ECE 595: Foundations of Blockchain Systems **October 7th, 2020**

Lecture 3

Lecturer: Sreeram Kannan *Scribe: Ivan Iturriaga*

In this lecture we will review the structure of a block, one important property of the Blockchain and proceed into our discussion on the double-spend attack and ways to counter it. We will conclude these lecture notes with a general discussion on the proof-of-work system.

3.1 Anatomy of a Block

We begin by first examining the mining process and to do that, we must specifically look at the anatomy of a new block being added to the chain. That new block includes the following:

- Hash of the previous block (hash pointer)
- New transactions
- Hash of the two items above and a nonce, which is a random string that is less than the threshold (since you have to try x many times before you find this string, this is also your proof-of-work)

Once it has all those elements, the block can then be floated to the network.

3.2 Immutability

One property of the blockchain is immutability. This means that the chain cannot be changed given the last block in the chain. This is because it is difficult to find a hash of x that is equal to hash of y in computationally feasible time (collision-resistance). We add the qualifier "given the last block" because if we disagree on which is the last block, we may have problems. With distributed mining, there is a possibility of simultaneous mining, however these ties should be resolved quickly with proper tuning of parameters. Therefore, although we may not agree on the last block all of the time, all blocks will lead back to the genesis, starting block, and the large majority of the chain will be in agreement.

3.3 Double-Spend Attacks

Nevertheless on the ends of the blockchain, we are susceptible to something called the double-spend attack. To accomplish this attack, a user would have to do the following:

1. Spend money in a certain transaction (ex. user pays Honda dealership 2 Bitcoins for a new car)
2. Privately mine blocks from the block preceding the transaction so that they now have the longest chain (this can be done in advance, as long as you have the longest chain in the end)
3. Spend the bitcoin that they had promised in the original transaction by paying themselves or a friend (ex: using the 2 Bitcoins from Honda to pay yourself)

4. Release the privately mined blocks so that users switch from the original chain to your new longer chain

The reason that this works is that all transactions from the original chain are appended to your newly created chain, but since you spent the money that you had promised, the original transaction is invalidated. We are able to add multiple blocks to the system at one time because this is something that actually happens in blockchain systems. Firstly, from the perspective of users, transactions can be made online or offline, this feature makes the system robust to dynamically entering users. Secondly, from the network perspective, transactions can be made synchronously or asynchronously, which makes the system robust against system failures (power outages, etc.) and latency.

3.4 K-Deep Confirmation

To counter the double-spend attack, we, the users of Bitcoin, can use a k-deep confirmation policy. With this policy, users can be "sure" that their transaction and the entire block will remain in the blockchain once k number of blocks are produced after your block of interest. This means that users receiving money from a transaction will only consider the transaction confirmed once there are k blocks following their block.

3.4.1 Latency vs. Reliability

There is a tradeoff between latency and reliability. Specifically this means that if you want to confirm your transaction with higher certainty (larger value of k) you will have to wait a longer time for those blocks to be mined (larger latency). K is NOT a system parameter, k is a private, transaction specific parameter. This means that your Honda dealer may be very particular (want a high k value) because there is a lot of money involved, however a restaurant may be less particular about you paying for your meal (require a lower k value) because it is a relatively small amount.

3.4.2 Interarrival Process

The interarrival between blocks being added to the chain is a random poisson exponential process. The interarrival time for blocks is 1/lambda. Lambda is proportional to mining power. Therefore if a competing adversarial chain wanted to take over the network, they would need a larger lambda than the lambda of the rest of the miners put together (in the long run). Therefore, we can confirm blocks with high reliability after we get k deep depending on the mining power of adversaries in the system.

3.4.3 Choosing a Value of k

One important design choice in Bitcoin is that a block B is valid on a chain C if all the transactions within B are valid. All transactions are valid within B if for each transaction the customer has the money to pay that transaction according to the ledgers accounting up to that point (ex: S cannot pay 1 Bitcoin to R if S does not have 1 Bitcoin from prior transactions). The idea of k-deep confirmation makes Bitcoin a probabilistic confirmation system as opposed to a deterministic one. Satoshi Nakamoto, the creator of Bitcoin, made tables listing the probability that a block will remain in the chain at different values of k for different percentages of adversarial computational

power (denoted by the greek letter Beta and calculated by dividing the adversarial computational power by all of the computational power in the system).

3.5 A Closer Look at Proof-of-Work in Bitcoin

The proof-of-work system has led to just a few blockchain organizations being able to dominate the market. This happens because if there were a small developing blockchain, people with high computational power could move over to this blockchain and completely take over the network (own more than half of the network). Here are some of the pros and cons of proof-of-work systems:

Pros of POW systems:

- Sybill attacks are impossible because no node with small computational power can take over the network.
- There is no need to manage identity, anyone can join the network.

Cons of POW systems:

- There is a large wastage of power.
- only one (or very few) large proof-of-work blockchains can exist.

One radical method to counter being taken over by miners from a larger proof-of-work network is to make a specific puzzle which cannot be easily solved by the highly specific hardware used on the larger networks. This can be counterproductive because it creates a barrier to entry for the blockchain which goes against one of the core principles of blockchain that anyone can join the network.