Introduction to Cryptography 03/27/2018

Lecture 17: Bitcoin I

Instructor: Vipul Goyal *Scribe: Yimin Yang*

1 History of Bitcoin

Bitcoin is the first truly decentralized cryptocurrency. In 2008, Satoshi Nakamoto published the paper *Bitcoin: A Peer-to-Peer Electronic Cash System*. In January 2009, Nakamoto released the first bitcoin software, and the mining formally started. On 22nd May 2010, Laszlo Hanyecz made the first real-world Bitcoin transaction by buying two pizzas for 10,000 BTC. Now Bitcoin is getting more and more popular, and people also begin to pay attention to the underlying blockchain technology.

2 Bitcoin Mining

Bitcoin and other cryptocurrencies are just like a public ledger. There is no centralized authority. People can write data to the public ledger, and the ledger is append-only. The "block" is just like a page of the ledger. People add one page at a time, or one block at a time. "Mining" is the process of adding the next block.

To start the mining process, the first step is to choose a genesis block B_0. The genesis block is designed by the designer of the cryptocurrency.

For Bitcoin, the genesis block is: B_0 = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

2.1 One miner

For simplicity, suppose there is only a single miner, and multiple users in the system. Users want to write information on the next page of the public ledger.

When the miner collects all the information, it starts to mine the next block. To mine the next block, it must solve a puzzle:

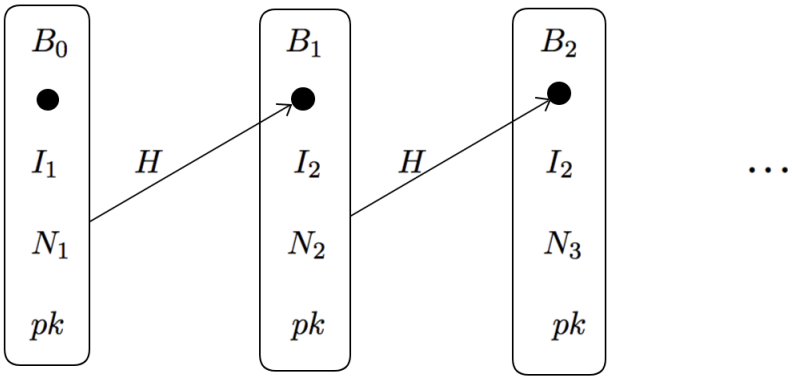
Puzzle to mine block B_{i+1}: $H(B_i, information, nonce, pk) = \underbrace{0000...0}_{\text{(k-zeros)}}XXXX...X$.

- H is a hash function
- B_i: the i-th block
- information: the information users want to write
- nonce: very long random string set by the miner so that the hash will contain a run of leading zeros
- pk: public key of the miner

The miner need to try a large number of nonces to get "acceptable" hash output for nonce R:

$$H(B_i, information, R, pk) = B_{i+1}$$

Then the miner mines the next block. The process goes on.



When we want to read data from the first page, we must hash the first page, and check if the result matches the hash given by the second page. By doing this, we can authenticate every page of the ledger.

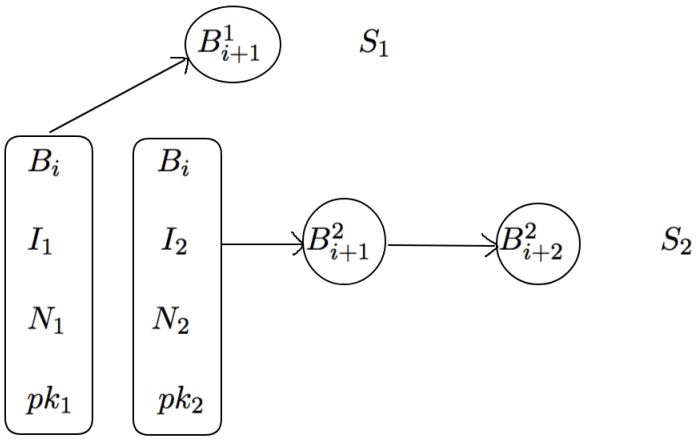
In Bitcoin network, one block will be mined roughly every 10 minutes. As more and more miners join the network, the computing power goes up. Then the system will automatically adjust the difficulty of the puzzle, to make one block be mined roughly every 10 minutes.

So why does the miner spend a lot of computing power to mine the block? Because it can get some new bitcoins as reward when a new block is mined. This process is just like real-world mining. These new bitcoins will automatically be associated with the public key of the miner. That is why we need the public key of the miner. And the reward keeps going down with time. The Bitcoin protocol specifies that the reward for adding a block will be halved approximately every four years. In 2140, the reward will diminish to zero.

2.2 Multiple miners

Suppose there are many miners trying to mine block B_{i+1}. They all have the puzzle about B_i, and some of them might solve the puzzle. So how do we choose which miner to write the next page? The strategy is: whoever solves the puzzle first mines the next block.

But there is the problem: since this is a decentralized network, if two miners solve the puzzle roughly at the same time, it is not clear for the network who is the first. At this time, we have two different versions of the public ledger: the public keys will be different, the nonces will be different, and the information that they want to write will be different. In particular, who gets the new bitcoins as reward will also be different. At this point, we have **fork** in the blockchain.



3 Bitcoin Fork

The miners follow two rules to resolve this conflict:

- Longest chain is the right chain
- First chain is the right chain

Suppose one chain is longer than the other chains. Even if the longer chain came later on, the miners will think it is the right one. If multiple chains have the same length, the chain which the miner sees the first is the right chain.

Now there is fork in the blockchain. Let S_1 and S_2 denote the two different sets of miners. Now they are all trying to mine the next block.

The miners in S_1 will try to solve this puzzle:

$$H(B^1_{i+1}, information, nonce, pk) = 0000...0XXXX...X.$$

The miners in S_2 will try to solve this puzzle:

$$H(B^2_{i+1}, information, nonce, pk) = 0000...0XXXX...X.$$

At some point, one of the miners will succeed in mining the next block. Suppose a miner in S_2 succeeded in mining the next block B^2_{i+2}. Then it broadcast the next block to everybody. Since S_1 has not progressed, S_2's chain is the longest chain. Now the conflict is solved.

So how about the reward? When miner 1 in S_1 mined B^1_{i+1} and miner 2 in S_2 mined B^2_{i+1} at the same time, there were two versions of the public ledger. One was saying that miner 1 got the reward, and the other was saying that miner 2 got the reward. It was a conflict, because both miners had the reward at this point. Then S_2's chain progressed, and everyone moved to this chain. So miner 1 got the reward in the first place, then the reward went away. In this way, the conflict is solved.

We just assume that the majority of the computing power belongs to honest guys. Suppose a malicious guy controls more than half of the computing power. In that case, more than half of the computing power of the network will work on the wrong chain. After some time, the wrong chain will be longer than the right chain, and the malicious guy will get the reward.

4 Infanticide

People who have a large amount of Bitcoins do not want other cryptocurrencies to survive. They want people just to use Bitcoins. For a new cryptocurrency, at the beginning there are only a small number of miners. And some Bitcoin miners start to mine the new cryptocurrency to destroy it. Since they have much larger computing power than the miners of the new cryptocurrency, they will make one chain longer, then make another chain longer. Then everyone will lose confidence in this new cryptocurrency. This is called infanticide.

5 Cryptocurrency Application

To build cryptocurrency application, we just write all the transactions to the public ledger. When a new block is mined, the public key of the miner gets some bitcoins. There is a particular state in the system:

- pk_1: has k_1 bitcoins
- pk_2: has k_2 bitcoins
- ...

We can scan the ledger to find how many bitcoins a public key has. And bitcoins are transferred from one public key to another public key by using digital signatures.

For example, pk_1 wants to transfer 1 bitcoin to pk_2. It just needs to sign a statement:

$Sign_{sk_1}$ ("pk_1 transfers 1 bitcoin to pk_2 AND pk_1 transfers 0.1 bitcoin to miner")

and broadcast it to the network.

The miner will append the information as a part of the block. Before input the information, the miner should make sure this is a valid transaction. For this example, it should check the following:

- pk_1 had 1.1 or more bitcoins
- signature is valid

If the transaction is valid, the miner appends the transaction to the information which it is currently working with, and tires to mine the next block. Once the next block is mined, the transaction appears on the next page, and the miner gets the transaction fee. If the transaction fee is too low, some miners will ignore the transaction, and the transaction might need to wait a long time.

The signature ensures that no one else can spend your money; you cannot spend the money you do not have; you cannot double spend your money. But if you lost your secret key, you will lose the money, and your bitcoins will be "dead".