Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

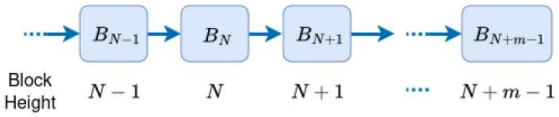
Week - 11

Lecture - 66

The Bitcoin Cryptocurrency: Part 6

Hello, in this lecture, we will continue our discussion of the Bitcoin cryptocurrency. We discussed blockchain integrity, that is, how difficult it is for some malicious entity to modify a block in the blockchain. In particular, suppose Alice wants to modify an existing block B_N, which is at height N in the blockchain, as shown in this picture and it has received m confirmations. That is, again shown in this picture. Notice that there are m-1 blocks added after the block B_N.

- Suppose Alice wants to modify an existing block B_N, which:
  - is at height N in blockchain
  - has received m confirmations
- E.g., Alice may want to delete a transaction from B_N
- Let B'_N be the modified block



By definition, the block B_N has received m confirmations. We discussed in a previous lecture that the typical value of m is 6. After m=6, the transfer of the goods from the seller to the buyer takes place. But in this case, m may not be 6, m may be anything, so the block B_N has received m confirmations. This does not have to do with transfer of goods, but there is just a certain block B_N which has received m confirmations.

Now, Alice wants to modify the block B_N. For example, Alice may want to delete a transaction from B_N. This transaction may say that Alice has transferred a certain number of bitcoins to someone else, say Bob, and if Alice manages to delete a transaction from B_N, then she can spend these bitcoins again. So, Alice may want to delete such a transaction,

which involves the expenditure of bitcoins from Alice from the block B_N. Let B_N' be the modified block.

So, Alice wants to replace the block B_N with the block B_N'. So, this is an instance where the integrity of the blockchain is compromised. Let's discuss how difficult it is. Recall that to replace B_N with B_N' in all the copies of the blockchain stored across the Bitcoin network, what must Alice do? Alice must create another branch of the blockchain which is longer than the existing branch of the blockchain.

So, Alice must create a branch containing B_N' that is longer than the branch containing B_N and broadcast it on the network. So, this is the block B_N, which Alice wants to replace, and there are some following blocks. Alice must create a branch containing the block B_N', which is the replacement for B_N, and this branch must be longer than the original branch. Only then will the other nodes replace their local copy of the blockchain with this branch containing B_N'. Once all the nodes in the Bitcoin network switch to the branch containing B_N', it will become the block at height N in the blockchain.

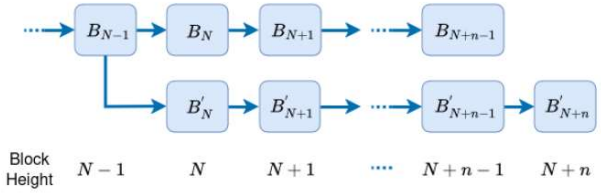
Then, this branch will be removed, and the blockchain will become this. However, assuming that Alice controls less than 50% of the network hash rate—recall that typically a single miner controls much less than 50% of the network hash rate. So, assuming that this is the case for Alice, the larger the value of m, the less likely it is that Alice is able to create a branch containing B_N' that is longer than the branch containing B_N. So, the more the number of confirmations that block B_N has received, the more difficult it is for Alice to create a longer branch. Because to create a branch that is longer than the existing one, Alice has to mine blocks faster than all the other miners in the network can collectively mine blocks.

So, given that Alice controls less than 50% of the network hash rate, it is unlikely that Alice alone will be able to mine blocks faster than all the other miners collectively can mine. Here's an example. It can be shown that assuming Alice controls a fraction of the network hash rate, which is less than 0.4, it is nearly impossible for her to tamper with blocks which have received 50 or more confirmations. So, the probability of tampering in this way is less than 1.05×10^{-9}. It is an extremely small probability.

So, this will be the typical case. A single miner will definitely control a fraction of the network hash rate which is less than 0.4. So, in this situation, once a block has received 50 or more confirmations, then the probability of being able to replace the block with another

block is less than about 10^{-9}. So, this shows the integrity of the blockchain. It's very difficult for someone to modify a block in the blockchain.

- To replace B_N with B'_N in all the copies of the blockchain stored across the Bitcoin network, Alice must:
  - ❑ create a branch containing B'_N which is longer than branch containing B_N and broadcast it
    - ○ once all the nodes in the Bitcoin network switch to the branch containing B'_N, it will become the block at height N in blockchain
- However, assuming that Alice controls less than 50% of the network hash rate:
  - ❑ the larger the value of m, the less likely it is that Alice is able to create a branch containing B'_N which is longer than branch containing B_N
- E.g.: assuming Alice controls a fraction of the network hash rate which is less than 0.4, it is nearly impossible for her (probability less than 1.05×10^{-9}) to tamper with blocks which have received 50 or more confirmations



Now, suppose a block contains a transaction where Bob transfers some bitcoins to Carol. And such a transaction will have an input which unlocks UTXO owned by Bob. We discussed UTXO in a previous lecture. And the transaction will have an output which creates a UTXO that can only be unlocked by the intended recipient, that is, Carol. Now, can Alice modify this transaction to make herself the recipient of Bitcoins instead of Carol?

So, this is another instance where the integrity of the blockchain is compromised. So, the claim is that it is difficult to modify this transaction in this way. The reason is that the response script that Bob uses to unlock his UTXO requires a digital signature, which can only be generated using Bob's private key, and only Bob knows his private key. The output of the transaction, which specifies Carol as the recipient, is part of the message that is used to generate this signature. If Alice replaces the output with an output which specifies herself as the recipient, then the message used to generate the signature changes, and Bob's private key is required to generate the new signature.

Alice does not have Bob's private key. Hence, Alice is not able to replace the output that specifies Carol as the recipient and replace it with herself as the recipient. If she makes this replacement, then she'll have to create a digital signature using Bob's private key. But Alice obviously does not have Bob's private key. Hence, she cannot make herself the recipient of the bitcoins instead of Carol. Now, we discuss a case where one miner has managed to gain more than 50% of the network hash rate. Such an attacker is called a 51%

attacker. An attacker who controls more than 50% of the network hash rate is called a 51% attacker in the Bitcoin literature.

Before this discussion, we noticed that for controlling more than 50% of the network hash rate, an attacker will have to have a huge amount of resources. Hence, it's difficult for one individual miner to control more than 50% of the network hash rate. In order to understand what happens in such a situation, let's assume that someone has managed to control more than 50% of the network hash rate. So, what can such an attacker do? A 51% attacker can, with probability 1, launch double spending attacks because we discussed how a double spending attack can be launched. The attacker needs to create a branch that is longer than the branch on which the other miners are working.

Since the attacker has more than 50% of the network hash rate, this attacker can mine blocks faster than all the other miners collectively can. Hence, the 51% attacker can with probability 1 launch double spending attacks. Eventually, the branch on which the attacker is working, that branch will become longer than the branch on which the other miners are working. The attacker can also delete transactions from old blocks. For example, if the attacker had paid some other parties and those transactions are stored in some old blocks, then the attacker can delete those transactions.

And this is irrespective of the number of confirmations received. Consider a block which has received, say, 1,000 confirmations, but still given sufficient amount of time, the attacker can create a branch that is longer than this branch. Hence, the attacker can launch these attacks on the blockchain. A 51% attacker can also launch other attacks which are more serious. Suppose a 51% attacker performs mining like a regular mining node, except that he or she does not switch to longer branches which are announced by the rest of the network.

So, for example, this attacker is mining blocks, so this is the blockchain initially. Now, one block is created by someone else, someone other than the attacker, but the attacker ignores that block and keeps on in parallel mining blocks by themselves. So, whenever some blocks are added by other parties, say this is added by some other party, the miner ignores that and creates their own branch. So in this way, it can happen that blocks are added only by the attacker. Since the branch mined by the attacker will eventually become the longest branch of the blockchain, all new Bitcoins generated as part of the block subsidy will be owned by only the attacker.

So, this will make mining financially unviable for the other miners in the network, and they may stop mining. Even if the other miners manage to generate a valid block, eventually that block will be replaced because the attacker will create a longer branch. So, in that case, mining will become financially unviable for the other miners, and they may stop mining. Then, the attacker will become the only miner in the network. The Bitcoin system will then resemble a centralized system that is controlled by the 51% attacker.

So, it will have several disadvantages of a centralized system, as we discuss next. So, the attacker can then harm the Bitcoin system as follows. The attacker can unilaterally decide which transactions get recorded on the blockchain. If the attacker has, for example, some parties whose blocks the attacker does not want to include, then the attacker can ignore those transactions by those other parties. So, the attacker can unilaterally decide which transactions get recorded on the blockchain.

For example, the attacker can censor transactions that transfer Bitcoins to a merchant by not including such transactions in new blocks. For example, if there is a merchant, say Bob, and the attacker does not want payments to be made to Bob, in that case, the attacker can ignore such transactions which transfer Bitcoins to Bob and not include those in new blocks. Another serious attack is what we discussed in a previous lecture: how the fee rate of transactions is set. But when a 51% attacker is present, the attacker can decide the minimum fee rate for transactions by not including those transactions that pay less than this minimum rate into new blocks. Recall that the 51% attacker is the only entity which adds new blocks to the blockchain.

So, if there are any transactions that pay less than the desired fee rate—the minimum fee rate set by the attacker—then the attacker will not include those transactions in the new blocks that he or she is adding. So, this will force all entities to pay a very high fee rate in all transactions. So, this way, the attacker can extract a lot of Bitcoins from other parties. A 51% attacker can cause the Bitcoin system to stop functioning as a payment system by mining only empty blocks. So, what are empty blocks?

Empty blocks are blocks that contain only the coinbase transaction and no regular transactions. So, in all new blocks, if no regular transactions are added, then clearly no one can pay Bitcoins to someone else. Hence, there is no point in using the Bitcoin system if this happens. So, without any new regular transactions appearing on the blockchain, the Bitcoin currency would be worthless. Hence, this would discourage others from using the system.

So, we have shown that the presence of a 51% attacker can lead to the collapse of the Bitcoin system. But such an event is highly unlikely. Because the cost—for example, acquiring mining equipment, electricity, cooling, and so on—involved in generating a majority of the network hash rate is prohibitive. A large number of parties in the world are involved in mining Bitcoins. So, for one party to have a hash rate that is more than 50% of the network hash rate is extremely difficult.

So, they would have to pay a huge cost to acquire the necessary mining equipment, electricity, cooling, and so on to generate a majority of the network hash rate. Another reason why this event is unlikely is that someone will not have any incentive to launch a 51% attack. The 51% attacker cannot hope to recover these costs by selling bitcoins because the attack itself will drive the price of bitcoins to zero. So, if no one wants to use bitcoins, then the price of bitcoins will go to zero. Even though the attacker mines blocks and gains the block subsidy in them and keeps on gaining bitcoins, the attacker cannot hope to recover these huge costs that have been invested because the attack itself will drive the price of bitcoins to zero.

So, these are the reasons why this event is unlikely. The first reason is the cost is huge, and the second reason is that there are no incentives to launch this attack because it will only result in a loss to the attacker. For these reasons, such an attack is unlikely. So, in summary, we discussed blockchain integrity. We discussed that modifying blocks or transactions in blocks is difficult.

Then, we discussed the 51% attacker and what harm such an attacker could cause to the Bitcoin system, and then we discussed why such an attack is unlikely. This concludes our discussion of the Bitcoin cryptocurrency. Our discussion has been brief. We omitted several topics. For example, smart contracts is one important topic that we did not get into.

If you are interested in learning more about the Bitcoin cryptocurrency and other blockchains, you can refer to the references. Thank you.