CHAPTER 5: CHALLENGES AND TRENDS OF BLOCKCHAIN

5.1. Challenges of Blockchain

So that Bitcoin can become *"new type digital assets"* the same (and possibly more) way that gold does in the real world, or Ethereum plays a role *world's computers* (Vitalik Buterin, co-founder of Ethereum), or Cardano is *Public Blockchain platform serving billions of people* (Charles Hoskinson, founder of Cardano) ... Blockchain platforms need to overcome a series of challenges. This chapter will analyze from basic technical challenges, known as the "impossible triangle" (Blockchain Trilemmas), to challenges related to mass application of Blockchain platforms in life. .

The "Impossible Triangle" was first mentioned in an article by Vitalik Buterin in 2017, referring to three important factors that any Blockchain platform must balance: decentralization), security level, and scalability. In theory, it is difficult for a Blockchain to optimize all three of these factors at the same time. For example, if the focus is on scalability to process more transactions in a short time, the platform may have to sacrifice some degree of decentralization or security. Conversely, when security or decentralization is a priority, scalability is often reduced. This challenge forces developers to come up with creative solutions to achieve the right balance between factors without undermining the core goal of Blockchain.

In addition to technical challenges, Blockchain platforms also face many other problems. Legal challenges are one of them, stemming from the newness of the technology and the fact that some individuals or organizations take advantage of Blockchain to carry out illegal acts such as money laundering, fraud, or trading. multi-level. These problems not only reduce public trust but also cause regulators to enact stricter control policies, sometimes slowing down the industry's development.

Besides, the complexity of Blockchain applications is also a major barrier. Understanding and using this technology requires a certain level of knowledge, making it inaccessible to the majority of users. Society's awareness of Blockchain is still limited, and many people even consider it an impractical or highly speculative technology. Furthermore, the shortage of experienced professionals in this field also hinders the ability to apply Blockchain to practical areas, reducing the speed at which this technology can be integrated into everyday life.

We will learn about the challenges together in the section below

5.1.1. Technically challenging

5.1.1.1. Scalability

One of the biggest challenges of blockchain is scalability. This problem is expressed through the following aspects:

• **Block size limit**: Each block on the blockchain has a fixed size, limiting the number of transactions that can be processed in a certain time. For example, Bitcoin with its 1 MB block limit often experiences congestion when the number of transactions increases, causing confirmation times to lengthen. Ethereum has had similar problems in the past due to its reliance on gas limits for each block, especially when there are many decentralized applications (dApps) operating on the platform.

• **Transaction processing time**: With consensus mechanisms as outlined in the previous chapter, transaction confirmation times can range from minutes to hours during times of network congestion. For example, Bitcoin uses a Proof of Work (PoW) mechanism, which makes the average time to add a new block about 10 minutes. Meanwhile, Ethereum, after switching to a Proof of Stake (PoS) mechanism in 2022 through "The Merge," has improved performance and reduced energy consumption. However, transaction processing wait times can still be long during peak periods.

• **Transaction costs**: As traffic surges, both Bitcoin and Ethereum have seen transaction costs skyrocket. On Ethereum, gas costs have decreased thanks to Layer-2 solutions like Optimistic Rollup and zk-Rollups, but fee spikes can still occur when multiple smart contracts or dApps are active simultaneously.

To solve scalability issues, many options have been implemented and continue to be developed:

1. **Conversion of consensus mechanism**: Ethereum has completed the transition from Proof of Work (PoW) mechanism – slow and energy consuming – to Proof of Stake (PoS) – fast and minimal energy consumption – in 2022 through the historical event "The Merge." This is an important step in the Ethereum 2.0 roadmap to improve scalability and reduce environmental impact. Before "The Merge," the Ethereum network operated two chains in parallel: the main chain (Mainnet) based on PoW and the Beacon Chain based on PoS. When "The Merge" occurs, these two chains are

merged, removing PoW completely and Ethereum officially operates entirely on PoS. After switching to POS, the Ethreum network achieved impressive initial results:

- **Energy efficiency**: PoS reduces up to 99.95% of energy consumption compared to PoW.
- **Higher security**: PoS requires validators to lock up a large amount of ETH to participate, increasing the cost of attacking the network.
- **The foundation for further improvements**: The move to PoS paves the way for scaling solutions like sharding.

2. **Sharding**: This is one of the important solutions in Ethereum's development roadmap. Sharding divides the blockchain network into smaller segments, called "shards." Each shard can process transactions and smart contracts independently, helping the network process multiple transactions in parallel instead of sequentially on a single chain. For example, a bank must process 1,000 transactions at the same time. If a bank has 10 branches (similar to shards), each branch only needs to process 100 transactions instead of the full 1,000 transactions. This saves time and reduces the load on the main system. On Ethereum, sharding will reduce pressure on the main network (Layer-1), helping to increase transaction speed and reduce costs.

   As of 2025, sharding is still in the implementation phase, expected to become an important part of Ethereum in the coming years with appropriate improvements. This is the next step after "The Merge," helping Ethereum achieve its goals of scalability and better compatibility with decentralized applications.

3. **Layer-2**: Layer-2 solutions such as Lightning Network for Bitcoin, Optimistic Rollup, zk-Rollups, and Polygon on Ethereum have been widely adopted. They help reduce the load on the main network (Layer-1) and improve processing speed as well as reduce transaction costs.

4. **New generation Blockchain**: Projects like Solana, Avalanche, Cardano, Sui, Aptos… have introduced new innovations in scalability and interoperability between blockchains. Solana stands out for its high transaction processing speed, while Aptos and Sui focus on programming efficiency and parallel data processing capabilities.

Thanks to these improvements, the blockchain ecosystem has gradually overcome many limitations in scalability, creating a foundation for sustainable development and expanding real-world applications.

5.1.1.2 Security issues

Although blockchain is designed to be highly secure thanks to its encryption and decentralization mechanisms, there are still some potential weaknesses that, if not managed well, can seriously impact the system.

- **51% Attack**: This is one of the biggest risks for blockchains that use Proof of Work (PoW) consensus mechanism. A 51% attack occurs when one entity or group controls more than 50% of the computing power (hash power) of the entire network. With this power, attackers can manipulate the network by creating fake blocks, reversing confirmed transactions, or blocking new transactions. This destroys the integrity and trustworthiness of the blockchain network. However, this attack is often difficult to occur with large blockchains like Bitcoin due to the huge costs and resources required.
- **Vulnerabilities in smart contracts**: Smart Contracts are pieces of code that automate rules and transactions on the blockchain, but they are not immune to programming or design errors. Vulnerabilities in source code can be exploited by hackers to steal money or destroy data. A prime example is the DAO attack on Ethereum in 2016, when hackers took advantage of a bug in smart contract code to withdraw millions of dollars from the fund. Therefore, thorough source code testing and auditing is extremely important to minimize this risk.
- **Dangers from quantum computers**: With superior computing power, quantum computers could threaten to break current blockchain encryption algorithms such as SHA-256 (Bitcoin) or ECDSA (Ethereum). These algorithms were originally designed to resist attacks from classical computers, but are not capable of resisting advances in quantum computers. If the encryption algorithms are broken, all data on the blockchain can be decrypted, leading to the risk of losing information and assets. We can rest assured that at the present time, researchers and developers are actively working to create quantum-resistant encryption algorithms to protect blockchain in the future.

These weaknesses highlight that, although blockchain is an advanced and highly secure technology, it is not invulnerable. Continuous upgrades, combined with safeguards such as source code audits, increased decentralization, and quantum-resistant technology research, are necessary to maintain the safety and sustainability of blockchain.

5.1.1.3. Energy consumption and environmental impact

Blockchain networks, especially those that used Proof of Work (PoW) consensus mechanisms such as Bitcoin and Ethereum before converting to Proof of Stake (PoS), have been criticized for their high energy consumption. and negative impact on the environment.

Energy consumption of Blockchain networks

PoW requires “miners” to solve complex cryptographic problems to verify transactions and create new blocks. This process uses a large amount of computational resources, leading to huge energy consumption. According to estimates:

- The Bitcoin network consumes about 110 TWh per year (equivalent to the consumption of a small country like the Netherlands).
- Ethereum before converting to PoS consumed about 70 TWh/year.

Energy consumption mainly comes from data centers and specialized equipment (ASIC, GPU), which are often operated 24/7 in countries with low electricity prices.

Environmental impact

The power source for blockchain networks often comes from fossil energy such as coal or natural gas, leading to large amounts of CO2 released into the environment. Studies show that:

- Bitcoin mining emits about 60-70 million tons of CO2 per year.
- Global warming and depletion of energy resources are significant consequences.

In addition, the production and operation of mining equipment also generates huge electronic waste, putting additional pressure on the environment.

Operational methods reduce impact

Proposed and implemented solutions to minimize the environmental impact of blockchain include:

- **Convert to Proof of Stake (PoS):** Ethereum successfully transitioned to PoS in 2022, reducing energy consumption by over 99.9%. PoS does not require complex cryptographic math, instead, validators are chosen based on the amount of assets held.
- **Use renewable energy:** Mining data centers are looking to use solar, wind and hydropower to reduce carbon emissions. For example, in Iceland and Canada, mining companies take advantage of abundant geothermal and hydroelectric energy resources.
- **Off-chain and Layer 2:** Scaling solutions such as Lightning Network or Optimistic Rollup help offload transactions directly onto the blockchain, thereby reducing overall energy consumption.
- **Regulations and policies:** Some countries are adopting policies that restrict PoW mining or prioritize environmentally friendly blockchain projects.

Real-life example

Ethereum, after switching to PoS, has become a clear demonstration of how blockchain can maintain decentralization and security without consuming too much energy. In addition, new blockchain networks such as Algorand, Cardano, and Polkadot also use energy-efficient consensus mechanisms right from the design, to optimize performance and reduce environmental impact.

In summary, although blockchain brings many benefits to society and the economy, energy and environmental issues still need to be strictly managed to ensure long-term sustainability.

5.1.2. Governance and interoperability challenges

5.1.2.1. Governance challenges of Blockchain networks

Blockchain governance refers to how decisions are made and enforced within the system, including managing updates, changes in the protocol, and how disputes are resolved. Major blockchain governance challenges include:

a. Centralized decision vs. decentralized

Although blockchain is often designed to be decentralized, many projects suffer from the problem of concentrating power in the hands of a few people. This happens when development teams, project "leaders" or majority token holders can control important decisions, such as protocol changes or software updates.

For example, in the case of Bitcoin, control by miners or large organizations over protocol changes or network upgrades can cause divisions in the community, as happened with the fork. into Bitcoin and Bitcoin Cash in 2017.

b. Lack of consensus in the community

Even though blockchain is a distributed system, achieving consensus among community stakeholders is very difficult. Protocol changes or network upgrades may encounter resistance from some users or developers. This can lead to network fragmentation (hard forks) or major problems in maintaining network integrity. For example, Ethereum's upgrade from Proof of Work (PoW) to Proof of Stake (PoS) encountered a lot of controversy before succeeding.

c. Community's ability to decide

Some blockchains, such as Ethereum, have adopted decentralized governance through DAOs (Decentralized Autonomous Organizations), where decisions are made through community voting. However, this still faces many problems such as limited community participation, lack of control mechanisms and risks of manipulation by influential groups.

5.1.2.2. The challenge of interoperability of Blockchain networks

Cross-chain interoperability is one of the important factors to create a comprehensive blockchain ecosystem, where networks can communicate and exchange data or assets with each other. . However, this problem faces some major challenges:

a. Lack of common standards

Each blockchain has its own unique characteristics and protocols, which creates massive fragmentation in the blockchain space. Different networks may use completely different consensus systems, encryption methods, and economic models. This makes connection and interaction between blockchains complex and requires the development of common technologies and standards. Currently, there is no single common standard for the interoperability of blockchain networks.

b. Bridge and intermediary

One of the current methods to solve the problem of interaction between blockchains is through bridges, which allow the transfer of assets and data between different networks. However, bridging also brings risks, especially security issues. Attacks on blockchain bridges, such as the Poly Network hack in 2021, have exposed vulnerabilities in the system, causing hundreds of millions of dollars in losses.

c. Layer 2 solutions and cross-chain protocols

Layer 2 solutions like Lightning Network (for Bitcoin) and cross-chain protocols like Polkadot, Cosmos, or Avalanche were developed to solve the interoperability problem. These solutions allow multiple blockchains to communicate and interact with each other without having to change the internal structure of each network. However, these solutions are still in the development phase and are not always easy to deploy and maintain.

5.1.2.3. Real-life example

- **Ethereum and Bitcoin:** Even though Ethereum and Bitcoin are both the two largest and most popular blockchains, they cannot communicate directly with each other. Solutions like wrapped Bitcoin (WBTC) on Ethereum help solve this problem, but have limitations and are not an optimal solution.
- **Polkadot:** Polkadot is an example of a blockchain designed from the ground up to support interoperability between blockchains. The Polkadot network uses a mechanism called parachains to connect blockchains together, allowing applications and assets to transfer between networks.

5.1.2.4. The future of governance and interoperability

Although blockchain governance and interoperability are currently challenging, the development of new protocols and platforms is opening up huge opportunities. Decentralized governance mechanisms are increasingly being perfected and popular, and Layer 2 solutions and cross-chain protocols promise to help create a stronger and more closely linked blockchain ecosystem in the future. future.

In short, governance and interoperability challenges are important issues that need to be resolved for blockchain to become a truly developed and widely applied technology in society.

5.1.3. Legal and compliance challenges

5.1.3.1. The legal framework is not complete

One of the biggest challenges in blockchain and cryptocurrency adoption is the incomplete legal framework. Even though blockchain has existed for many years, regulatory agencies have not yet completed the necessary regulations to regulate the operation of these networks. Issues related to the legal framework include:

a. Lack of clear regulations on cryptocurrency and blockchain

While some countries have begun to develop regulations related to cryptocurrency and blockchain, the majority of these regulations lack clarity and completeness. Countries such as the US, China, and the European Union have all begun testing and introducing some regulations, but many aspects remain unresolved, such as how to classify cryptocurrencies and taxes on them. blockchain transactions, or consumer protection regulations.

For example, in the US, the Securities and Exchange Commission (SEC) has not yet provided a clear definition of cryptocurrency and the management objects for each type of digital currency. This leads to instability in transactions and investment decisions related to cryptocurrency.

b. Differences in regulations between countries

Another major challenge is the difference in regulations between countries. Each country has a different approach to blockchain and cryptocurrency, creating a complex regulatory environment. Some countries such as Japan and Switzerland have embraced cryptocurrency and blockchain as part of the mainstream economy, while other countries such as China and India have introduced bans or restrictions. Strict regulations for activities related to blockchain and cryptocurrency.

This difference not only creates a lack of uniformity in regulations but also makes it difficult for businesses and individuals to operate cross-border. The absence of a unified legal system could make it difficult for blockchain companies to expand and comply with international regulations.

The good news is that in 2024, Vietnam issued Decision No. 1236/QD-TTg of the Prime Minister on the National Strategy for applying and developing blockchain technology until 2025, oriented to 2030. This decision identifies Blockchain as a key technology that needs to be prioritized for development, with the vision of making Vietnam a leading country in the region and an international position in research and implementation. Blockchain technology by 2030. This is an important legal foundation, contributing to promoting comprehensive digital transformation, while also opening up strong development opportunities for Blockchain technology in Vietnam now and in the future.

c. The challenge of applying existing law to new technology

One of the big issues is the application of current laws to blockchain and cryptocurrency. Current laws are designed for traditional financial systems and do not accommodate blockchain's unique characteristics such as decentralization, anonymity, and automation through smart contracts. This makes it difficult for regulatory agencies to regulate and apply current regulations to these new technologies.

5.1.3.2. Protect users in the Blockchain ecosystem

One of the important factors that need to be considered in blockchain networks is user protection. While blockchain offers transparency and security, user protection issues are complex, especially in a decentralized and intermediary-free environment. Major user protection challenges include:

a. Lack of user protection mechanism when problems occur

In a blockchain system, transactions are immutable and there is no clear mechanism to deal with problems, such as when a user's assets are stolen or lost. The lack of legal or consumer protection mechanisms puts users at risk when participating in blockchain networks.

A typical example is hacks of cryptocurrency exchanges, where users can lose assets without a chance to recover or protect their interests. Since there is not a regulatory body or legal protection like traditional banks, claiming compensation or resolving disputes becomes difficult.

b. Difficulty in recovering lost or stolen digital assets

Another big problem in blockchain is the recovery of lost or stolen digital assets. With its decentralized nature and no intermediary monitoring mechanism, when users lose access to their wallets or assets are stolen, it is difficult to recover or obtain legal assistance. Miners or hackers can steal funds from digital wallets without an easy mechanism to get the assets back.

Some exchanges or e-wallet services offer password or account recovery solutions, but they are limited and not always effective.

c. Issues of privacy and information security

Blockchain provides a high level of security thanks to encryption and decentralization, but protecting privacy remains a challenge. Transactions on the blockchain, although protected by complex encryption, cannot be tracked and analyzed without the use of additional protections such as coin mixers or dedicated privacy blockchains. like Monero and Zcash.

In addition, the management and protection of users' personal data on blockchain platforms is still not clearly regulated, especially when blockchain is an immutable technology and permanently stores data. Storing sensitive data on blockchain without proper security mechanisms can create the risk of information leakage and violation of user privacy.

5.1.3.3. The future of legality and user protection in Blockchain

To address legal challenges and protect users, countries and international organizations need to cooperate to develop clear and appropriate legal frameworks for blockchain technology. This could include developing global standards for consumer protection, strengthening security and privacy regulations, and developing mechanisms to protect users in the event of an incident. problem.

5.1.4. Social challenges and acceptance

5.1.4.1. Cognitive barriers

Although blockchain technology has great potential in many fields, there are still some cognitive barriers that organizations and users need to overcome. Here are important issues related to social perception of blockchain:

1. **Lack of understanding of blockchain technology**: One of the biggest barriers to blockchain adoption is a general lack of understanding of the technology. Many people and businesses still do not fully understand how blockchain works, as well as its potential applications. The lack of information and education about blockchain prevents many people from experimenting or investing in this technology, even though it can bring many benefits.
2. **Concerns about security and reliability**: While blockchain can provide high security, vulnerabilities in software, cyber-attacks, and improper use can raise security concerns. The community is still concerned about issues such as fraud, loss of funds, and hacks that have occurred in the past. This affects user trust in blockchain, especially in applications such as cryptocurrencies and smart contracts.
3. **Habit of using traditional systems**: Consumers and institutions are accustomed to traditional financial systems and legacy business models. Moving to new decentralized systems requires time and a change in mindset. This change is not only technically difficult but also challenges long-standing habits in the use of financial services, payments, and data management.

5.1.4.2. Implementation costs

Although blockchain brings many benefits, implementing and applying this technology also encounters cost issues, especially for small and medium-sized businesses.

1. **High initial investment costs**: To deploy blockchain, businesses face huge initial investment costs. This includes building infrastructure, recruiting specialized human resources, and developing blockchain applications. These costs can make blockchain implementation difficult for businesses with limited resources.
2. **Lack of professional human resources**: Blockchain is a new technology, and finding human resources with blockchain expertise is still a big problem today. Blockchain engineers and experts in this field are rare and expensive, making it difficult for businesses to deploy blockchain solutions. Besides, employee training also faces a big challenge because in-depth knowledge about blockchain is not commonly taught in universities.
3. **Operation and maintenance costs**: After implementation, businesses still have to face operating and maintenance costs. Blockchain platforms require system maintenance, software upgrades, and continuous security monitoring. Especially for large applications, this cost can become a long-term burden.

5.2. Blockchain 3.0: New Breakthroughs in Blockchain Technology

Blockchain 3.0 represents the evolution of blockchain technology, solving the limitations and problems that existed in previous versions (Blockchain 1.0 and 2.0). It focuses on factors such as performance, scalability, security, and especially sustainability. Three prominent elements in Blockchain 3.0 are: **Green Blockchain**, **Zero-Knowledge Proof (ZKP)**, and **Layer 2 and Rollups**.

1. Green Blockchain

One of the big problems of current blockchain platforms is high energy consumption, especially networks that use Proof of Work (PoW) consensus mechanism, like Bitcoin. While Blockchain 2.0 (Ethereum) is moving towards Proof of Stake (PoS) to reduce energy consumption, Blockchain 3.0 continues to go further with the concept **Green Blockchain**.

- **Green Blockchain** are blockchain systems designed to minimize environmental impact. These platforms use energy-efficient consensus mechanisms, such as PoS, or

other alternative technologies to help reduce the amount of energy needed to operate the network.

- A typical example is **Algorand**, a blockchain platform that uses PoS and is committed to maintaining an extremely low carbon footprint. This helps green blockchains not only scale and perform transactions quickly, but also minimize negative impacts on the environment.
- **Cardano goes Tezos** are also examples of platforms that focus on sustainability and energy efficiency while maintaining security and scalability features.

2. Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) is one of the key technologies in Blockchain 3.0 that helps enhance user security and privacy without revealing sensitive data. ZKP is a technique in which one party (the prover) can prove to another party (the verifier) that a statement is true without revealing any information other than the correctness of the statement. there.

Suppose Peggy needs to prove to Victor that she is in possession of a secret without revealing it. Can she do so in a way that convinces Victor that she really knows the secret? This is the question that lies at the heart of one of the most powerful cryptographic processes we can use in identification systems: zero-knowledge proofs (ZKP). Suppose for example that Peggy has a digital driver's license and wants to prove to Victor, the barman, that she is over 21 without showing her driver's license or even needing it. Show him her date of birth. ZKPs allow Peggy to prove that her driver's license states that she is at least 21 years old without disclosing any other information (i.e., without redundant knowledge).

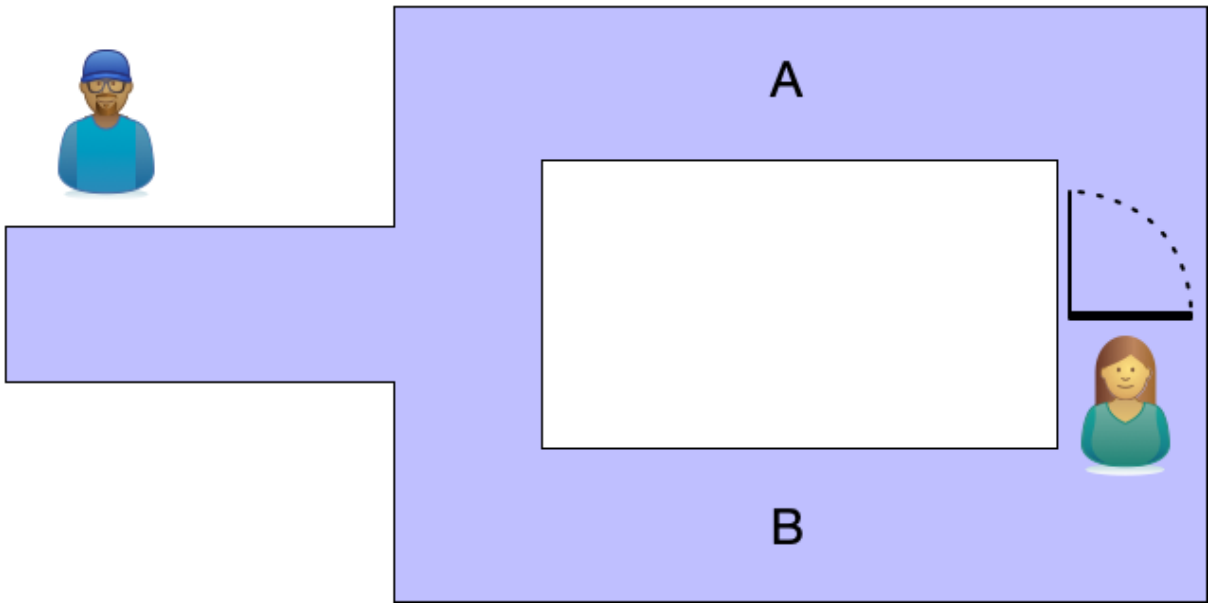
This problem was first discovered by MIT researchers Shafi Goldwasser, Silvio Micali, and Charles Rackoff in the 1980s as a way to combat information leaks. The goal is to reduce the amount of redundant information that the verifier, Victor, can know about the prover, Peggy.

One way to understand how ZKP works is the story of the Alibaba Caves, first published by cryptographers Quisquater, Guillou, and Berson. The following diagram provides an illustration.

Peggy and Victor in “Alibaba Cave”

Alibaba Cave has two passages, marked A and B, branching off from a single hallway connecting to the entrance. Peggy possesses a secret code that allows her to unlock a door

connecting A and B. Victor wants to buy the code but will not pay until he is sure that Peggy knows the code. Peggy won't share it with Victor until he pays.



The algorithm for Peggy to prove that she knows the code proceeds as follows:

1. Victor stands outside the cave while Peggy enters and chooses one of the passages. Victor is not allowed to see which path Peggy chooses.
2. Victor enters the cave and calls out "A" or "B" at random.
3. Peggy appeared from the right entrance because she could easily open the door no matter which entrance she chose to enter.
4. Of course, Peggy might just guess right and get lucky, so Peggy and Victor will try the experiment over and over again.
5. If Peggy can always return from the path Victor takes, then the probability that Peggy actually knows the code increases. After 20 tries, there was less than a one-in-a-million chance that Peggy would simply guess the correct word that Victor would say. This is a proof of probability that Peggy knows the secret.

This algorithm not only allows Peggy to convince Victor that she knows the code, but does so in a way that ensures Victor cannot convince anyone else that Peggy knows the code. Suppose Victor records the entire transaction. The only thing the observer sees is Victor calling out the letters and Peggy appearing from the correct tunnel. The observer cannot be sure that Victor and Peggy have not agreed upon a string of letters in advance to deceive the observer. Note that this property depends on the algorithm using a good pseudorandom

number generator with a highly random seed so that Peggy and the third observer cannot predict Victor's choices.

Thus, while Peggy cannot deny to Victor that she knows the secret, she can deny that she knows the secret to other third parties. This ensures that whatever she proves to Victor will remain just between them, and Victor cannot reveal it - at least in a way that cryptographically proves that it came from Peggy. Peggy retains control over both her secret and her knowledge of that secret.

When we say "no knowledge" and talk about Victor learning nothing beyond the statement being tested, that's not entirely accurate. In Alibaba's cave, Peggy proves without her knowledge that she knows the secret. But there are so many other things that Victor learns about Peggy that ZKP can't do anything about. For example, Victor knows that Peggy can hear him, speak the same language, walk, and cooperate. He can also learn things about the cave, like how long it takes to open the door. Peggy learns similar things about Victor. So the evidence is in fact near-absence of knowledge rather than complete absence of knowledge.

ZKP system

The Alibaba Caves example is a very specific application of ZKPs, called zero-knowledge proof of knowledge. Peggy is proving that she knows (or possesses something). All in all, Peggy may want to prove many truths to Victor. These truths can include propositions or even values. ZKP can do this.

To understand how we can prove propositions in zero knowledge, let's look at another example, sometimes called the Socialist Millionaire Problem. Suppose Peggy and Victor want to know if they are paid fairly. Specifically, they want to know whether they are paid the same salary, but do not want to reveal their specific salaries to each other or even to a trusted third party. In this case, Peggy doesn't prove she knows a secret, but she proves a proposition about equality (or inequality).

For simplicity, let's say Peggy and Victor are paid one of $10, $20, $30, or $40 per hour. The algorithm works as follows:

1. Peggy buys four lock boxes and labels them $10, $20, $30, and $40.
2. She threw away the keys to every box except the one labeled her salary.

3. Peggy gives all the lock boxes to Victor, who secretly puts a piece of paper with a "+" sign in the slot on the box with his salary. He will put a piece of paper with a "-" mark in all the remaining boxes.
4. Victor returns the boxes to Peggy, who uses her key to open the box containing her salary.
5. If she finds a "+" sign, it means they have the same salary. Otherwise, they have different salaries. She can use this to prove the truth to Victor.

This is called unknown transfer and proves the proposition "VictorSalary = PeggySalary" to be true or false in the absence of knowledge (i.e., without revealing any other information).

For this to work, Peggy and Victor must trust each other to be transparent and declare their true salaries. Victor needs to believe that Peggy will throw away the remaining three keys. Peggy has to trust that Victor will just put a piece of paper with a "+" sign in the boxes.

Just as digital certificates require a PKI system to build trust beyond what is possible with self-issued certificates alone, ZKPs are more powerful in a system that allows Peggy and Victor to establish facts from what others say about them, not just from what they say about themselves. For example, instead of Peggy and Victor asserting their own salaries, suppose they could rely on a signed document from HR to make the assertion, so they both know that the other is declaring your real salary. **Verifiable Credentials** provides a system for using ZKPs to demonstrate various facts, individually or in combination, in a way that creates confidence in the method and confidence in the data.

Non-Interactive ZKPs

In the previous examples, Peggy was able to demonstrate things to Victor through a series of interactions. For ZKP to be practical, interactions between provers and verifiers should be minimized. Fortunately, a technique called SNARK allows for non-interactive zero-knowledge proofs.

SNARKs have the following characteristics (from which their name is derived):

- **Brief**: the size of the messages is small compared to the length of the actual proof.
- **No interaction**: aside from some initial setup, the prover only sends a single message to the verifier.

- **Argument**: this is really an argument that something is true, not a proof as we understand it mathematically. Specifically, the theory prover can prove false statements if given enough computing power. So SNARKs are "computationally certain" instead of "absolutely certain".
- **Knowledge**: the person who proves knows the truth in question.

Typically, you will see "zk" (an acronym for zero-knowledge) added in front to indicate that during this process, the verifier learns nothing beyond the proven facts.

The basic mathematics of zkSNARKs involves homomorphic computation on higher-order polynomials. However, we can understand how zkSNARKs work without knowing the underlying mathematics that ensures they are certain. If you want to learn more details about mathematics, I recommend "zkSNARKs in a Nutshell" by Christian Reitwiessner.

As a simple example, suppose Victor is provided with a sha256 hash, H, of some value. Peggy wants to prove that she knows a value s such that sha256(s) == H without revealing s to Victor. We can define a C function that describes this relationship:

C(x, w) = (sha256(w) == x)

So C(H, s) == true, while other values for w will return false.

Computing a zkSNARK requires three functions G, P, and V. G is a key generation function that takes as input a secret parameter called lambda and a function C, and generates two public keys, the proof key pk and the confirmation key. Minh vk. They only need to be created once for a given C function. The lambda parameter must be destroyed after this step because it is no longer needed and anyone who has it can create false proofs.

The proof function P takes as input a proof key pk, a public value x, and a (secret) proof w. The result of executing P(pk,x,w) is a proof, prf, that the prover knows a value w that satisfies C.

The verification function V calculates V(vk, x, prf), and the result is true if prf is proved true and false otherwise.

Returning to Peggy and Victor, Victor chooses a function C that represents what he wants Peggy to prove, generates a random number lambda, and runs G to generate the proof key and verification key:

(pk, vk) = G(C, lambda)

Peggy is not allowed to know the value of the lambda. Victor shares C, pk and vk with Peggy.

Peggy wants to prove she knows the value s satisfying C for x = H. She runs the proof function P using these values as input:

prf = P(pk, H, s)

Peggy gives the prf proof to Victor, who runs the verification function:

V(vk, H, prf)

If the result is true, Victor can be assured that Peggy knows the value s.

The C function need not be limited to just one hash as in this example. Within the limits of basic mathematics, C can be very complex and involve any number of values that Victor wants Peggy to prove, all in one go.

ZKP application in blockchain helps protect user privacy, as transaction information does not need to be made public but still ensures that the transaction is valid. This can help solve security and privacy issues on public blockchain networks like Ethereum.

- **Zcash** is an example of a cryptocurrency that uses ZKP. It allows users to make transactions without revealing the amount or recipient, thereby protecting their privacy.
- **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) is a specific form of ZKP, which has been applied on Ethereum to improve security and optimize the performance of smart contracts.

3. Layer 2 and Rollups

In the context of Blockchain 3.0, **Layer 2** and **Rollups** are solutions that enhance the scalability and performance of blockchains, especially Ethereum, without sacrificing security or decentralization.

Layer 2

Layer 2 (L2) is a solution that improves the scalability and performance of blockchain networks without sacrificing security or decentralization. To better understand Layer 2, imagine blockchain like a traffic road, where all transactions must move through the main road (Layer 1). If this road is too crowded, transactions will be very slow and expensive. Layer 2 is like building additional side roads, helping transactions move faster without clogging the main road.

How does Layer 2 work?

Layer 2 works by processing transactions off the main chain (Layer 1) and only sending important data or the results of that transaction to the main blockchain. This reduces the load on Layer 1, increases transaction speed and reduces transaction costs without having to record every transaction to the main blockchain.

There are two common types of Layer 2 solutions:

1. **State Channels**:
    - Is a communication channel between two parties (or more parties) whose transactions take place outside of the main blockchain. Once the transactions are complete, the final results are recorded on the main blockchain.
    - For example: Suppose you and I want to exchange money over a long period of time. Instead of writing to the blockchain each time (which takes time and cost), we can transact off-chain through a state channel and only write the final result to the blockchain.
2. **Rollups**:
    - Rollups work by transferring transactions and calculations outside the main blockchain (Layer 1), but these results are still verified and recognized on the main blockchain. This helps reduce congestion and transaction costs of the main blockchain, while still ensuring security and decentralization. Transactions are performed on Layer 2 and then "rolled" into a single transaction or group of transactions for recording on the main blockchain. As a result, only aggregate data of transactions is stored on the main blockchain, without the need to store all detailed transactions. There are two main types of Rollups:
        - **Optimistic Rollups**: It is assumed that transactions are valid and not immediately checked, but may require proof if there is doubt about the validity of the transaction.
        - **zk-Rollups**: Uses Zero-Knowledge Proof (ZKP) technology to verify the accuracy of transactions without having to reveal the entire transaction data, enhancing security and performance.

Benefits of Layer 2

- **Speed up transactions**: Layer 2 makes transactions faster because it reduces congestion on the main blockchain.
- **Reduce costs**: By processing transactions off-chain, transaction costs are significantly reduced compared to having to do it all on the main blockchain.
- **Scale expansion**: Layer 2 solutions make it possible for blockchain to process more transactions without encountering congestion or high costs.

Layer 2 example

- **Lightning Network** on Bitcoin is a prominent example of Layer 2. It allows users to make transactions faster and cheaper without having to write them all to the main Bitcoin blockchain.
- **Optimism and Decision** on Ethereum are two Layer 2 solutions that are helping Ethereum solve the problem of congestion and high transaction costs.

Layer 2 is an important technology that makes blockchain scalable and handles more transactions without sacrificing security or decentralization. Solutions like State Channels and Rollups will help improve blockchain performance and reduce transaction costs, creating a more robust and efficient blockchain ecosystem in the future.

Thus, developing solutions for the 3.0 generation Blockchain network and beyond is not simply about technological improvements but also focuses on important factors such as security, performance, and capacity. expansion and sustainability. New technologies such as Green Blockchain, Zero-Knowledge Proofs and Layer 2, Rollups are factors that help blockchain solve existing problems in previous versions, while also opening up many opportunities for blockchain application. in many different fields in the future.

5.3. Summary

Blockchain is a technology full of potential but is facing many complex challenges. Solving these challenges requires the efforts of the entire blockchain community, from developers to businesses to regulators. Technological developments and new solutions are gradually addressing these challenges, opening up prospects for broader blockchain adoption in the future.

Review questions

1. Analyze key blockchain scalability challenges and propose solutions.

2. Why is energy consumption such a big challenge for blockchain? What solutions are being developed to solve this problem?
3. Compare technical and administrative challenges in implementing blockchain.
4. Discuss the role of the legal framework in the development and application of blockchain technology.
5. Assess the impact of societal challenges on the widespread acceptance and adoption of blockchain technology.

References

1. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain
2. Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey
3. Swan, M. (2015). Blockchain: Blueprint for a New Economy
4. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution
5. https://www.windley.com/archives/2021/11/zero_knowledge_proofs.shtml?form=MG0AV3