第一页

The topic of my speech is “The meaning of blockchain and China’s development in blockchain”

第二页

First of all, I want to introduce the content of this speech to you. I decided to divide it into four parts. The first part is to tell you the definition of blockchain. The second part is to tell you what the consensus mechanism is and its importance. In the third part, I want to study the dangers and risks of blockchain with you. Finally, I want to introduce the existing blockchain innovation and technology in China.

第三页

Let’s get into the first part, what is blockchain?

第四页

I don’t want to talk about any complicated concepts. I want to tell you what blockchain is by telling you a very simple story.

Imagine you are living in a village now. There is no physical currency in this village, and all transactions are completed by everyone's accounting.

One day, A spent 10 dollars to buy some books from B

第五页

A and B used the radio to tell everyone: A's account will be reduced by 10 dollars, and B's account will be increased by 10 dollars.

第六页

At this time, everyone will take out their account books and write down this transaction information. Later, everyone discovered that it was very difficult to keep accounts at all times, and most of the accounts had nothing to do with them, so at this time everyone made a decision

第七页

They decided to make the village chief the bookkeeper, and all transactions would be recorded by the village chief. The village chief will clean up today's accounts every afternoon and publish the accounts so that everyone can check if there are any problems. If everyone thinks there is no problem, they will take out their own paper and pen, take a copy home, write down today's date and keep it. In this case, everyone is saved from the trouble of keeping accounts all the time.

第八页

In this case, a ledger will appear in this village every day, such as January 1st, January 2nd, and January 3rd. Because these ledgers exist independently, we can regard each ledger as a block, such as block 1, block 2, and block 3. This is how the blocks are generated.

A block can be simply understood as multiple accounts

第九页

The purpose of the chain is to connect two adjacent ledgers.

第十页

After the village chief published the account book every day, there was an ending balance. We can see that A has 125 dollars left at the end.

第十一页

When the accounting begins the next day, the village chief will write down yesterday's balance at the beginning of the account as the opening balance. Today's transactions will be based on yesterday's balance

Because the balance at the end of yesterday is the same as the balance at the beginning of today, we can simply understand that yesterday's ledger and today's ledger are linked through balance carryover. And this chain is the chain in the blockchain

第十二页

But at this time a problem arose. The village chief has been keeping accounts, so how does the village chief’s income come from? If there is no income, no one will keep accounts.

第十三页

So everyone agreed that every time a transaction was completed, the village chief would be given a sum of money as a reward. And these money are also transaction fees.

第十四页

At this time, another problem arose. When A saw that the village chief’s income was so high, he thought it was unfair and wanted to keep accounts.

第十五页

Soon everyone discovered that the village chief's salary was very high, so they all wanted to keep accounts. After some discussion, they decided to create a system for selection. This is the selection mechanism.

第十六页

Now that we're on the topic of mechanism, let's get into the second part, "Mechanism."

第十七页

The consensus mechanism is of great significance, and he ensured that nodes in the network can agree on a set of transactions without a central authority

第十八页

And it has many characteristics, such as Improve efficiency

safety

Simplify operations

ensure consistency

第十九页

When the consensus mechanism is discussed, it is necessary to discuss the Byzantine problem. As we all know, Byzantium was a very large country, so soldiers were often far away, and they could only convey news by writing letters. One day a war breaks out, and in order to win, the generals must reach a consensus and decide whether to attack the enemy.

In this case, it is known that a traitor may appear. How do we correctly convey information when we know that there is a traitor?

第二十页

At this time we can use PBFT (Practical Byzantine Fault Tolerance). Its principle is to use a large number of communications to obtain reliability.

第二十一页

Let me give you an example. For example, there are four generals ABCD, because we know that if there are two traitors, there is no solution. So we set up as a traitor. If A is a traitor, then BCD will receive three different times. At this time, they will know that A is a traitor.

第二十二页

If B is a traitor, then C and D will receive two identical times and one different time. At this time, the information with the largest amount is correct information, so b is the traitor.

At this time we can summarize a rule. If there are N invalid nodes, as long as the total number of nodes exceeds 3N, the correctness of the message can be guaranteed

第二十三页

When discussing blockchain, we have to mention Bitcoin. What is the consensus mechanism used by Bitcoin? , the answer is here, it uses proof of work. So how do we prove that the computer is hard working？

第二十四页

First, we take a binary number, and when it is hashed, we get the data on the right. At this time, we have reversed one of the binary numbers. At this time, the number we calculate through hashing will be completely different from the original number. He's as random as a die. At this time, people thought of a way. Since the hash value is so random, everyone should look for the last four digits of the hash value with 0. Whoever finds it first will get the reward.

第二十五页

So how do we find the desired hash value that ends with four zeros? This is very difficult. At this time, people thought that we only need to enter a number at the end of the binary to see if the output result is four zeros. If not, then we will modify the number. By constantly modifying this number, we finally found a number that ends with 4 zeros. And this number that we constantly modify is NONCE, and NONCE can reflect the real workload

The process of constantly searching for NONCE is also called "mining"

第二十六页

When we find NONCE, we organize the transaction data into blocks. And here is a coinbase, which is a reward for mining machines.

At this time, the new block is still in the mining machine, and the mining machine will send this block and NONCE to other nodes.

第二十七页

Other nodes will verify this information. If the result is four 0s, then the verification passes. It shows that this mining machine is working effectively, so the block is added to the blockchain of this node.

Therefore, the reward of this mining machine is recognized by this node. In the same way, all nodes will recognize the rewards of the mining machine

第二十八页

However, nothing is absolutely safe, and blockchain also has its potential dangers. Let's move on to the third part.

第二十九页

Students who know Bitcoin should have heard of the 51% attack, but what does it mean?

There is a description in the Bitcoin white paper that if honest nodes are larger than malicious nodes, then it is safe. Otherwise, there is a possibility of being attacked. We can know that if a malicious node controls more than 50% of the computing power to launch an attack, it is a 51% attack.

第三十页

If one person owns more than 51% of the computing power of the entire network, he will be able to perform operations such as double spending, reversing transactions, etc., thereby spending a sum of money twice, so this is also called a double-spending attack.

Suppose A wants to conduct a 10-bitcoin transaction with B. The first transaction is packaged in block 100. After five more blocks are added later, A initiates another 10-bitcoin transaction to himself.

He decided to fork the main chain, generate another block 100, and package another transaction in it. At this time, two main chains are generated, others work on the original chain, and A works on the newly forked chain. Since A has more than 51% of the computing power, the length of the new chain will soon exceed the old chain. This is based on the principle of longest chain first. Others will also work on the new chain, making the new chain the main chain, and the old chain will be abandoned. In this way, A can get the resources belonging to B without spending any money.

第三十一页

1. Lack of third party protection(for example banks)

If a dispute occurs, there is no way to mediate the dispute

2. Lack of privacy

The transaction is fully public

3. Fraud risk

Such as Internet fraud

4. Legal Risk

May not be legal in some areas

5. Risk of key loss

If the key is lost, then we will have no way to access our account again

第三十二页

In the last part, I would like to introduce to you some existing blockchain applications in China.

第三十三页

From this document we know that blockchain technology has been used in some important areas in China

第三十四页

第三十五页

第三十六页

The above is the entire content of my speech. Thank you everyone for listening.