gradually during the operation of the network. For example, Bitcoint (BTC) adopts Proof-of-Work mechanism, Ethereum (ETH) adopts Proof-of-Stake mechanism.

Minting is the process of issuing new digital assets in the cryptocurrency ecosystem. This method puts new coins or tokens into circulation, allowing them to be traded or used within the ecosystem. In many ways, minting is similar to mining. However, there are a few important differences.

Proof of Stake (PoS) systems use minting to put new coins into circulation. This system relies on validators or stakers to verify transactions and add new blocks to the blockchain.

On the other hand, mining is associated with the Proof of Work (PoW) mechanism. In these systems, miners use specialized hardware to solve complex cryptographic problems to create new blocks on the blockchain.

While mining is a process that consumes a lot of energy, minting is much more environmentally friendly. Unlike minting, which only happens once when a new token is created, mining is a continuous activity. It remains active throughout the blockchain network, continuously verifying transactions and reinforcing the security of the network.

In addition to regular cryptocurrency units, minting is also an indispensable process to create Non-Fungible Tokens (NFTs). Typically, the process of minting an NFT includes the following steps:

Step 1: Create or select digital assets

This asset can be an image, video, music, or any type of digital file that the creator wants to turn into an NFT.

Step 2: Choose platform and blockchain

Creators choose the NFT minting platform (e.g. OpenSea, Rarible, Mintable) and the blockchain on which the NFT will live (e.g. Ethereum, Binance Smart Chain, Solana).

Step 3: Create smart contract (Smart Contract)

The smart contract will define the parameters of the NFT, including ownership, transfer, and other conditions.

Step 4: Mint NFT

The minting process begins when the asset is uploaded to the platform and the smart contract is activated. This creates a unique token on the blockchain, confirming ownership and uniqueness of the asset.

Step 5: Pay gas fees (if any)

Gas fees are the payment costs for transactions on the blockchain, and in the case of Ethereum, they can be quite high. Creators must pay gas fees to complete the minting process.

Step 6: Sell or transfer the NFT

Once the NFT is minted, the creator can sell it on NFT marketplaces or transfer it to someone else.

Airdrop Token:

Released for free to users to encourage participation or promote the project.

A cryptocurrency airdrop is a project that distributes new tokens or coins to many individuals in the cryptocurrency community.

The teams behind these projects often use airdrops to raise awareness about their projects and encourage people to become users or investors. Airdropped assets are given away for free, but some airdrops require users to complete specific tasks before they can claim their tokens. Cryptocurrency airdrops became popular during the initial coin offering (ICO) boom of 2017, but are still used by many crypto projects today.

When a project announces an airdrop, it often also sets out specific criteria or requirements that participants must meet to qualify. These requirements may include joining a specific Telegram group, following the project on social media, subscribing to a newsletter, or holding a minimum amount of a specific coin in a wallet. Airdrops can also only be given to wallets that have interacted with the project's platform before a set date.

However, these criteria are not always announced in advance. Some famous airdrops have surprised active users of the platform by airdropping new tokens before revealing the airdrop criteria. There are no rules for airdrops and each project can have its own methods and plans.

“Why Do Crypto Projects Do Airdrops?”

Cryptocurrency projects often use airdrops as part of their token launch strategy to raise awareness within the crypto community and encourage recipients to use their tokens. Airdrops can also be used to distribute tokens to users or potential investors fairly by ensuring that the initial supply is distributed among many, rather than being concentrated in the hands of a few. initial investment. This distribution model can contribute to a more balanced and decentralized ecosystem.

Airdrops were also initiated as part of the project's marketing strategy to create buzz and attract attention to the project. Recipients may be curious about the project and explore it further or discuss it on social media. This increased exposure could lead to a larger pool of users, investors, and potential partnerships.

Airdrops can also improve user adoption because free tokens encourage people to directly experience the benefits of their cryptocurrency. This can encourage users to participate in the project and provide valuable feedback. This can help improve the platform over time.

d) Classification according to economic value

Asset-Backed Token (Asset-Backed Token):

Asset-backed tokens are digital claims to a physical asset and are backed by that asset. Gold, crude oil, real estate, stocks, soybeans or almost any other real physical asset can be tokenized and become an asset-backed token.

Asset-backed tokens are an evolution created thanks to blockchain technology. Bitcoin, of course, was the first token, but this cryptocurrency is not backed by any physical assets. Since Bitcoin, a lot has changed and there are now thousands of different cryptocurrencies, from new digital coins to stablecoins tied to fiat currencies. However, the cryptocurrency revolution and its volatility have spurred the creation of more stable tokenized assets, designed to store value and be exchangeable between parties without intermediation of financial institutions.

The next iteration of cryptocurrency innovations brings this interface into the real and physical realm, with asset-backed tokens representing real-world assets. real world. The value of an asset-backed token is directly affected by the value of its underlying asset, and is often classified as a security by financial regulators.

Token ownership typically represents ownership of an asset and, depending on the asset, may come with an expectation of future returns as the asset increases in value. As the asset itself increases in value, so does the token.

The development of these tokens also means that an individual, company or other entity can seek investment in exchange for tokens and raise capital through a blockchain-based system, implemented currently by issuing asset-backed tokens as new equity instruments, in accordance with financial regulations.

Additionally, businesses can tokenize existing assets for sale. Individual investors, not just the wealthy, it is now possible to buy into actual business assets without needing to store or exchange them. This not only reduces trade friction but also reduces logistics costs. Through asset-backed tokens, transactions can take place faster and more efficiently.

Asset-backed tokens can also solve problems caused by inflated or devalued currencies, as well as unpredictable stock markets, giving individuals a new financial alternative. combines digital liquidity with hard asset value when needed. We are already observing the potential of asset-backed tokens as they attract more adoption.

Governments are tying crude oil prices to the value of official digital tokens, and real estate markets are gradually moving toward tokenized fractional ownership. Asset-backed tokens are improving liquidity to previously illiquid markets and enabling cost-effective transactions without reliance on a central party, while promoting both security and transparency. This is having a major impact on the way we do business and think about ownership and future wealth creation. (author: *Johannes Schweifer)*

Non-Asset-Backed Token (Token does not guarantee assets):

Value is based on supply and demand, not tied to actual assets. For example: Dogecoin (DOGE).

Non-Asset-Backed Tokens are tokens that have no guarantee or value from a specific physical asset. Their value mainly depends on market factors, community acceptance or technical factors, instead of being backed by assets such as gold, real estate or stocks.

Example of Non-Asset-Backed Token:

- Bitcoin (BTC): Is a cryptocurrency not backed by any physical assets. The value of Bitcoin depends on supply and demand and the trust of the user community.

- Ethereum (ETH): Also not an asset-backed token, but has value thanks to its use in distributed applications (dApps) and smart contracts.

- Cardano (ADA): ADA is the native cryptocurrency of the cardano blockchain. ADA is not tied to a physical or financial asset like Stablecoin (USDT or USDC); ADA's value comes from:

+ *Uses of the Cardano blockchain*: This blockchain supports smart contracts, decentralized applications (DApps), and many other projects.

+ *Community trust*: Cardano is considered a new generation blockchain with technology based on proof of stake (Proof of Stake - PoS), helping to save energy and improve scalability.

+ *Technical features*: Cardano focuses on academic research and building sustainable blockchain protocols.

The value of ADA has fluctuated widely, depending on project development and market conditions; For example: During the 2021 bull run, ADA increased in price significantly thanks to important updates such as the Alonzo Hard Fork, which allowed running smart contracts on Cardano.

Features of Non-Asset-Backed Tokens:

- No physical collateral: They do not represent any real assets but have value based on market acceptance and demand.

- High price volatility: Since there is no underlying asset to protect the value, these tokens can experience large price fluctuations.

- Liquidity: These tokens can be easily bought and sold on cryptocurrency exchanges.

In short, Non-Asset-Backed Tokens are cryptocurrencies that do not have collateral assets, but whose value is mainly based on usage, market demand and technical factors.

2.4.2.3. Key elements of a tokenomics

"Tokenomics" is a portmanteau of "token" and "economics," used to describe the economic structure surrounding a token in a blockchain system or blockchain network. This includes factors such as supply and demand, value, distribution, and how the token is used within the system.

a) Coin/token supply

- Total supply: total number of coins/tokens circulating in the market plus the number locked minus the amount burned. Some types of total supply: fixed total supply, non-fixed total supply (increasing total supply, decreasing total supply, continuously changing total supply).

- Circulating supply: the number of coins/tokens circulating in the market.

- Maximum supply: maximum number of coins/tokens that can exist, including tokens that have already been mined or are available in the future.

b) Token governance (Token governance)

Mainly divided into 3 main groups

- Decentralized (Decentralized Token): coins/tokens are governed entirely by the decisions of the decision community and are not subject to any intervention by third parties. For example Bitcoin, Ethereum, Cardano...

- Centralized (Centralized Token): the coin/token is managed by a decision-making organization who has the right to influence the nature of the coin/token or the project that the token represents. Take Tether, for example, True USD, Ripple,…

- From centralized to decentralized: the coin/token is built by an organization but then gradually decentralizes to the community, converting from centralized to decentralized. For example, Binance Coin was initially completely governed by Binance. However, after launching Binance Smart Chain (BSC), Binance gradually decentralized BSC and BNB tokens to community control.

c) Token allocation (Token allocation)

Token allocation is the process of determining how the total number of tokens issued in a blockchain project will be distributed and used. This is an important factor in **tokenomics**, directly affecting the value, sustainability, and community trust in the project.

**) Team (Development team):*

These tokens will be allocated to the project's development team including founder, co-founder, developer, marketer, advisor,... (those who have made important contributions).

- **Common ratio**: 10% - 20%.

- **Purpose**: Rewards for the founding and project development team.

- **Vesting Period**: Usually locked for 1-4 years to avoid token sell-offs that reduce value.

- **For example**: Ethereum locks tokens to the development team for long periods of time to ensure long-term commitment. ADA token allocation has a fixed total supply of 45 billion and the development team has allocated it into three parts with the following ratio: 25,927,070,538 ADA (about 57.6%) were sold to the market via ICO; 13,887,515,354 ADA (about 30.9%) are reserved for staking rewards.

**) Liquidity mining (liquidity):*

This factor has appeared more recently, especially after the September 2020 period when DeFi projects started to grow strongly. This is a token extracted as a reward for investors who actively provide liquidity.

Users deposit digital assets (crypto) into Liquidity Pools on DeFi protocols. These Liquidity Pools are often used on DEX platforms such as Uniswap, PancakeSwap, or on blockchains such as Cardano, Ethereum, or Binance Smart Chain. In return, users receive rewards in the platform's native tokens or other tokens (like ADA, ETH, or governance tokens).

- How it works:

+ Liquidity provision: Users deposit token pairs (e.g. ADA/USDT) into a Liquidity Pool on the DEX.

+ Transaction fees: Liquidity Providers (LPs) receive a percentage of fees from transactions taking place in the pool.

+ Additional rewards: In addition to transaction fees, they often receive rewards in the form of the protocol's native tokens. This is the Liquidity Mining mechanism.

- Liquidity Mining on major blockchains:

+ Ethereum: With famous platforms such as Uniswap, Sushiswap, Curve.

+ Binance Smart Chain (BSC): PancakeSwap is one of the largest platforms.

+ Cardano: Platforms like Minswap, SundaeSwap.

+ Avalanche, Solana: Support DeFi protocols focused on high performance.

- Example of Liquidity Mining:

Let's say you participate in providing liquidity to an ADA/USDT pool on Cardano:

+ You deposit 1,000 ADA and the equivalent amount of USDT into the pool.

+ Within 30 days, you receive:

- Transaction fees**:** 0.3% from trading volume.
- Bonus tokens**:** 50 governance tokens from the protocol.

+ Total profit = Transaction fee + Reward token value (market price calculated).

**) Private/ Public sale (forms of token sale):*

This is the token parameter for sales to raise capital for product development. Normally, a project will have about three sales: Seed sale, Private sale and Public sale.

- Seed Sale: is the first stage in the capital raising process of a blockchain or cryptocurrency project. This is a form of token sale before both Private Sale and Public Sale, to raise initial capital to develop the project.

+ Objective:

Mobilize capital at a very early stage of the project; Funding research activities, product development, and building the basic foundation of the project.

+ Participants:

Angel investors; Venture capital funds; Strategic partners; A small number of individuals have close relationships with the development team.

+ Token price:

Usually very low, cheapest in capital raising rounds; Represents the highest level of risk, but also offers great profit potential if the project is successful.

+ Number of tokens sold:

Very limited, usually about 5–10% of total supply.

+ Terms:

Usually comes with token locking conditions (vesting period), to avoid a sell-off after the project lists the token; For example: Tokens are released gradually over 12–24 months.

- Private sale: is a capital mobilization stage for blockchain and cryptocurrency projects, taking place before the Public Sale stage. This is one of the popular forms of token sales to fund project development activities.

+ Participants:

High-net-worth individuals, venture capital funds (VCs), or strategic partners; Usually requires a high minimum investment and limits the number of participants.

+ Objective:

Calling capital on a larger scale than Seed Sale, helps the project expand its scale and prepare for the next stages such as Public Sale or listing tokens on the exchange.

+ Token price:

Usually lower than Public Sale, but higher than Seed Sale; Preferential prices to attract strategic investors.

+ Conditions:

There are often vesting periods to ensure investors do not sell off immediately after the token is listed. For example, 20% of tokens are unlocked immediately upon listing, the rest are unlocked gradually over 12–24 months.

+ Token distribution:

Tokens sold in Private Sale account for about 10–20% of total supply, depending on the project's strategy.

- Public sale: Is the final token sale stage in the capital raising process of a blockchain project. This is the step of opening the token sale to the public, where any investor can participate (depending on legal regulations and project conditions). This phase is usually done later **Seed Sale** and **Private Sale**.

+ Participants:

Open to the public, not limited by strategic relationships or large investments; Suitable for retail investors or newcomers to the cryptocurrency market.

+ Objective:

Raising capital for expansion to complete products or officially launch; Increase project recognition in the community; Distribute tokens more fairly than in previous stages.s

+ Token price:

Usually higher than the price of Seed Sale and Private Sale but lower than the price listed on the exchange; Reflects the maturity level of the project.

+ Token distribution:

The majority of tokens are reserved for the community, typically 20–30% of total supply.

+ Form:

Can take place through ICO (Initial Coin Offering), IEO (Initial Exchange Offering), or IDO (Initial DEX Offering) on centralized or decentralized trading platforms.

**) Airdrop (gift giving):*

This is a form of free distribution of tokens or cryptocurrency to user wallets to increase recognition, attract the community, or encourage the use of blockchain projects. This is a popular marketing strategy in the cryptocurrency sector.

- Airdrop's goal:

+ Increase project recognition: Introduce tokens to a large number of users, helping the project become more known.

+ Community building: Attract new users to join the project ecosystem.

+ Promote use: Encourage users to experience the project's products or services.

+ Token distribution: Ensure tokens are widely distributed to increase decentralization.

+ Increase liquidity: When users own tokens, they can trade, increasing liquidity in the market.

- Popular types of Airdrop:

+ Standard Airdrop: Users receive free tokens just by performing simple steps such as registering an account, filling in wallet information, or following social networks.

+ Bounty Airdrop: Users must perform tasks such as sharing articles, joining Telegram groups, posting tweets, or writing blog posts introducing the project; Often applied to large marketing campaigns.

+ Holder Airdrop (Airdrop for holders) Distribute free tokens to those who already hold a specific cryptocurrency (e.g. ETH, BTC); Usually based on the user's wallet balance at a certain time (snapshot).

+ Exclusive Airdrop: For special users such as early investors, partners, or major contributors to the project.

+ Hard Fork Airdrop: Occurs when a blockchain splits, and users on the old blockchain receive new tokens from the new blockchain (for example, Bitcoin Cash from Bitcoin).

- Real-life example of Airdrop

+ Stellar (XLM):

Stellar once held a large airdrop, giving away millions of XLM tokens for free to Bitcoin owners.

+ Uniswap (UNI):

Release free UNI tokens to those who have used the Uniswap exchange before a specific time. Each person received at least 400 UNI, worth thousands of USD at the time.

+ ApeCoin (APE):

Owners of NFTs from the Bored Ape Yacht Club (BAYC) collection receive free APE tokens based on the number of NFTs they own.

- How to Airdrop on cardano blockchain

+ Cardano's native token (Native Token):

Cardano supports the issuance of native tokens without the need for complex smart contracts; This makes airdrop distribution quick and cost-effective.

+ Cardano knows:

Users often use wallets like Yoroi, Daedalus, or Nami to receive airdrops; The wallet needs native token support and interoperability with the Cardano network.

+ Snapshot and staking:

Some projects require users to stake ADA (stake into the pool) to qualify for airdrops; Snapshot will be taken at a certain time to determine wallet balance or activity.

+ Low transaction fees:

Thanks to the Proof-of-Stake (PoS) consensus mechanism and cost optimization, airdrops on Cardano are often cheaper than on Ethereum.

**) Foundation reserve (foundation fund reserve):*

This is a portion of assets or tokens set aside by blockchain projects to support the long-term operations of the organization or platform behind the project. This is an important strategy to ensure the sustainability and long-term development of the project, especially during the expansion phase or facing financial challenges.

Examples of Foundation Reserve in featured projects

- Cardano (ADA):

The Cardano Foundation manages a large portion of its reserves to fund research, ecosystem development, and community expansion.

This fund is also used to promote strategic partnerships.

- Ethereum (ETH):

The Ethereum Foundation holds a reserve fund to fund research, network development, and protocol improvements.

- Binance Smart Chain (BNB):

Binance Foundation uses its reserves to promote the development of the Binance ecosystem, funding DeFi, GameFi, and NFT projects.

- Polkadot (DOT):

The Web3 Foundation manages Polkadot's reserves to support parachain projects, development communities, and long-term research.

**) Token release (release):*

This is the process of releasing tokens from the previously allocated supply into circulation on the market or into the hands of owners. This is an important step in blockchain projects, helping to properly manage token supply, maintain value and ensure transparency in project operations.

Examples of Token Release of prominent projects:

- Ethereum (ETH):

Initially, Ethereum issued ETH tokens to investors participating in the ICO (Initial Coin Offering), with an initial supply of 72 million ETH. The remainder is gradually exploited through the PoW mechanism and later PoS.

- Cardano (ADA):

Cardano uses a vesting model for the founding team and development fund, with the majority of tokens distributed to the community through staking rewards.

- Polkadot (DOT):

DOT tokens are released gradually to support parachains, encourage staking, and fund development projects on the platform.

- Uniswap (UNI):

UNI tokens are issued according to a clear roadmap: 60% for the community and distributed gradually over 4 years.

2.5. NFT

2.5.1. Concept

NFT (Non-Fungible Token) is a type of digital asset built on blockchain technology that represents unique ownership or access to a specific digital product or service. The characteristic feature of NFTs is their non-fungibility, meaning that each NFT is unique and cannot be replaced with another NFT of equivalent value, unlike "fungible" assets. like cryptocurrencies (for example, 1 Bitcoin has the same value as 1 other Bitcoin).

NFT (Non-Fungible Token) is a unique type of digital asset, used to create and authenticate ownership of digital assets such as images, music, video clips and virtual real estate. Each NFT is marked with a unique identifier and stored on the blockchain, ensuring the authenticity and ownership of the asset.

Unlike traditional assets like stocks or currencies, NFTs cannot be replaced or exchanged at par with another similar item, due to their unique nature. This makes NFTs similar to rare collectible items in the real world. Interest in NFTs has surged in recent years, especially in 2021, as the value of digital artworks and other digital assets soared.

Blockchain technology plays an important role in establishing ownership of NFTs. Blockchain operates as a decentralized ledger, allowing public validation of NFTs. This technology uses digital signatures to prove ownership and originality of a work. The buyer of an NFT does not own a physical piece to hang on the wall, but instead a digital image of the piece along with a digital certificate of authenticity.

The unique properties of NFTs make them irreplaceable. This is in contrast to fungible assets, for example Bitcoin and other cryptocurrencies, dollar bills, gold bars and stocks, are worth a specific amount of money and are interchangeable. While a dollar bill can be exchanged for another dollar bill or a bitcoin can easily be swapped for another, that is not true with NFTs.

NFTs are typically not divisible. The basic unit of an NFT is the token, which typically cannot be divided into smaller denominations, as one dollar can be divided into 10 coins. However, partial ownership of NFTs has been introduced by several platforms recently, such as Fractional. Fractional ownership allows the NFT to be divided into smaller NFTs, which can be sold to multiple buyers.

Additionally, NFTs are immutable. They cannot be changed after they are made encrypted using blockchain technology . The originality and legality of the item is authenticated through the blockchain where it is stored.

Why are NFTs important?

Justin Herzig, co-founder of Own the Moment NFT , a company that provides content, tools, and analysis about NFTs, explains that the rise in popularity of NFTs is a result of their "ease of use, speculative nature as a collectible, and invest, and develop with the grassroots community around the products."

NFTs allow individuals to buy and sell digital assets in new ways. They help artists and other content creators express their skills digitally and provide the ability to securely price, purchase, and exchange digital art using a digital ledger number. Using NFTs, new and

previously decentralized actors can develop innovative value exchanges to build new market structures.

Herzig said NFTs are an important form of alternative investment that appeals to buyers' personal interests and passions. With NFTs, retail investors will be able to invest in things they have a personal connection to, as well as things that provide financial value and utility.

NFT buyers hope the value of the token will increase over time, similar to any other investment. Like their fungible cousins, NFTs are subject to changes in supply and demand. Theo Grand View Research , the NFT market is valued at $20.44 billion in 2022 and is expected to grow to $211.72 billion in 2030.

NFT on cardano platform?

The first NFT on the Cardano platform was launched in March 2021 with the SpaceBudz project. This is a collection of 10,000 unique astronaut animal images, each encoded as an NFT on the Cardano blockchain. SpaceBudz pioneered the adoption of the NFT metadata standard and deployed the first smart contract-based marketplace on Cardano.

The launch of SpaceBudz marks an important turning point in the development of the NFT ecosystem on Cardano, paving the way for many other NFT projects on the platform.

To participate in the NFT market on Cardano, users need a Cardano-compatible cryptocurrency wallet, such as Nami or Daedalus, and a connection to NFT exchanges such as CNFT.io or jpg.store.

2.5.2. Characteristic

a) Uniqueness

Each NFT is unique and cannot be copied. NFT metadata information is stored on the blockchain, ensuring that each token has unique characteristics.

b) Non-fungibility

Unlike fungible assets (like Bitcoin or cash), NFTs cannot be exchanged at par. Each NFT has its own value based on rarity, uniqueness, or market value.

c) Clear ownership (Ownership)

NFTs record ownership in the blockchain. Owners can prove their ownership and transfer tokens if desired.

d) Sustainability and Transparency (Immutability & Transparency)

NFT information and transaction history are publicly stored on the blockchain and cannot be changed or deleted.

e) Limited divisibility (Indivisibility)

Most NFTs are not divisible like cryptocurrencies. You can only own the entire NFT, not parts of it (except in some special cases).

f) Interoperability

NFTs can be used across a variety of platforms and applications, as long as they are compatible with the same blockchain or standard.

For example:

- NFTs on Ethereum follow the ERC-721 or ERC-1155 standard.

- NFTs on the Cardano blockchain are called CNFTs (Cardano Non-Fungible Tokens). Cardano uses the CIP-721 standard, similar to ERC-721 on Ethereum, to define and manage NFTs. This standard ensures consistency and compatibility for NFT projects on the network.

g) Diverse applications

NFTs are not just limited to digital art but also apply to:

- Gaming (items, characters, assets in the game).
- Virtual real estate.
- Event tickets or intellectual property.
- Digital collectibles (cards, artwork).

h) Ability to earn passive income

Some NFTs allow the owner to receive commissions or income from the use of the work, for example when the work is resold.

For example: In mid-March 2022, rapper Binz (Vietnam) collaborated with blockchain company Tuniver to launch an NFT collection for the new song 'Don't Break My Heart'. He divided the copyright of this song into NFTs with 4 different classes, corresponding to 4 levels of revenue copyright sharing rates.

2.5.3. Application

NFT (Non-Fungible Token) has many practical applications in various fields, from art and entertainment to education and finance. Here are common uses of NFTs:

1. Digital Art

Collect and sell digital art. Artists can sell their work directly to buyers as NFTs without the need for an intermediary. For example, Beeple sold the work “Everydays: The First 5000 Days” for $69.3 million.

Authentication and copyright protection. NFTs record the origin and ownership of the work, helping to prevent copying or counterfeiting.

2. Gaming (Game)

Owning in-game items:

Players can buy, sell or trade in-game assets (weapons, characters, costumes) as NFTs. For example, Axie Infinity allows players to own and trade digital creatures in the game.

Play-to-Earn:

NFT games reward players with cryptocurrency, turning gaming into a source of income.

3. Metaverse and virtual real estate

Buy and sell virtual land: Users can own and develop virtual land in metaverse platforms. For example: Decentraland, The Sandbox, and Pavia (on Cardano).

Digital assets in the metaverse: NFTs are used to trade assets in the virtual world, such as houses, furniture, and decorative items.

4. Music and entertainment

Music Royalties: Artists can release songs or albums as NFTs, allowing fans to purchase and own a portion of the royalty revenue. For example, Kings of Leon released albums as NFTs.

Event tickets: NFTs can be used as e-tickets, preventing fraud and creating exclusive experiences for attendees.

5. Digital Collectibles

Cards and Collectibles: Featured digital cards, images or videos released as NFTs.

For example, NBA Top Shot offers highlights of basketball games as NFTs.

6. Education and digital materials

Degrees and certificates: NFTs can be used to store and authenticate degrees and certificates, ensuring they cannot be faked.

Learning materials: Textbooks, lectures can be issued as NFTs, allowing tracking and copyright management.

7. Finance (DeFi)

Collateral: NFTs can be used as collateral in financial transactions, borrowing on the blockchain platform.

Asset management: NFTs represent ownership of real-world assets such as real estate or stocks.

8. Fashion and e-commerce

Digital Clothing: Major fashion brands release digital products as NFTs for use in the metaverse. For example, Gucci and Nike have begun testing selling fashion NFTs.

Tracking and authentication: NFTs can be used to prove the authenticity and origin of products in the supply chain.

9. Charity and community fundraising

Fundraising through NFTs: NFTs are sold to raise funds for charities or community projects.

For example, WWF released NFTs of endangered animals to call for environmental protection.

10. Copyright and intellectual property

Copyright protection: Creative works such as videos, articles, or images can be stored as NFTs for copyright tracking and management.

Profit Distribution: Creators can earn royalties every time their NFTs are traded on the marketplace.

2.5.4. Challenges and opportunities

2.5.4.1. The challenge of NFTs

While NFTs have brought many creative and economic opportunities, they also face many notable challenges. Here are the main problems NFTs are solving:

a) Market instability

- Price fluctuations: The value of NFTs is often unstable, easily increasing or decreasing sharply in a short period of time. This makes NFTs a risky investment.

- Lack of valuation standards: Assessing the value of an NFT depends heavily on the buyer's feelings and tastes, leading to speculation.

- For example:

+) Beeple's NFT - "Everydays: The First 5000 Days":

Event: This work was sold for a record price of 69.3 million USD at Christie's in March 2021, shocking the NFT market.

Volatility: After the craze, a series of other NFTs were also born but could not achieve the same price. The market became saturated and cooled quickly.

+) Axie Infinity (AXS):

Event: Axie Infinity game was very popular in 2021 with its "play-to-earn" model. Players buy NFTs to participate and earn money from the game.

Volatility: As the number of players decreased, the value of AXS tokens and Axie NFTs decreased by more than 90%, causing many investors to suffer heavy losses.

+) Ethereum Gas Fee

Event: During the peak of the NFT market, transaction fees on Ethereum increased, sometimes reaching hundreds of USD for a single transaction.

Volatility: Expensive transaction costs have driven users away from Ethereum-based NFT platforms, leading to a significant decline in trading volumes.

b) Copyright and ownership issues

- Copyright disputes: Some NFTs are created from other people's works without permission, causing controversy over intellectual property rights.

For example: Hermès vs. Mason Rothschild: Hermès sues creator Mason Rothschild because the "MetaBirkins" NFT collection used images of Birkin handbags without permission. Hermès won the case in 2023, asserting ownership of the brand.

- Separation of ownership of NFTs and content: When purchasing an NFT, the buyer owns a digital token associated with an asset (artwork, music, video, etc.), but is not synonymous with ownership of copyright in that work. Buyers often mistakenly believe that they have the right to copy, distribute or modify the work, whereas these rights remain with the original creator, unless otherwise agreed.

For example: Bored Ape Yacht Club (BAYC): NFT owners in this collection have the right to commercialize the images of the "Bored Apes" they own. However, this is the exception thanks to the express terms given by the creator, not the general rule of NFTs.

c) High transaction costs

Transaction costs in the NFT market are often very high, especially on blockchain-based platforms like Ethereum. This is a major challenge for users and developers, causing barriers to scaling the market and encouraging new user participation.

For example:

- OpenSea and high gas fees on Ethereum:

During the NFT boom in 2021, gas fees on Ethereum once reached $200–300 just to make a simple transaction like buying or selling an NFT.

Small users are excluded from the market because they cannot afford this high fee. For example, if an NFT costs $50 but the transaction fee is up to $200, buyers will find it difficult to accept.

- Mint NFTs are expensive:

To mint an NFT on Ethereum, creators typically have to pay between 50–200 USD in gas fees, depending on the level of network congestion.

An independent artist wanting to mint 10 NFTs would have to pay $500–2,000 in gas fees, making them hesitant to enter the market.

d) Environmental concerns

Large energy consumption: Blockchain technology, especially Proof of Work (PoW)-based networks, consumes large amounts of energy, contributing to climate change.

Pressure to transition: Networks are having to find ways to switch to friendlier mechanisms like Proof of Stake (PoS), but the process is not easy.

For example:

- Beeple và "Everydays: The First 5000 Days":

Beeple's work sold for a record $69.3 million on Ethereum in 2021;

Environmental impact: Auctions and ownership transfers consume large amounts of energy, with total carbon emissions equivalent to thousands of tons of CO_2.

- "Space Cat" NFT Collection:

NFT "Space Cat" (image of a cat traveling in space) was minted and released on Ethereum. The creation and trading of Space Cat consumes **more than 200 kWh**, equivalent to the amount of electricity consumed by a European family in one month.

e) Fraud and deceit

Fake NFTs: Some people create NFTs from content that doesn't belong to them or copy other people's NFTs to scam buyers.

Untrusted trading platforms: Some trading platforms lack transparency, are vulnerable to attacks or collapse, causing losses to users.

For example:

- Frosties NFT (2022): One of the biggest rug pulls of 2022, the founding team of Frosties NFT defrauded users of more than 1.3 million USD before deleting their social media accounts and ceasing communication.

- OpenSea and Counterfeit NFTs (2022): One of the major incidents was artists discovering that their work had been copied and resold as NFTs on OpenSea without permission. OpenSea had to deal with thousands of fake NFTs, putting buyers at great risk.

- MetaMask and OpenSea spoofing (2021): In a series of scams, hackers send emails impersonating OpenSea and MetaMask, asking users to verify accounts or provide personal information. After the user complied, the hacker obtained the private key and appropriated the NFT from their wallet.

- The Evolved Apes (2021): An NFT project called Evolved Apes attracted millions from investors, but the development team suddenly disappeared and nothing was actually developed. Users were unable to continue trading NFTs and the project died shortly after collecting funds.

f) Lack of usability

Technical complexity: Creating, trading, or storing NFTs requires users to understand blockchain technology, cryptocurrency wallets, and related processes.

Limitations in user experience: The interface of current NFT platforms is difficult to use for newcomers.

For example:

- Difficulty in using MetaMask and other cryptocurrency wallets

A newcomer to the NFT market may have difficulty setting up a MetaMask wallet, connecting it to platforms like OpenSea, and making transactions. This process can be time-consuming and confusing if the user is not experienced.

Users may miss investment opportunities or even lose assets due to not being able to execute transactions correctly.

- The NFT minting process is time-consuming and complicated

An artist wants to mint an NFT but has difficulty creating and configuring a smart contract, choosing a platform, and paying gas fees. This can make them feel confused and prone to giving up.

Creators are unable to develop their projects, leading to a lack of participation by independent artists in the NFT market.

- High gas fees cause discomfort for users

An investor wants to buy an NFT priced at $100 but must pay an additional $80 in gas fees to complete the transaction on Ethereum. This reduces usability and can make users unhappy with transaction costs.

Investors may decide not to buy or miss out on potential opportunities because transaction fees are too high.

g) Legal regulations are not clear

Lack of legal framework: Many countries do not have clear laws on NFTs, leading to legal risks for both buyers and sellers.

Tax management: Tax regulations for NFT transactions have not been unified, making it difficult to comply with the law.

For example:

- NFT copyright issues on OpenSea:

On the OpenSea platform, an artist discovered that his work had been copied and resold as NFTs without permission. However, when they try to complain, they encounter difficulties because there is no clear legal regulation of art ownership in the NFT world.

Creators cannot protect their rights due to the lack of legal mechanisms, and the platform cannot ensure effective protection of intellectual property rights.

- Consumer protection issues in the NFT scam:

A group of scammers created a fake "Bored Ape" NFT project and defrauded buyers of large amounts of money. Once discovered, buyers cannot claim compensation or protection because there is no legal regulation governing fraud in the NFT market.

Consumers are left unprotected and unable to recover lost assets, leading to a loss of trust in the NFT market.

h) Long-term viability

Long-term value: Many are concerned that interest in NFTs is just a temporary fad and that their value could plummet in the future.

Platform dependency: If the platform hosting NFT content goes down, the content associated with the NFT may be lost.

For example:

- NFTs in the gaming industry:

NFTs have been adopted in the gaming industry, especially in video games that allow players to own, trade and sell in-game items as NFTs. For example, the game Axie Infinity has attracted millions of players and uses NFTs to represent creatures in the game.

NFTs in the gaming industry can last a long time if games maintain their appeal and community of players, while ensuring the real value of NFT items.

- NFT in the digital art industry:

NFTs have provided an opportunity for artists to sell their artwork as digital assets. For example, artists like Beeple have sold digital art as NFTs for millions of dollars, and this shows that a portion of NFTs can last a long time if the digital art market continue to develop.

If NFTs continue to create real value for artists and buyers, the NFT market in the digital art industry can sustain and grow over the long term.

2.5.4.1. NFT opportunities

NFTs (Non-Fungible Tokens) are not only part of the digital asset investment market but also open up many new opportunities in the fields of art, entertainment, real estate, gaming and many other industries. . Below are some of the potential opportunities of NFTs in the future.

a) NFTs in the arts and creative industries

NFTs create a huge opportunity for artists and content creators by allowing them to sell and distribute artwork as digital assets. This helps artists reach a global market and receive the recognition they deserve.

- Opportunity:

+) Artists can protect their copyright and receive revenue from the sale of artwork without interference.

+) NFTs allow the distribution and proof of ownership of digital artworks.

+) Artists no longer depend on auction houses or large companies to sell their works.

- For example

Beeple: A famous digital artist sold his work "Everydays: The First 5000 Days" as NFT for 69 million USD in 2021. This has opened a huge opportunity for other digital artists to

continue reach the market and make money from your works without going through intermediaries.

b) NFTs in the gaming industry

NFTs could completely change the way assets are exchanged in video games. Players can own and trade in-game items as NFTs, giving them long-term control and ownership of digital assets.

- Opportunity:

+) Players can own, buy, sell and exchange in-game items such as weapons, characters, costumes or land in the form of NFTs.

+) NFTs can make games more valuable by allowing players to own items that can be traded with others.

- For example:

Axie Infinity: This is a blockchain game that allows players to raise, train, and battle creatures called Axies. Axies are represented as NFTs, and players can buy and sell them on the marketplace. This game has attracted millions of participants and has become a prime example of NFTs in gaming.

c) NFTs in real estate

NFTs can be applied in the real estate industry to represent ownership of physical assets, helping to simplify transactions and reduce complex administrative procedures.

- Opportunity:

+) Real estate can be tokenized and represented as NFTs, making ownership transfers and asset transactions fast and transparent.

+) NFT can help reduce legal and paperwork issues, while also facilitating retail investors to participate in the real estate market.

- For example:

RealT: This is a platform that allows investors to buy real estate shares through NFTs. NFT holders can receive profits from the real estate they invest in. The platform is experimenting with real estate tokenization and has attracted interest from investors.

d) NFTs in music and entertainment

NFTs are opening up new opportunities for music artists and content producers to sell their products directly to fans without going through intermediaries like record companies or online platforms. .

e) NFTs in real estate

NFTs can be applied in the real estate industry to represent ownership of physical assets, helping to simplify transactions and reduce complex administrative procedures.

- Opportunity:

+) Artists can release albums, songs, music videos, and even concert tickets as NFTs, helping them retain the majority of revenue and build a loyal fan community.

+) NFTs can create exclusive opportunities for fans, such as early access to events or special recordings.

- For example:

Kings of Leon: This band released the album "When You See Yourself" as an NFT, providing special access to buyers, including exclusive content and tickets to concerts.

f) NFTs in the sports industry

NFTs can be used to create digital sports trading cards, collectibles, or unique souvenir items related to athletes and sporting events.

- Opportunity:

+) Fans can purchase and own player cards or highlights from sports matches as NFTs.

+) Sports teams and athletes can generate new revenue streams from selling special NFTs such as player cards or videos of memorable moments.

- For example:

NBA Top Shot: This is a platform that allows NBA fans to buy, sell and trade special moments from NBA games as NFTs. Video moments like highlight dunks and game-winning plays can be owned as a single digital asset.

g) NFT in identity authentication and certification

NFTs can help authenticate identities or certify achievements and certificates in many fields such as education, technology or medicine, making information confirmation faster and more secure.

- Opportunity:

+) NFTs can be used to create educational certificates, awards, or honors that are securely stored and cannot be counterfeited.

+) Organizations, schools, and companies can use NFT to issue certificates or titles, making authentication easy and transparent.

- For example:

Coursera and other education platforms: Some online education platforms are experimenting with issuing course certificates as NFTs, allowing students to demonstrate their learning achievements without worrying about counterfeiting.

g) NFT in identity authentication and certification

NFTs can help protect the intellectual property rights of creative works, especially in fields such as art, music, and writing, where the work is protected and proven using blockchain.

- Opportunity:

+) NFTs can be a powerful tool to protect creators' copyright and ownership, helping them receive their fair share of profits when their work is used.

+) NFTs can create a transparent way to track and distribute profits from the use of the work.

- For example:

Async Art: This platform allows artists to create dynamic works of art in the form of NFTs. These works can change over time, and each NFT work can be owned and traded on the blockchain, helping to protect the rights of the artist.

In short:

NFTs open up many potential opportunities in the arts, entertainment, gaming, real estate and many other fields. By providing innovative solutions, NFTs can help artists, creators, athletes, and consumers build new values and improve traditional business models. As blockchain technology develops and legal regulations become clearer, the NFT market may continue to expand and offer even more opportunities.

2.6. WALLET AND ADDRESS

Wallets and addresses are two important concepts in the world of blockchain and digital assets, including cryptocurrencies and NFTs. Wallets and addresses play an important role in digital asset management, transactions, and information security.

2.6.1 Ví (wallet)

2.6.1.1 Concepts

Wallet in the context of digital assets is a software, device or service that helps users store, send and receive digital assets, including cryptocurrencies and NFTs. A wallet is not a place to store real assets, but a tool to manage and access those assets through private keys and public keys.

Wallets can be used for a variety of purposes, from trading cryptocurrencies to managing other digital assets, like NFT collections or digital certificates.

With code money , there is no tangible currency, no paper money to put in a physical wallet or handbag. Cryptocurrency exists on blockchain and there are no physical manifestations that the user touches. But there is still a need for individuals and institutions to understand the ownership of crypto assets and be able to see how much is held, much like a bank account provides a bank balance.

Cryptocurrency wallets provide users with a way to validate account balances to provide visibility into how much cryptocurrency the user owns. Cryptocurrency wallets allow users to send and receive cryptocurrency transactions, an approach similar in concept to how a traditional bank account allows users to make transactions. For many users, cryptocurrency wallets are the primary mechanism for managing cryptocurrency balances.

Why are cryptocurrency wallets important?

Like any currency, cryptocurrencies can be accumulated and used for a variety of purposes and transactions. Cryptocurrency wallets play a fundamental role in enabling crypto assets and cryptocurrencies to have useful functions for individuals and institutions, just as bank accounts are fundamental to fiat currency.

Cryptocurrency wallets are necessary for several important purposes that help take advantage of the practical utility of cryptocurrencies, including:

- *Cryptocurrency management:* Cryptocurrency wallets provide users with the ability to track crypto asset balances.

- *Transaction:* Sending and receiving cryptocurrency payments is an important feature of cryptocurrency wallets.

- *Connect with applications decentralized (dApp)*: Cryptocurrency wallet required to connect and interact with dApps Web 3.0 .

- *Username recognition:* All cryptocurrencies are stored on the blockchain. Cryptocurrency wallets allow transactions using usernames that can be linked to public key addresses on the blockchain.

- *Key management*: Functionally, cryptocurrencies exist on the blockchain as public key addresses. Cryptocurrency wallets help users manage encryption key private is used to access a certain address and authorize transactions.

2.6.1.2 Wallet classification

Wallets in the digital asset world can be classified according to different criteria, mainly based on storage method, security level and usability. Below are the wallet classifications and popular wallet types today:

1. Software Wallet

Software wallets are a popular type of wallet, installed on computers, phones or mobile devices. This wallet provides users with access to digital assets and ease of trading. Software wallets can connect to the internet to perform transactions.

Types of software wallets:

a) Mobile Wallet: Installed on mobile phones, helping users make transactions anytime, anywhere. This is a popular choice for cryptocurrency users on the go.

Popular wallets:

- Trust Wallet: A popular mobile wallet that supports many cryptocurrencies and NFTs.

- MetaMask: A mobile wallet and browser for Ethereum and ERC-20 tokens.

- Yoroi Wallet: Yoroi Wallet is a lightweight software wallet for Cardano, developed by Emurgo (a subsidiary of Cardano). Yoroi supports users in managing ADA and other Cardano assets. This is a user-friendly wallet and is easily accessible via a web browser or mobile app.

b) Ví Desktop (Desktop Wallet): Install on desktop or laptop. Desktop wallets are generally more secure than online wallets but can be easily lost if the computer crashes or is hacked.

Popular wallets:

- Exodus: A software wallet with an easy-to-use interface and support for many cryptocurrencies.

- Electrum: A lightweight Bitcoin wallet, allowing users to have better control over transactions.

- Yoroi Wallet

2. Hardware Wallet

Hardware wallets are physical devices designed to store cryptocurrencies and NFTs offline, helping to protect assets from online threats like malware or hacks. A hardware wallet is considered the most secure option because it does not connect directly to the internet when storing private keys.

Types of hardware wallets:

a) Knows Ledger:

One of the most popular hardware wallets, supports multiple cryptocurrencies and offers high security with private keys stored in the device.

Popular wallets:

- Ledger Nano S: Compact, affordable hardware wallet device, suitable for beginners.

- Ledger Nano X: Upgraded version of Nano S with Bluetooth connectivity and higher storage capacity.

b) The Treasury knows:

Another hardware wallet with high security, supporting many different coins and tokens.

Popular wallets:

- Trezor One: A basic hardware wallet, easy to use and compatible with many platforms.

- Trezor Model T: High-end version with touch screen and the ability to support many cryptocurrencies.

3. Online Wallet (Web Wallet)

Online wallets (or web wallets) are wallets hosted on online platforms, allowing users to access and manage digital assets through a web browser. Online wallets can be easy to use but security is lower as private keys can be exposed if the platform is hacked.

Types of online wallets:

a) Via Blockchain: A simple online wallet that allows users to store and trade cryptocurrencies such as Bitcoin and Ethereum.

Popular wallets:

Blockchain Wallet: Easy-to-use wallet with friendly interface and ability to store Bitcoin and Ethereum.

b) Via Coinbase: It is an online wallet and also a cryptocurrency exchange platform, allowing users to easily trade and store cryptocurrencies.

Popular wallets:

Coinbase Wallet: A mobile and web wallet that helps users store assets and interact with decentralized applications (dApps).

c) Daedalus Wallet: Daedalus is the official wallet of Cardano, developed by IOHK (Input Output Hong Kong), the company behind Cardano. This is a full-featured wallet that runs on the desktop and provides users with the ability to store the entire Cardano blockchain, helping to synchronize and confirm transactions directly from the Cardano network.

Main features of Daedalus:

+) Full Wallet: Daedalus is a full-node wallet, meaning it downloads the entire Cardano blockchain to the user's computer to ensure integrity and security.

+) High security: Supports strong security features with private key and PIN code.

+) Support for multiple wallets: Allows users to create and manage multiple wallets at the same time in one application.

+) Staking support: Users can stake ADA right in the Daedalus wallet to earn rewards from Cardano.

+) Compatible with hardware wallets: Can integrate with hardware wallets such as Ledger or Trezor.

Supported platforms: Desktop (Windows, macOS, Linux

d) Adalite Wallet: Adalite is a lightweight Cardano web wallet that is easy to use and does not require downloading the entire blockchain. It allows users to interact with the Cardano network, send and receive ADA, and participate in staking activities without having to install heavy software.

Adalite main features:

+) Lightweight web wallet: No need to download the entire blockchain, helping users save space and synchronization time.

+) Compatible with Ledger: Can connect to Ledger hardware wallet to enhance security.

+) Staking support: Users can stake ADA and earn rewards in the wallet.

+) Good security: Although it is a web wallet, Adalite supports strong security with encrypted private keys.

Supported platforms: Web browsers (Chrome, Firefox, Safari)

4. Paper Wallet

Paper wallets are a method of storing private and public keys in a physical printout. This wallet helps store assets outside the internet, but users must be very careful when storing them because they can easily be lost or damaged.

Bitcoin Paper Wallet: This is a simple paper wallet created by printing Bitcoin's public and private keys. Services such as *bitaddress.org* Helps users create paper wallets for free.

Popular wallets:

Bitaddress.org: Free Bitcoin paper wallet creation service, helping users create safe and secure wallets.

5. Card Wallet

Card wallets are new and relatively uncommon wallets that help users store cryptocurrencies and NFTs in a physical card similar to a bank card. This is a convenient, safe and easy to carry storage method.

Card wallet:

Trezor card wallet: An integrated hardware wallet in the form of a card, allowing users to store cryptocurrency on a physical card.

Popular wallets:

Trezor Model T (card): Provides high security for cryptocurrencies and has a touch screen to easily check transactions.

2.6.1.3 Principle of operation

Wallets in the world of blockchain and digital assets operate on strong security principles and the structure of the blockchain network. Here's how a digital wallet basically works:

1. Public Key and Private Key

Digital wallets are mainly based on two important components: public key and private key. They generate a key pair for each wallet.

Public Key: This is the wallet address where others can deposit money or digital assets (like cryptocurrency or NFTs). The public key is public and can be shared with anyone.

Private Key: This is a secret key that only the wallet owner knows. The private key is used to authenticate transactions and prove ownership of assets. If the private key is lost, the user will lose access to his assets.

2. Asset Management (Digital Signature)

When a user wants to make a transaction (e.g. send ADA or NFT to someone else), they will have to use their private key to sign that transaction. Signing transactions with a private key helps ensure that only the wallet owner can make transactions involving his or her assets. This is the process of authenticating property ownership.

Transaction process:

Create transaction: Users create transactions by entering the recipient wallet address and the amount of assets they want to transfer.

Digital signature: Transactions are signed with the sender's private key, which helps prove that they have the authority to transfer assets.

Transaction confirmation: The transaction is then broadcast to the blockchain network to be confirmed by nodes in the network (for example, via Proof of Work or Proof of Stake).

Transactions will only be accepted when the sender's digital signature is valid and matches their private key.

3. Private Key Storage and Management

The private key is not stored in the wallet as easily visible information. Instead, it is secured within the wallet and can be encrypted, helping to protect users from external threats.

Software wallet: Private key information is stored locally on the user's computer or phone. Software wallets use security measures, such as encryption, to protect private keys from unauthorized access.

Hardware Wallet: A hardware wallet stores private keys in a peripheral device that is not connected to the internet. This helps protect assets from malware or hacking threats.

4. Asset Management (Blockchain and Trading)

When a transaction is made, the wallet will not actually transfer the asset (e.g. ADA or NFT) between wallets, but it will change the state of the asset on the blockchain. Blockchain is a distributed ledger that records every transaction, helping to maintain transparency and immutability.

Assets do not actually exist in the wallet: Instead, the wallet only stores information about asset ownership, which is confirmed through transactions on the blockchain.

Wallet address: Wallet address is where assets "live", and wallets only help users access these assets by signing transactions and managing ownership.

5. Authentication and Security

Wallets use a variety of security measures to protect users' digital assets:

Encryption: The user's private key is encrypted and only the wallet owner can decrypt it for use.

Two-factor authentication (2FA): Some wallets support 2FA for added security, requiring users to provide a second credential in addition to the password.

Wallet recovery: Some wallets provide a recovery phrase or backup keyword, helping users recover their wallet if the device is lost or damaged.

6. Transaction and Interaction with DApps

Wallets are not only used to store cryptocurrencies but also support users interacting with decentralized applications (DApps) on the blockchain.

Wallet as a gateway: Wallet is a gateway between users and decentralized applications on the blockchain network. Users can use the wallet to make transactions, participate in staking, trade NFTs, or interact with smart contracts.

Wallet-enabled DApps: Wallets such as MetaMask (on Ethereum) or Yoroi (on Cardano) allow users to interact directly with DApps without having to leave the wallet application.

In short, the wallet operates according to the principle:

1. Public and private key pairs help users manage access rights and secure assets.

2. Digital signature ensures transactions can only be performed by the owner of the private key.

3. Software wallets and hardware wallets secure private keys and store assets in the blockchain network.

4. Digital assets are not actually stored in a wallet but are recorded in the blockchain.

5. Security measures such as encryption, two-factor authentication, and recovery keywords help protect user assets.

6. The wallet also helps users interact with DApps and participate in staking, trading, or NFT management activities on the blockchain.

The operating principle of the wallet ensures safety and security for users when they make transactions or manage digital assets.

2.6.1.4 Security issues and risks

When using digital wallets to store and trade assets on blockchains such as Bitcoin, Ethereum, Cardano, or any other platform, users need to be careful of security risks. Although wallets offer many benefits, they also pose risks that can lead to loss of assets or personal data. Below are some common security issues and risks that wallet users should be aware of:

1. Lost or Revealed Private Key

Risk:

Lost private key: If a user loses their private key, they will not be able to access their digital assets. This is serious because blockchain is a distributed system and it is impossible to recover transactions or assets once the private key has been lost.

Exposed private key: If the private key is exposed (due to incorrect sharing by the user, hacking, or unsafe storage), bad actors can appropriate the user's assets.

For example:

Hacked software wallets: Some software wallets like Exodus or Electrum have been attacked by hacker groups, and if users do not protect their private keys with encryption or other security methods, they can lose their funds. product. A notable example is the MyEtherWallet hack in 2018, where hackers hijacked DNS and tricked users into providing private keys.

2. Lost Wallet or Device Damage

Risk:

Loss of hardware wallet: If a user loses their hardware wallet (like Ledger or Trezor) and does not back up enough information (like recovery keywords), they will not be able to recover assets.

Device damage: Hardware or software wallets can be damaged or lost if wallet data is not securely backed up.

For example:

Loss of Trezor hardware wallet: A user may accidentally drop or lose his or her Trezor wallet. Without backing up their recovery phrase, they won't be able to restore access to their assets.

Software wallet damage: Exodus wallet can crash if the user's computer or phone is damaged and there is no backup of the private key or recovery key.

3. Phishing and Fraud Attacks

Risk:

Phishing Attack: This is a phishing technique where hackers impersonate websites or emails from famous wallets such as MetaMask, Trust Wallet, or Coinbase Wallet to steal private keys or personal information.

Fake link scams: Users can be tricked into clicking fake links in emails or messages and entering information on unofficial websites.

For example:

MetaMask Phishing: Some MetaMask users have been tricked into clicking on phishing links and entering passwords or private keys into fake websites, resulting in the loss of all assets.

Coinbase fake email scam: There are phishing attacks where hackers spoof emails from Coinbase and ask users for wallet login information or 2FA authentication codes.

4. Cyber Attacks and Malware (Malicious Software)

Risk:

Malware: A user's computer or phone can be infected with malware to monitor wallet activity, steal private key information, and perform transactions without the user's knowledge. know.

Remote attack: If the wallet is stored on a computer or phone with malware, a hacker can infiltrate and withdraw funds without the user's consent.

For example:

Malware on the computer: A user downloaded a free software, but the software was actually malware that monitored Bitcoin wallet activities and withdrew funds from the wallet without the owner's consent.

Man-in-the-middle (MITM) attack: When a user makes a transaction over an unsecured network, such as public Wi-Fi, a hacker can eavesdrop and interfere with the user's transaction.

5. Security Vulnerabilities in Wallets

Risk:

Software vulnerabilities: Software wallets may encounter security vulnerabilities in the source code, allowing hackers to exploit and appropriate user assets.

Protocol vulnerabilities: Blockchain protocols or wallets may have programming errors or omissions, leading to assets being withdrawn without user consent.

For example:

Security errors in Ethereum wallets: Previously, some Ethereum wallets encountered security errors in smart contracts, causing users to lose money in transactions or when participating in staking.

6. Risks from Social Networks and Fake Advertising

Risk:

Fake ads: Some ads on social media or unofficial websites can lure users into downloading fake wallets or apps.

Investment scams (Ponzi schemes): Scams that involve investing in digital assets or NFTs with promises of high returns, only for users to lose their money.

For example:

Fake wallets on Twitter: There are famous fake wallet accounts like MetaMask or Trust Wallet on Twitter or Telegram, advertising promotions or discounts, and when users download, they install the fake app to steal property.

7. Ownership Rights and Legal Disputes

Risk:

Legal disputes: In cases where the law is unclear about the ownership of digital assets, users may have difficulty protecting their assets if there is a dispute with a partner or the government.

Loss of assets due to legal uncertainty: If there is a legal issue such as hacking or asset appropriation, users cannot recover assets from government agencies or the legal system.

For example:

Legal disputes about NFTs: There can be disputes over ownership or copyright over NFTs, especially when the NFT is resold or exchanged without the creator's consent.

2.6.1.5 Applications

Digital wallets are not simply tools for storing digital assets but also play an important role in many different applications in the world of blockchain and cryptoassets.

Common applications of wallets:

1. Store and manage digital assets (Bitcoin, Ethereum, ADA, NFT).

2. Cryptocurrency trading and payments.

3. Join DApps (DeFi, blockchain games, NFTs).

4. Staking assets to receive rewards.

5. Management of NFTs (Non-Fungible Tokens).

6. Transactions outside the blockchain ecosystem.

7. Store security tokens and certify asset ownership.

8. Identity verification (KYC).

The digital wallet is a powerful tool not only for storing and trading cryptocurrencies, but also supporting users to participate in decentralized applications, staking, NFT management, and many financial services. other.

2.6.2. Address

In the blockchain ecosystem, an address is a string of characters or a unique identifier used to identify a location where a user can receive or send digital assets, such as cryptocurrencies, tokens, or NFTs. This address is often directly related to digital wallets and is an important part of blockchain transactions. In the blockchain ecosystem, an address is a string of characters or a unique identifier used to identify a location where a user can receive or send digital assets, such as cryptocurrencies, tokens, or NFTs. This address is often directly related to digital wallets and is an important part of blockchain transactions.

2.6.2.1. Concept

A blockchain address can be thought of as an "account number" in a bank or a "phone number" used to receive money or assets. However, instead of using names or account numbers, blockchain uses strings of numbers and letters as addresses.

An address is usually created through hashing functions from the public key and strong encryption algorithms to ensure security and protect property ownership.

For example:

Bitcoin Address (BTC): Bitcoin addresses usually start with the character "1" or "3", for example: 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC.

Ethereum Address (ETH): Ethereum address starting with "0x", for example: 0x740ECBbCe82c3F000E01a0038e281f3097d403C5.

Cardano (ADA): Cardano addresses may start with "addr1" and are encoded in a different structure than Bitcoin and Ethereum. For example:
addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

2.6.2.2. Classify

Blockchain addresses can be classified according to the type of blockchain and how the address is used in each system. Common address types include:

a) Bitcoin Address (BTC)

Concept: Bitcoin address used to receive and send Bitcoin in the Bitcoin network.

Characteristics: Bitcoin addresses can start with the characters "1", "3" or "bc1".

For example: *1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC*

Wallet: "P2PKH" (Pay-to-PubKey-Hash) addresses begin with "1", "P2SH" (Pay-to-Script-Hash) addresses begin with "3", and SegWit addresses begin with "bc1".

b) Ethereum Address (ETH)

Definition: An Ethereum address is a 40-character string (excluding the "0x" prefix) used to receive and send Ethereum and ERC-20 tokens.

Characteristics: Ethereum addresses start with "0x".

For example: *0x740ECBbCe82c3F000E01a0038e281f3097d403C5*

c) Cardano Address (ADA)

Concept: A Cardano address is a string of characters generated from special rules of the Cardano blockchain.

Features: Cardano addresses may start with "addr1" and are encoded in a different structure than Bitcoin and Ethereum.

For example:
addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

d) Binance Smart Chain (BSC) Address

Concept: BSC address is the address used to receive and send assets on the Binance Smart Chain network.

Characteristics: BSC addresses are similar to Ethereum addresses, starting with "0x".

For example: *0x6f99fcd64af42c4e2c7289cab0f039080d997f21*

e) Solana Address (SOL)

Concept: Solana address is a long string of characters used in the Solana ecosystem.

Characteristics: Solana addresses are about 32 characters long and have no special prefixes.

For example: *6rKWh6j8jfTpzcsYXsdvxdTt2EZSY61qbb9XfX5g97DE*

2.6.2.3. Principle of operation

Blockchain addresses operate mainly on the principle of linking public key and private key. This process helps authenticate and protect transactions:

1. Create Address

Step 1: Generate public key: The address generation process starts from generating a public key through algorithms such as Elliptic Curve Cryptography (ECC) (in Bitcoin, Ethereum, etc.).

Step 2: Hashing and encryption: To create the address, the public key is re-hashed using hash functions such as SHA-256 and RIPEMD-160, then encrypted into the address.

Step 3: As a result, the address will be a string of characters that represents a unique address in the blockchain network, which can send and receive assets.

2. Transaction with Address

When you want to send money or assets to a blockchain address, you use a private key to authenticate the transaction.

This transaction is transmitted through the network and confirmed by nodes on the blockchain.

Once the transaction is complete, the assets will move from your wallet to the destination address. This process is recorded on the blockchain's public ledger.

3. Security and Authentication

Private key: Only the owner of the private key can sign and approve transactions from his address. Securing your private key is extremely important. If you lose your private key, you will lose access to the assets in your wallet.

Public key: This is public information and is used to create addresses to receive funds from other transactions. The public key cannot be used to sign transactions, but only to receive assets.

2.6.2.4. Security issues and risks

Addresses on the blockchain play an important role in receiving and sending digital assets. However, as with any technology, the security issues and risks associated with blockchain addresses are huge and can cause serious damage if not managed properly. Below are the main security issues and risks of blockchain addresses.

1. Lost Private Key

Risk:

Private keys are the most important security element for managing assets in a blockchain wallet. If you lose your private key, you will not be able to access your assets. This can happen when:

Lost or forgotten private key.

The private key is deleted without backup.

Private keys are stolen due to security breaches or fraud.

For example:

A Bitcoin user loses his private key and has no backup, resulting in the irrecoverable loss of all Bitcoin in his wallet.

Solution:

Back up your private key in multiple safe places, such as paper, security software, or hardware devices.

Use hardware wallets to securely store private keys.

2. Phishing Attack

Risk:

Phishing is a method by which scammers impersonate websites or wallet services, asking users to enter their private keys or sensitive information.

An attacker can spoof a user's wallet address and change the receiving wallet address during a transaction, causing assets to be sent to the fraudster's wallet.

For example:

A user receives a fake email from an exchange, asking to update his account information and enter his private key. After following the instructions, the user's assets are transferred to the scammer's wallet.

Solution:

Always check URLs and links before entering information into websites or wallet services.

Enable two-factor authentication (2FA) to protect wallet accounts.

3. 51% Attack (51% Attack)

Risk:

A 51% attack can occur if the attacker controls more than 50% of the computing power of the blockchain network. This could lead to the possibility of altering transaction history, manipulating transactions, or causing other serious security issues.

If several wallet addresses are hacked or controlled by an attacker group, it can lead to fraud or double-spending.

For example:

The Bitcoin Cash network faced a 51% attack in 2018, leading to some transactions being reversed and funds being double-spent.

Solution:

Use blockchains with highly distributed computing power or switch to proof-of-stake (PoS) instead of proof-of-work (PoW) to minimize this risk.

4. Errors Arising During Address Generation (Address Generation Flaws)

Risk:

Errors during address generation can occur when the software generates the address incorrectly or uses an insecure algorithm. This can lead to the creation of wallet addresses that can be easily predicted or even hacked.

For example:

Some buggy wallets can generate easily guessable addresses, increasing the possibility of attacks from bad actors.

Solution:

Use highly secure certified wallet tools and software, always updated with the latest security patches.

5. Wrong Address Transactions

Risk:

Sending assets to the wrong address can occur if users copy and paste the wrong wallet address, or when there is confusion between wallet addresses (for example, Bitcoin and Ethereum addresses have similar structures). .

Transactions on the blockchain are irreversible, so if assets are mistakenly sent, users will not be able to get them back.

For example:

Users send Bitcoin to an Ethereum address, and due to differences between blockchains, the transaction cannot be carried out, causing loss of assets.

Solution:

Double check the wallet address before sending the transaction.

Use QR codes or support tools to avoid errors in entering incorrect addresses.

6. Risks from Hot Wallets

Risk:

Hot Wallets are wallets that are directly connected to the internet and are vulnerable to external threats such as viruses, malware or hackers.

Intermediary wallets on exchanges can also be targets of attacks.

For example:

In 2014, the Mt. Gox was hacked and lost 850,000 Bitcoins, most of which were users' assets stored in the exchange's hot wallets.

Solution:

Store assets on cold wallets, especially large assets, and only use hot wallets for short-term or test transactions.

Enable two-factor authentication (2FA) and protect wallet accounts with other security methods.

7. Privacy Related Issues

Risk:

Blockchain is a public ledger, which means all transactions can be reviewed globally. This could lead to personal information being exposed if your wallet address is linked to a real identity.

Even though transactions on the blockchain are pseudonymous (anonymous), being able to trace wallet addresses to a specific individual is still possible if personal information is disclosed.

For example:

Users do not realize that their wallet addresses can be tracked through blockchain analytics tools, leading to the risk of exposing personal financial and identity information.

Solution:

Use a new address for each transaction for increased security and anonymity.

Consider using layer 2 solutions like CoinJoin to make transactions harder to trace.

In short

Address security on blockchain is an important issue for users and organizations using this technology. Understanding the risks and how to protect assets is essential to avoid asset loss and possible attacks.

2.6.2.5. Application

Addresses on the blockchain are not only places to store assets, but also play an important role in many different applications and services.

1. Cryptocurrency Transactions

Application: Blockchain addresses are mainly used to send and receive cryptocurrency. Each wallet address on the blockchain is a receiving point, allowing cryptocurrency transactions to take place between users.

For example:

A Bitcoin user can send BTC from the address 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC to the recipient's address.

Similarly, Ethereum users send ETH from the address 0x740ECBbCe82c3F000E01a0038e281f3097d403C5 to another Ethereum address.

Purpose: Perform online payment transactions. Cross-border money transfers without the involvement of intermediary financial institutions.

2. Use in Smart Contracts

Application: Smart contracts on the blockchain use wallet addresses to perform automatic transactions when certain conditions are met. The address in this case can be the address of the smart contract or the address of the contract participants.

For example, a smart contract on Ethereum can receive payments from users and then automatically perform an action (e.g. delivery or licensing) when the payment is complete.

Purpose: Automate agreements without the need for intermediaries. Ensuring transparency and reliability in complex transactions.

3. Address Linked to NFTs (Non-Fungible Tokens)

Application: In the NFT ecosystem, wallet addresses are used to buy, sell, and store NFTs. Each NFT can be transferred from one address to another when a transaction is made. Users who own NFTs will keep them in their wallets under separate wallet addresses.

For example, an artist can create and sell NFTs on platforms like OpenSea, where the wallet addresses of the buyer and seller play a decisive role in the transfer of ownership of the NFT.

Purpose: Transfer of unique digital assets (NFT). Confirm ownership and authenticity of digital items.

4. Digital Asset Management and Storage

Applications: Blockchain addresses are also used in managing digital assets other than cryptocurrencies, such as tokenizing assets (real estate, stocks, or digital items). These assets can be transferred or resold as tokens, and management of these tokens is done via a blockchain wallet address.

For example, financial institutions can issue Security Tokens to represent stocks or assets. Investors will own these tokens through their wallet addresses.

Purpose: Ensure ownership and legality of digital assets. Facilitates the trading of assets in a blockchain environment.

5. Transactions and Token Management in DApps (Decentralized Applications)

Application: Decentralized applications (DApps) use wallet addresses to conduct token transactions, participate in blockchain games, staking, or voting. Users interact with DApps through their wallet addresses, thereby performing actions such as staking tokens, participating in governance, or earning rewards.

For example, in a blockchain game like Axie Infinity, players can own tokens in their wallets and use them to buy items or participate in battles. In DeFi (decentralized finance) projects, users can use their wallets to stake or lend tokens.

Purpose:Create decentralized financial services (DeFi) without the participation of banks or intermediary financial institutions. Ensures complete control of assets and personal information for users.

6. Identity Ownership and Management (Identity Management)

Application: Blockchain provides a way for users to securely manage their identities through wallet addresses. These addresses can be used to verify identities, store and protect personal information on blockchain platforms without having to rely on intermediary organizations.

For example, Self-sovereign identity (SSO) allows users to control their personal information and share it when necessary without having to go through a centralized certification authority.

Purpose: Provide a secure method for online identity verification. Minimize fraud issues and protect user privacy.

7. Payments and Microtransactions

Application: Wallet addresses on the blockchain are also used to make payments and microtransactions. Payment services such as Lightning Network (Bitcoin) or payment protocols on other blockchain platforms allow fast and low-cost payments, helping users transact conveniently and easily.

For example: Use the Bitcoin Lightning Network to perform small, low-cost transactions, e.g., pay for digital content, use an online service, or send small amounts of money to friends.

Purpose: Increase the ability to pay online in small amounts without high transaction fees. Promote blockchain application in traditional payment services.

8. Create and Manage Gift Card Codes (Gift Cards)

Application: Some platforms use blockchain to issue and manage gift cards. The blockchain wallet address can be used to receive and pay with these gift cards.

For example, a gift card service can issue card codes as tokens on the blockchain, and recipients can use the blockchain wallet to pay for products and services.

Purpose: Reduce fraud risk and improve security in gift card exchanges. Use blockchain to make the card issuance and usage process transparent and secure.

In short: Addresses on the blockchain not only serve as a tool to store and transfer assets, but also support many different applications from decentralized finance (DeFi), blockchain games, to platforms. Identity and gift card management. Using blockchain wallet addresses opens up many opportunities for developing and applying blockchain technology in real life, while helping to create safe, transparent and efficient transactions.

2.7. Ledger (LEDGE)

2.7.1. Concept

In blockchain, **ledger** is a distributed database that is continuously updated and stores all verified transactions on the blockchain network. Unlike traditional ledgers, the ledger in

blockchain is not controlled by an intermediary organization, but instead is maintained and confirmed by all participating nodes in the network. Each transaction on the blockchain will be recorded in blocks and linked together into a chain, forming a public, unchangeable "ledger", helping to ensure integrity and security. confidentiality of transactions.

2.7.2. Characteristics of Ledger in Blockchain?

1. Decentralized and without intermediaries:

Blockchain is a distributed system, meaning there is no intermediary authority or organization that controls the ledger. Every node in the network has a copy of the ledger, increasing transparency and security.

2. Immutability:

Once a transaction has been recorded and authenticated in the blockchain, it cannot be altered or deleted. This ensures data integrity and prevents fraud.

3. Openness and transparency:

The blockchain ledger is public, accessible and auditable by anyone. However, sensitive information such as the identity of the transaction participant is often protected through encryption and wallet addresses.

4. Security:

Blockchain ledgers use strong encryption methods to protect data from unauthorized alteration or access. Transactions are confirmed by network nodes through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS).

5. Automation and no need to rely on third parties:

Transactions on the blockchain are authenticated and recorded automatically without the involvement of a third party intermediary, helping to minimize costs and risks associated with intermediaries.

2.7.3. How does the Ledger work in Blockchain?

1. Transactions and blocks:

Each transaction on the blockchain is recorded and confirmed by nodes in the network. Once transactions are confirmed, they are collected into a "block" and added to the ledger.

2. Consensus Mechanism:

Nodes in the network must reach consensus to accept a new block of transactions. Popular consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS) help ensure that transactions are valid and free of fraud.

3. Authentication and recognition:

Once consensus is reached, transactions in the block will be recorded on the blockchain. Each block contains a hash of the previous block, creating a tight chain between blocks, helping to protect data integrity.

4. Anti-fraud and security:

Transactions in the blockchain use asymmetric encryption to protect identities and important information. Once information has been recorded on the blockchain, it cannot be changed without altering all the blocks behind it, which helps protect against fraud.

Summary: The blockchain ledger is a distributed, secure, and immutable system that records and stores all transactions in the network. With features such as transparency, security, and lack of trust in intermediaries, blockchain has brought significant benefits in many fields and opened new opportunities for financial and other applications. non-financial.

2.8. APPLICATION AREAS

Blockchain has many practical application areas, including both traditional industries and new technology fields. Here are some specific areas:

2.8.1. Finance and banking

Blockchain has brought many breakthroughs in the finance and banking sector, helping to optimize processes, reduce costs and increase transparency. Specific areas such as: international payments, smart contracts, asset management, customer data management, automation of compensation processes through smart contracts, ...

For example: Bitcoin, Ethereum, and other cryptocurrencies use blockchain to provide a secure, fast, and bank-independent payment method. Ethereum**:** Allows building smart contracts to automatically process loans, insurance, or distribute dividends.

2.8.2. Supply Chain Management

Supply Chain Management (SCM) is one of the important fields and is being strongly improved thanks to the application of blockchain technology. Blockchain helps improve issues of transparency, security, efficiency and traceability in supply chain management. Here are some applications of blockchain in SC:

1. Enhance Transparency and Traceability

Blockchain helps businesses track the entire production and transportation process of a product from supplier to final consumer. With the immutable and transparent nature of blockchain, every transaction will be recorded on a public and auditable electronic ledger.

For example: *IBM Food Trust* is a blockchain platform used to track food products from farm to consumer's table. This helps ensure product quality, control food safety and limit fraud.

2. Reduce Costs and Transaction Time

Blockchain helps reduce costs and transaction times by eliminating intermediaries (e.g. banks, authentication service providers) in the payment and shipping process.

For example: *VeChain* is a company that uses blockchain to track and manage supply chains, specifically in industries like automotive and fashion. Blockchain helps reduce administrative costs and minimize errors.

3. Security and Fraud Reduction

Transactions in the supply chain can be fraudulent or tampered with, but with blockchain, each transaction is securely confirmed and stored, irreversible. This helps prevent fraud and ensures data integrity.

For example: *Everledger* is a company that uses blockchain to track and authenticate the origin of diamonds. Each diamond has a record on the blockchain, which helps prevent the exchange of fake diamonds and confirms legal origin.

4. Improve Contract Management and Payments

Through the use of smart contracts, blockchain can automate the contract execution and payment process without the intervention of a third party. These contracts can automatically execute when conditions have been met.

For example, a manufacturer can set up smart contracts with material suppliers, requiring payment when goods are delivered in sufficient quantity and quality. Blockchain will record all steps and conditions, helping to automatically carry out transactions without the need for an intermediary controller.

5. Inventory Management

Blockchain can help businesses easily track inventory status and coordinate resources, helping to minimize shortages or overstocks in the supply chain.

For example, Walmart uses blockchain to track inventory status and store data about products in stock. This not only helps improve inventory management but also ensures that every product can be traced back to its source easily and quickly.

6. Product Verification and Certification

Blockchain can support product quality certification, thereby enhancing consumer trust. Information such as quality standards, production processes, and product ingredients will be recorded on the blockchain.

For example, products such as coffee, cocoa beans, or organic products can have their origin verified through blockchain, giving consumers peace of mind that they are purchasing products that meet ethical and environmental standards. school.

7. Cooperation Among Stakeholders

Blockchain promotes collaboration between parties in the supply chain, creating a consensus system where all information is shared securely and transparently. This helps reduce risk and increase efficiency in supply chain operations.

For example: *TradeLens*, a blockchain platform developed by Maersk and IBM, helps shipping companies and ports share information about shipments quickly and transparently, minimizing waiting times and reducing costs.

In short: Blockchain helps optimize many aspects of supply chain management from increasing transparency, security, reducing costs, to automation and contract management. Companies are now increasingly aware of the technology's potential to optimize supply chain processes, creating a more secure and transparent trading environment.

2.8.3. Governance and smart contracts

Governance and smart contracts (Smart Contracts) are one of the prominent and important applications of blockchain, helping to automate administrative processes and contract enforcement without the need for third-party intervention. Here is a detailed look at how blockchain supports governance and smart contracts:

1. Governance with Blockchain

Governance in the context of blockchain refers not only to the management of transactions but also to the management of processes and decisions in distributed systems. Organizations and projects can use blockchain to ensure that decisions are made transparently, fairly, and without interference by anyone.

For example: DAO (Decentralized Autonomous Organization): Is a decentralized autonomous organization, where important decisions are made through votes decided by the

organization's members. These decisions are often made automatically through smart contracts.

2. Smart Contracts

Smart contracts are contracts that automatically execute when conditions have been confirmed. Instead of having to go through intermediaries such as lawyers or banks to enforce a contract, blockchain helps automate all processes and transactions without human intervention.

Smart contract application example:

Use in finance (DeFi - Decentralized Finance): Smart contracts in the financial sector help perform automated transactions such as lending, borrowing, and stock trading without the participation of banks or traditional financial institutions. For example **Compound**, where users can lend and borrow cryptocurrency without going through an intermediary financial institution.

Labor contract and payment: Smart contracts can automatically pay employees when work is completed or when contract conditions are enforced. For example, if a freelancer completes a task, the smart contract can automatically pay them immediately.

2.8.4. Own and collect Digital assets (NFT)

Owning and collecting digital assets (NFTs - Non-Fungible Tokens) is one of the prominent applications of blockchain technology, especially in the fields of art, entertainment, and creative industries. NFTs have created a new trend in buying, selling and collecting digital assets with their unique and irreplaceable nature.

Applications of NFTs in owning and collecting digital assets:

1. Digital Art

NFTs have revolutionized the art industry, helping artists sell their work digitally and receive direct payments without going through auction houses or intermediaries.

For example, one of the most famous artists in the NFT world is Beeple, who sold a piece of his digital art, "Everydays: The First 5000 Days", for nearly $70 million at one sale. Christie's auction.

Application: Each piece of digital art is encoded into a unique NFT, helping buyers claim ownership and ensure the uniqueness of the work.

2. Collectibles and Rare Items

NFTs are also used to collect rare digital items, such as sports trading cards, game items, or even videos, music, and other creative works.

For example, CryptoKitties is one of the popular NFT collectible games where players can buy, sell, and breed unique digital cats. Each cat is a unique NFT.

Application: Game items such as skins, characters, or weapons can also be encoded into NFTs, helping players own and trade them.

3. Events and Event Tickets

NFTs can be used to create digital event tickets, such as concert tickets, sporting events, or online concerts.

For example, Nifty Gateway is a platform that enables the sale of NFT tickets for online arts events and virtual concerts.

Application: Each NFT ticket can contain information about the event, including date, time, location, and even special benefits, and cannot be counterfeited.

4. Virtual Worlds and Metaverse

NFTs play an important role in virtual worlds and the Metaverse, where users can own land, items, or other digital assets in a virtual space.

For example: In worlds like Decentraland or Sandbox, users can buy and own virtual land in the form of NFTs, build projects and trade them.

Application: NFTs provide virtual asset ownership certificates in 3D environments, helping users build assets and value in the Metaverse.

2.8.5. Application in Health

Blockchain applications in healthcare is an area that is receiving increasing attention and development, thanks to the security, transparency and efficient data processing capabilities of this technology. Blockchain can help improve many aspects of the healthcare industry, from managing patient data to improving billing and insurance processes.

1. Manage and share patient data

Blockchain can help improve patient data management and sharing, ensuring that patient information is protected, transparent, and easily accessible when needed. Data such as medical records, test results, and treatment information can be securely stored on the blockchain.

Transparency and security: Data stored on blockchain cannot be changed or deleted, helping to protect the integrity of patient information. Only people with access can view or change data.

Share information quickly and easily: Hospitals, clinics and doctors can share information with each other quickly and securely without the need for complex intermediary systems.

For example, the MedRec Project is a blockchain-based platform that allows patients to control their medical records, while allowing doctors and other medical facilities to easily access information when needed, helping reduce errors and improve health care.

2. Safety and security of medical information

Medical information is one of the most sensitive types of data and is frequently the target of cyberattacks. Blockchain can provide a powerful security solution, ensuring that patient data is stored securely and only authorized people have access.

Anti-Fraud and Traceability: Blockchain has the ability to record all transactions and changes, making it easy to track and verify changes to medical records, preventing fraud and ensuring integrity. accuracy of data.

For example, platforms like Healthereum use blockchain to secure patient information and track participation in health programs, helping to ensure that all actions are transparent and immutable.

3. Pharmaceutical management and drug supply chain

Blockchain can help track and manage the drug supply chain, from production to consumer. This tracking can help prevent counterfeit drugs and ensure the quality and legality of drugs.

Prevent counterfeit drugs: Information about the origin of the drug and the shipping process can be recorded on the blockchain, helping to ensure that the drug is not tampered with or tampered with during transportation.

Tracking drugs and medical devices: Blockchain helps track the condition of drugs and medical devices from production to use, ensuring that products are always in the best condition.

For example, Modum uses blockchain to track pharmaceutical products and ensure that storage conditions are met throughout the shipping process.

4. Payment and health insurance

Blockchain can improve health insurance billing and processing, helping to reduce costs, processing times, and increase transparency in these transactions. Blockchain can support smart contracts to automate these processes.

Payment automation: Smart contracts can automatically process payments between patients, healthcare providers, and insurance companies, helping to reduce errors and fraud.

Fast and accurate insurance process: Insurance companies can use blockchain to store and retrieve patient information, making the insurance claim payment process faster and more accurate.

For example, Solve.Care is a platform that uses blockchain to manage healthcare and health insurance services, helping to automate the billing process and reduce administrative costs.

5. Manage ownership and sharing of genetic information

With the development of precision medicine, sharing and managing genetic information becomes very important. Blockchain can help protect this information and ensure ownership and privacy for individuals.

Privacy protection: Blockchain can help patients control access to their genetic information and decide who can see or use this genetic data for research or treatment purposes.

For example, Nebula Genomics uses blockchain to secure users' genomic data and give them control over their data.

2.8.6. Elections and Government Administration

The application of blockchain in elections and government administration is becoming a topic of intense interest, thanks to its ability to improve the transparency, security, and efficiency of political and administrative processes. Blockchain can help countries and governments make elections more fair, secure and transparent, and manage public systems more effectively.

1. Elections and electronic voting (e-Voting)

Blockchain can help improve the election and electronic voting process by providing a secure and transparent system for recording and verifying votes.

Security and anti-fraud: Each vote can be encrypted into a transaction and stored on the blockchain, helping to protect data from being altered or deleted. This prevents fraud such as changing votes or tampering with election results.

Transparent and public: All information about votes and results will be recorded on the blockchain, allowing everyone to check and verify the results without relying on a third party. Blockchain ensures transparency and accuracy throughout the entire process.

Remote voting: Blockchain can help implement remote voting systems, allowing voters to vote from anywhere without having to go to traditional polling stations. This is especially useful in global elections where voters can vote from abroad.

For example, Project Voatz is a blockchain-based electronic voting platform that has been tested in several US elections, allowing citizens to vote via mobile applications with a high level of security.

2. Manage citizen records and electronic documents

Blockchain can be used to manage citizen records, electronic documents, and other important information that the government stores. This improves transparency, security and reduces data tampering.

Secure citizen records: Citizen records such as birth certificates, identity cards, household registration, or tax information can be stored on blockchain, helping to protect personal information from being falsified or lost. cool.

Minimize administrative procedures: The government can reduce complex administrative procedures and save people time by using blockchain to automate processes related to issuing documents or certification.

For example: **Estonia** is a pioneer in using blockchain for public services, including the issuance of electronic identification cards, citizen record management and medical services.

3. Budget and public finance management

Blockchain can help improve government public finance and budget management processes, from tracking revenue and expenditure to distributing funds.

Transparency in public spending: Blockchain helps track all government spending, helping people and organizations monitor the use of public budget transparently and accurately.

Minimize corruption: Blockchain ensures that every public financial transaction is clearly recorded and cannot be changed, thereby minimizing the possibility of corruption and abuse of power in budget distribution.

For example, countries like Georgia are already using blockchain in land management and public finances to increase transparency and reduce corruption.

4. Smart Contracts in government management

Smart contracts can be used in government administrative and legal processes, helping to automate the execution of contracts without the need for third-party intervention.

Automate legal processes: Smart contracts can automatically enforce contract terms without the intervention of lawyers or intermediaries. This helps save costs and time for legal processes.

Transfer of public assets: Blockchain and smart contracts can support the transfer of public assets quickly and efficiently. For example, when a citizen purchases public property or participates in social housing programs, smart contracts can automatically handle contract terms without having to go through complicated procedures.

For example, Ukraine has tested the use of smart contracts to automate the process of issuing land ownership certificates.

5. Management of ownership and distribution of public assets

Blockchain can help manage ownership of public assets, such as land, natural resources, and other national assets. It helps clearly define ownership, avoid disputes and provide a transparent public asset distribution system.

Natural resource management: Blockchain can help governments track the exploitation of natural resources and ensure that the distribution of these resources is legal and fair.

Land management: Land records can be stored on blockchain, helping to minimize land ownership disputes and ensure transparency in land transactions.

For example, Ghana and Rwanda are two countries that have begun implementing blockchain in land ownership management, helping to reduce disputes and increase transparency in land transactions.

6. Fight corruption and increase transparency

Blockchain can help increase transparency in government operations and reduce corruption.

Financial monitoring: Public expenditures can be tracked directly on blockchain, helping people and organizations monitor government budget usage.

Monitor political decisions: Decisions made by government officials can be recorded on the blockchain, ensuring that the decisions made are public and transparent.

For example, Sierra Leone has been experimenting with using blockchain to track and monitor their elections, helping to ensure transparency and fairness.

In short, *Blockchain applications in elections and government management can help improve the transparency, security, and efficiency of political and administrative processes. Although blockchain offers many significant benefits, implementing this technology still faces a number of challenges, including changes in organizational structures, legal and security issues, and ensuring people's acceptance. However, with the benefits that blockchain brings, countries can take advantage of this technology to build a more transparent and fair government system.*

2.8.7. Data security and ownership

Blockchain application in data security and ownership is one of the important areas, as blockchain technology can solve problems of security, privacy and data control in an increasingly digitization. Blockchain helps users control their personal data, ensuring that information is not changed, copied or accessed illegally.

1. Personal data security and privacy

Blockchain helps protect users' personal data by storing information in a distributed network where there is no single central database, which minimizes the risk of attack or breach. .

Data Encryption: Blockchain uses strong encryption methods to ensure that data can only be accessed by authorized people. When information is stored on the blockchain, it is fragmented and encrypted, making unauthorized access very difficult.

Access Control: Users can decide for themselves who has access to their data through the use of private keys and encryption technology. This helps them retain control and protect personal data from intrusion by third parties.

For example: **SelfKey** is a platform that allows users to control ownership and access of their personal information. Through blockchain, users can share or retain their data without relying on intermediary organizations.

2. Manage data asset ownership

Blockchain can provide a way to certify ownership of digital assets, including data, files, images, videos, and other digital resources. Through blockchain, users can verify ownership and protect their digital assets.

Certificate of data ownership: Blockchain helps record ownership of digital assets by encoding the asset as a token and storing it on a blockchain. Each asset will have a unique and unchangeable identification code that helps identify who owns the asset.

Copyright and usage rights management: Blockchain can help organizations and individuals manage copyright rights of digital assets. Smart contracts can automatically confirm and enforce agreements on rights to use, distribute, and pay fees for the use of assets.

For example, Filecoin is a project that uses blockchain to create a decentralized storage platform where users can store and access data while maintaining ownership and security of information.

3. Managing ownership in the creative industries

Blockchain can help protect intellectual property in creative industries such as music, digital art, film, and literature. Through blockchain, artists and authors can certify ownership and control the use of their work.

Certificate of work ownership: Digital works of art, music, videos and other creative products can be encoded into NFT (Non-Fungible Token) tokens on the blockchain, helping to verify ownership and help artists receive profits from the sale and transfer of works.

Copyright management: Smart contracts can automatically enforce copyright terms, helping artists and authors manage and protect their rights.

For example, Audius is a decentralized music platform where artists can upload and manage their music, protect their ownership, and receive compensation directly from listeners.

In summary, Blockchain applications in data security and ownership open up a bright future for data management and protection in many different fields, from healthcare, finance, to the creative industry. create. Blockchain not only helps with security and privacy, but also helps users maintain control over their own data. With these benefits, blockchain is gradually becoming an important tool in solving issues of security and data ownership in the digital era.

QUESTIONS AND EXERCISES

1. What is Blockchain? Let's briefly explain this concept.

2. Outline the important characteristics of blockchain and explain why immutability is the most important factor.

3. What is the consensus algorithm? Compare PoW and PoS.

4. What is a smart contract? Give an example of its application.

5. Describes how blocks are linked together in the blockchain.

6. Who developed the Paxos protocol, which laid the foundation for consensus mechanisms in computer networks?
a. Satoshi Nakamoto
b. Leslie Lamport
c. Stuart Haber
d. David Chaum

7. What year was the article "Bitcoin: A Peer-to-Peer Electronic Cash System" published?
a. 1991
b. 2008
c. 2009
d. 2016

8. Which of the following characteristics is not a characteristic of blockchain technology?
a. Ledger only allows additional entries (Ledger)
b. Secure with password (Secure)
c. Centralize management
d. Distribute and share information

9. What was the first blockchain application?
a. Ethereum
b. Bitcoin
c. NFT
d. Hashcash

10. In what year was Blockchain officially introduced to the public?
a. 1989
b. 1991
c. 2009
d. 2016

11. Compare the basic differences between public blockchain and private blockchain.

12. How can hybrid blockchain be applied to the real estate sector? Give an illustrative example.

13. Why is consortium blockchain considered a solution that combines public and private blockchain?

14. Explain why the shutdown of a public blockchain originator does not affect the operation of the network.

15. In your opinion, how does the "less transparency" disadvantage of consortium blockchain affect real-world applications?

16. What is cryptocurrency?

17. How does cryptocurrency work?

18. Name some popular cryptocurrencies.
19. Distinguish between cryptocurrency and fiat money.
    Let's present the differences between cryptocurrencies and fiat currencies, especially in factors such as issuance mechanism, control and liquidity.
20. Analyze how blockchain technology ensures the security of cryptocurrency transactions.
    Let's explain the security mechanisms that blockchain uses to protect cryptocurrency transactions, including the role of cryptography, consensus mechanisms, and distributed architecture.
21. Research the applications of cryptocurrencies in various industries.
    Choose a specific application of cryptocurrency (e.g. decentralized finance - DeFi) and research how it affects that industry. Presents a real-life example of using cryptocurrency in this application.
22. What is Tokenomics?
    A simple explanation of tokenomics and its importance in the blockchain ecosystem.
23. Compare the difference between token economics and traditional economics?
    Let's explain the main differences between using currencies in the traditional economy and using tokens in blockchain.
24. Bitcoin has several important characteristics in tokenomics. Can you list and explain these characteristics?
    Outlines the key factors in Bitcoin's tokenomics and how they affect the value of Bitcoin.
25. Why is predicting the number of tokens in circulation important in blockchain projects?
    Analyze the importance of controlling the number of tokens and token distribution plans in cryptocurrency projects.
26. What are NFTs?

    Explain the concept of NFTs and the difference between NFTs and fungible assets like cryptocurrencies.

27. Why are NFTs important to artists and content creators?
    Let's explain the importance of NFTs for artists and content creators in authenticating ownership and creating value for digital works.
28. NFTs are not divisible, why do some platforms introduce partial ownership?
    Analyze why splitting NFTs into smaller pieces is the new trend, and how the Fractional platform has helped the NFT market.
29. Let's give an example of an NFT project on the Cardano platform and how it has grown the NFT ecosystem on Cardano.
    Introducing the first NFT project on the Cardano platform and its implications for the development of the NFT ecosystem on Cardano.
30. What factors do NFTs depend on for their value to increase over time?
    Analyze how supply and demand factors affect the value of NFTs in the investment market.

31. What are NFTs?
Explain the concept of NFTs and the difference between NFTs and fungible assets like cryptocurrencies.

32. Why are NFTs important to artists and content creators?
Let's explain the importance of NFTs for artists and content creators in authenticating ownership and creating value for digital works.

33. NFTs are not divisible, why do some platforms introduce partial ownership?
Analyze why splitting NFTs into smaller pieces is the new trend, and how the Fractional platform has helped the NFT market.

34. Let's give an example of an NFT project on the Cardano platform and how it has grown the NFT ecosystem on Cardano.
Introducing the first NFT project on the Cardano platform and its implications for the development of the NFT ecosystem on Cardano.

35. What factors do NFTs depend on for their value to increase over time?
Analyze how supply and demand factors affect the value of NFTs in the investment market.

36. What is the biggest challenge of NFTs in the current market? a) Market instability
b) Security of blockchain
c) Artistic value of NFTs
d) Ability to authenticate identity

37. Why are high transaction fees such a big challenge for NFT users? a) High transaction fees only affect the seller
b) Transaction fees reduce returns from investing in NFTs
c) Transaction fees reduce consumer participation and create entry barriers
d) Transaction fees do not affect the development of NFTs

38. How can NFTs help artists in protecting the copyright of their works? a) By allowing artists to reproduce their work as NFTs
b) By helping artists receive direct revenue from NFT sales
c) By allowing artists to sell their work through major companies
d) By devaluing the original work of art

39. What is a wallet in blockchain? Explain the importance of wallets for cryptocurrency users.

40. Distinguish between software wallets, hardware wallets, online wallets and paper wallets. State the advantages and disadvantages of each type of wallet.

41. What role do public and private keys in wallets play in securing digital assets?

42. What impact do cryptocurrency wallets have on trading and managing digital assets like cryptocurrencies or NFTs?

43. Let's explain how wallets work in the blockchain world, especially in signing transactions and securing assets.

44. Lists the security measures the wallet uses to protect user assets.

45. What common security issues and risks should wallet users be aware of when using digital wallets?

46. Why are blockchain addresses important for cryptocurrency transactions?

47. How can smart contracts use blockchain wallet addresses to automatically perform actions?

48. In the NFT ecosystem, what role do wallet addresses play in asset transfers?

49. How can blockchain help manage and store digital assets beyond cryptocurrencies?

50. What is the application of blockchain addresses in DApps and what benefits does it bring to users?

51. What applications can use blockchain to manage personal identities and protect privacy?

52. How are microtransactions on the blockchain implemented and why are they low-cost?

53. What is the function of a blockchain wallet address in creating and managing gift cards?

54. How is a blockchain ledger different from a traditional ledger?

55. Why doesn't blockchain need an intermediary organization to maintain the ledger?

56. Explain the concept of "immutability" in blockchain and why is it important for the security of transactions?

57. What characteristics of blockchain ledgers enhance transparency and security?

58. How does a consensus mechanism like Proof of Work (PoW) or Proof of Stake (PoS) work in confirming transactions on the blockchain?

59. Describe the process of recording and authenticating transactions in blockchain.

60. How does Blockchain use asymmetric encryption to protect transactions?

61. Why does not being able to change data in the blockchain help protect against fraud?

62. Explain the benefits that blockchain ledgers bring to financial and non-financial applications.

REFERENCES

1. https://www.pcmag.com - *By Rob Marvin*
2. https://www.techtarget.com - by *Ron Karjian and Robert Sheldon*
3. https://www.kaspersky.com -
4. https://www.coinbase.com -
5. https://www.businessinsider.com -
6. https://www.techtarget.com -
7. https://academy.binance.com -
8. https://www.researchgate.net
9. https://cointelegraph.com - by Guneet Kaur
10. https://coin68.com - by Phong – Update 04/2023
11. https://www.gao.gov/assets/gao-19-704sp.pdf - GAO-19-704SP Blockchain & Distributed Ledger Technologies