SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 6:

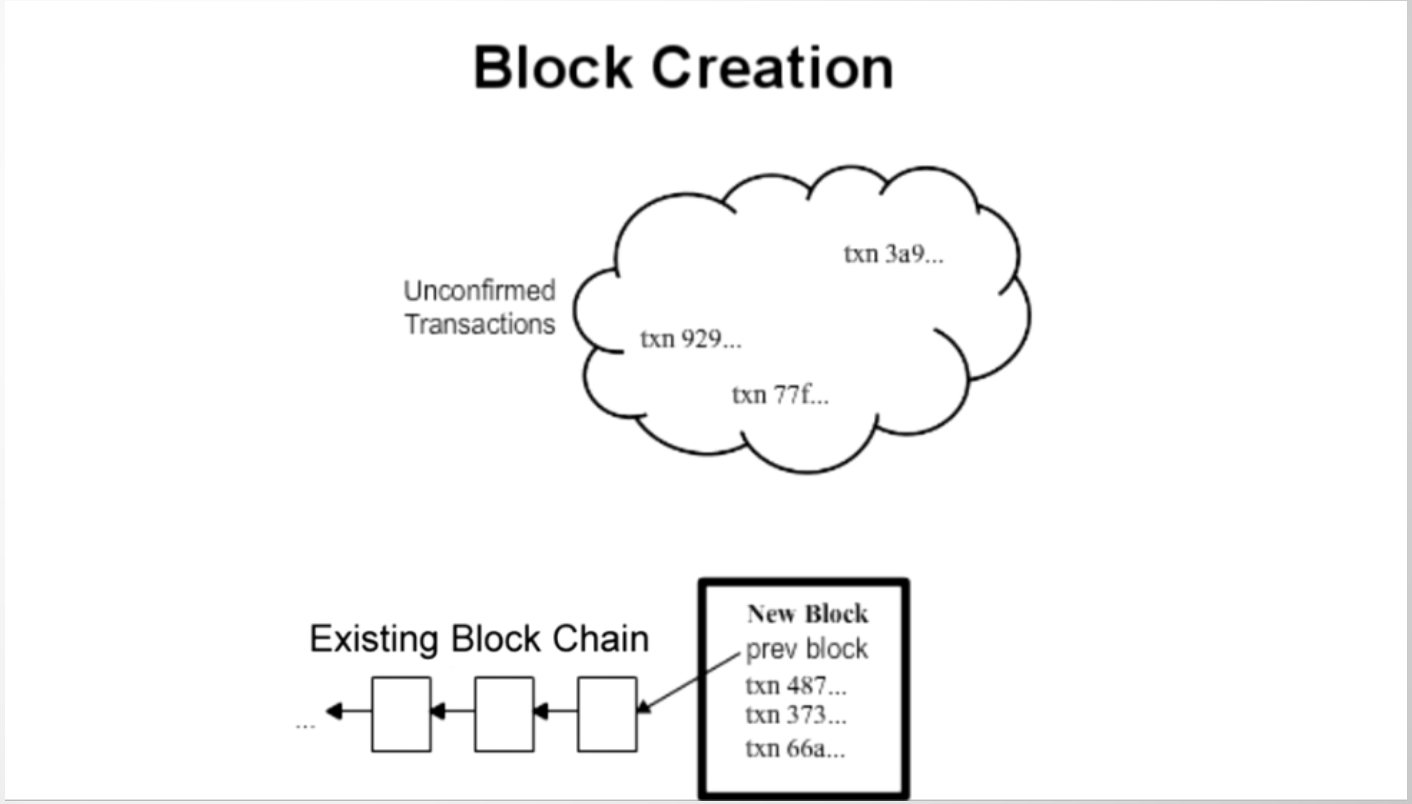
Bitcoin – Part 1

Module 2 – Double Spending Problem & Consensus Mechanism

How to make a block?

A block is made of a set of transactions happened in the same time slot (around 10 mins).

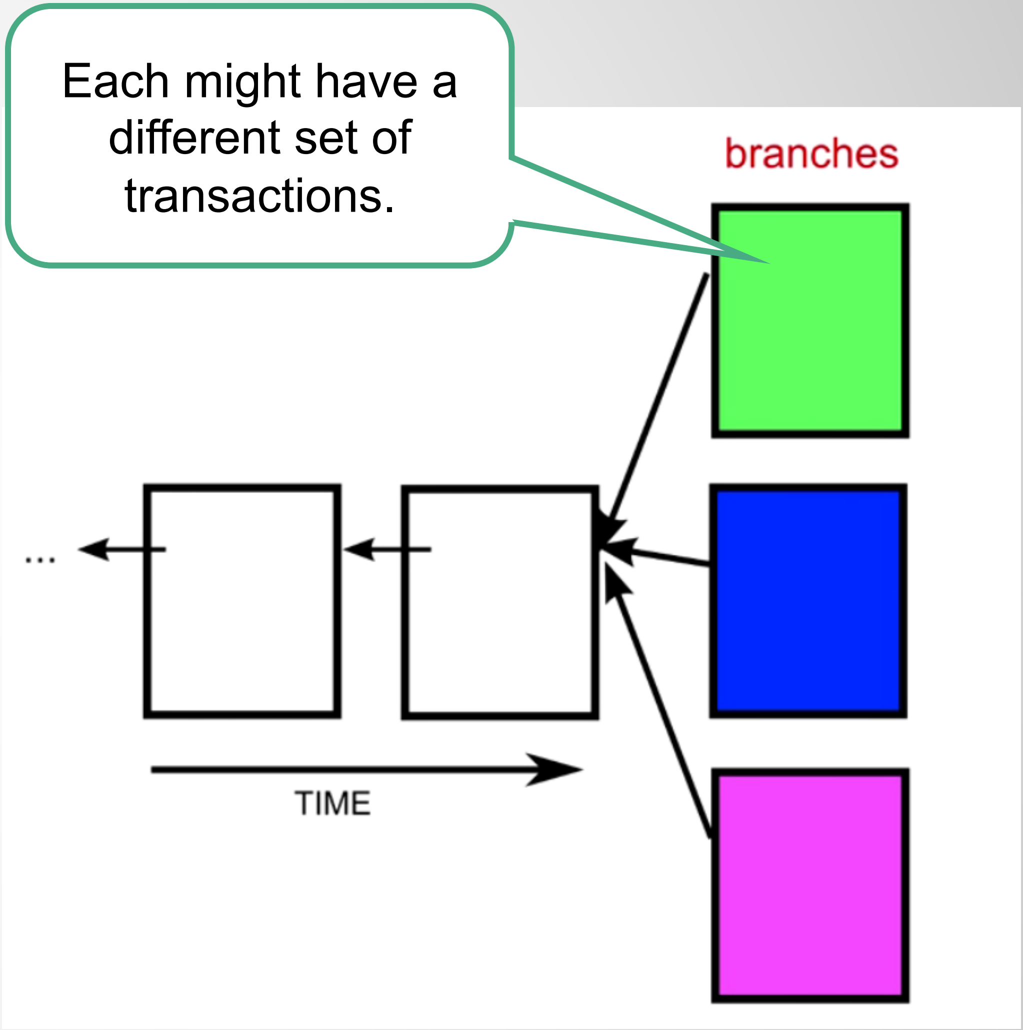
- Any node can pick a few unconfirmed transactions and create a block. By creating the block, it makes the transactions permanent (along his branch).
- To make a block, the node must solve a mathematical problem.



(How Bitcoin Works Under the Hood, Youtube)

What if two blocks are found at the same time?

- If two/more blocks are found at the same time interval, we have branching/forking.
- The branch that goes longer over the time, is taken as the main chain and the rest of transactions in other branches go back to the pool of unconfirmed transactions till somebody puts them into a valid block again.

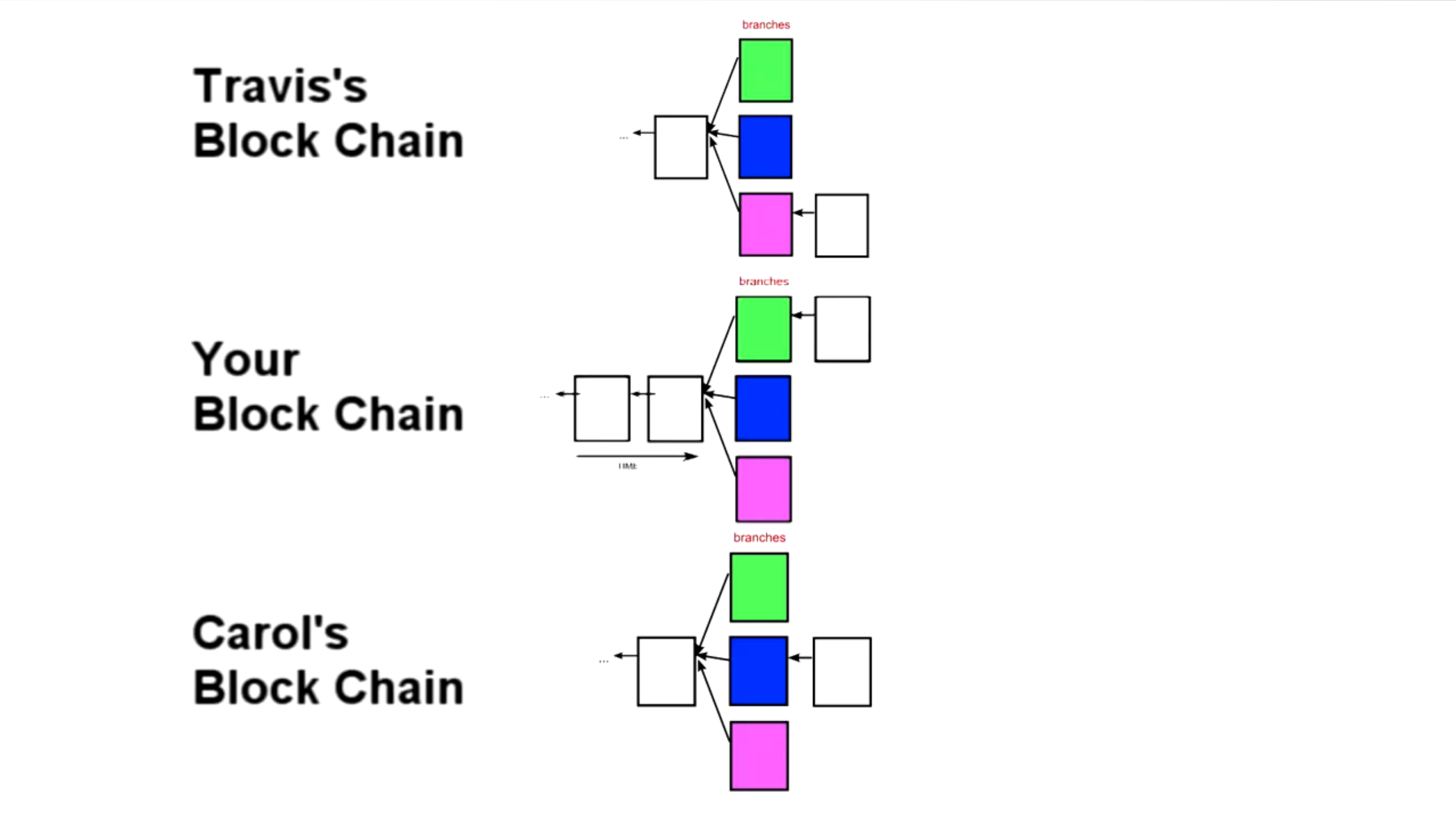


Each might have a different set of transactions.

Block chains along different branches

Let us assume 3 people build upon the branched chain, but differently. Which one is the main chain?

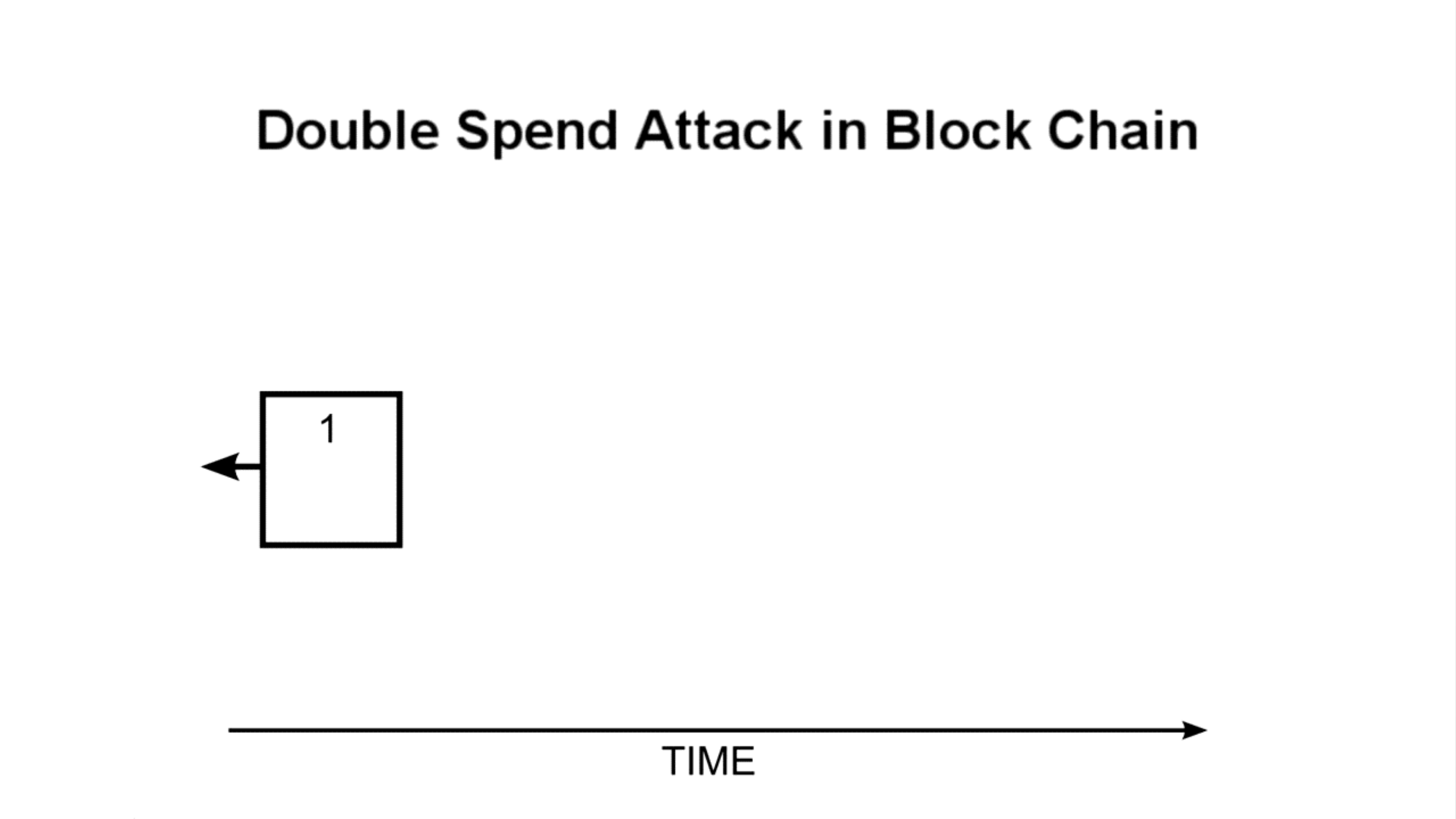
- The longest !
  - all the shorter ones will be voided and their transactions go back to the pool of unconfirmed transactions.
  - This means there can be some re-orderings at the end of the chain before it stabilizes.
  - This opens the door to the double spending fraud.



(How Bitcoin Works Under the Hood, Youtube)

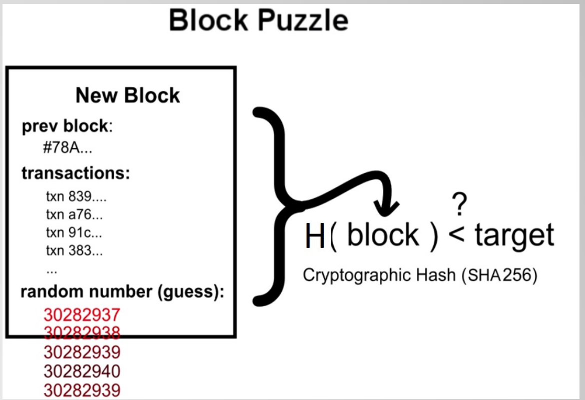
Double Spending Attack (animated)

If Alice can make a longer branch quicker than Bob and the rest of the network in that branch, she can void the block of payment to Bob and push it back to the unconfirmed pool. → She can double spend her money.



(How Bitcoin Works Under the Hood, Youtube)

Can a lone Alice do this?



- No. Why?
  - Because the whole network can in average find a valid block (none) in 10mins.
  - How probable is it that Alice with a limited processing power can generate many blocks and make a longer chain? → a high chance requires 50%+Ɛ of the whole network processing power.
  - So transactions order (which prevent double spending) is actually protected by a mathematical race.

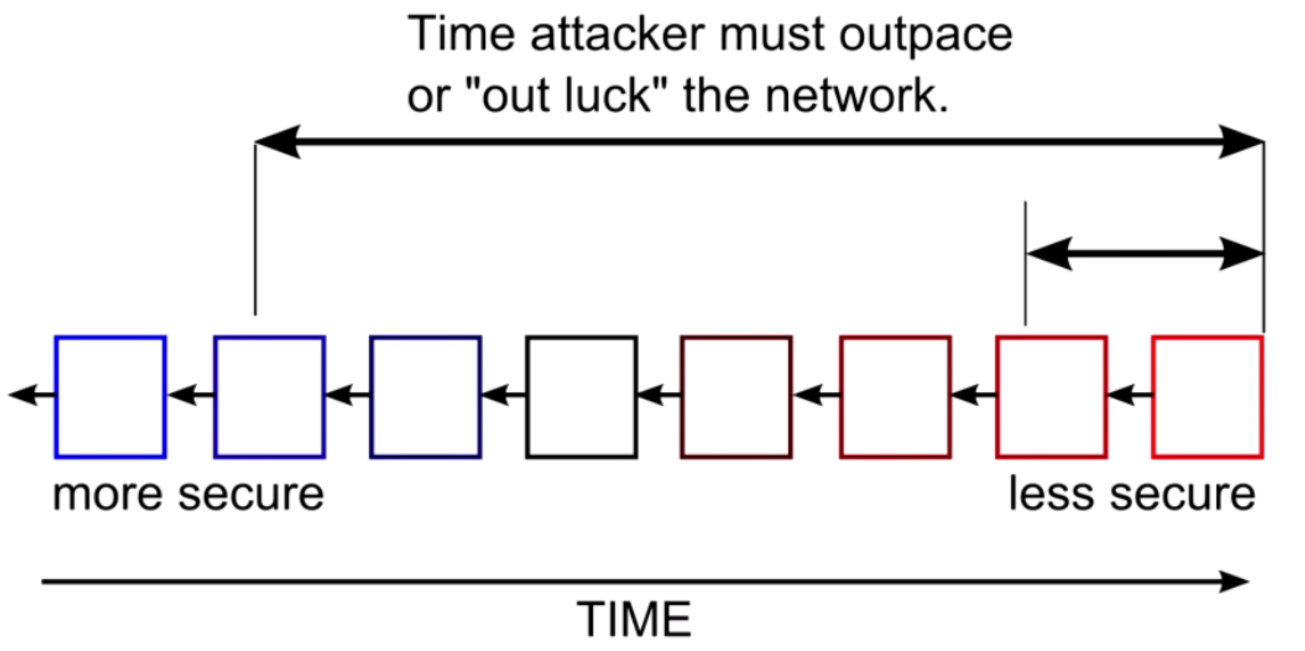
Can a lone Alice do this?

Limited processing power practically prevents double spending.

- Attack will be a race against the whole network.

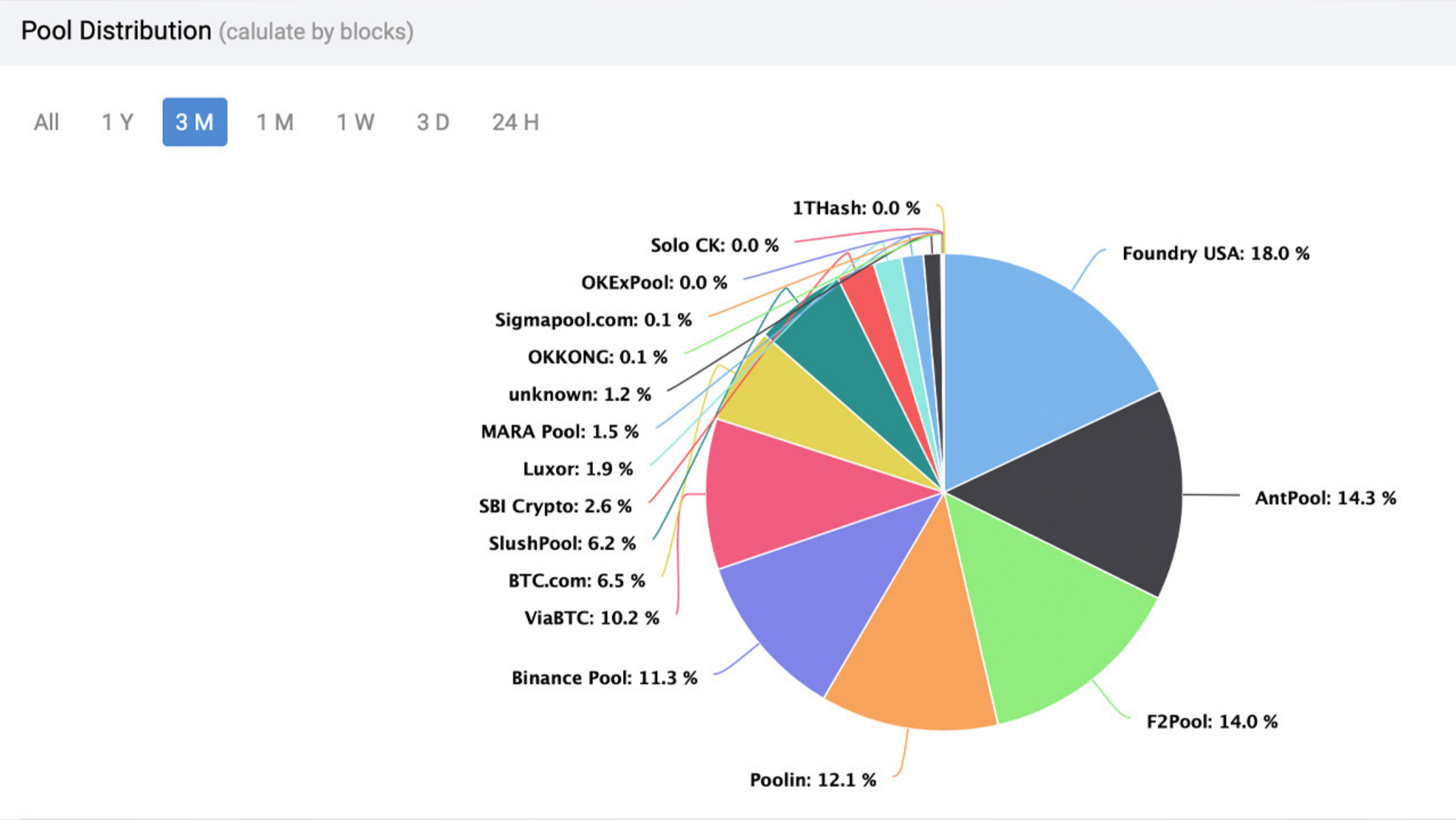
The more you wait, the more secure it is

The end of the block chain is less reliable, as it might change. But older-time blocks have been stabilized and the of double spending fraud is less probable.



(How Bitcoin Works Under the Hood, Youtube)

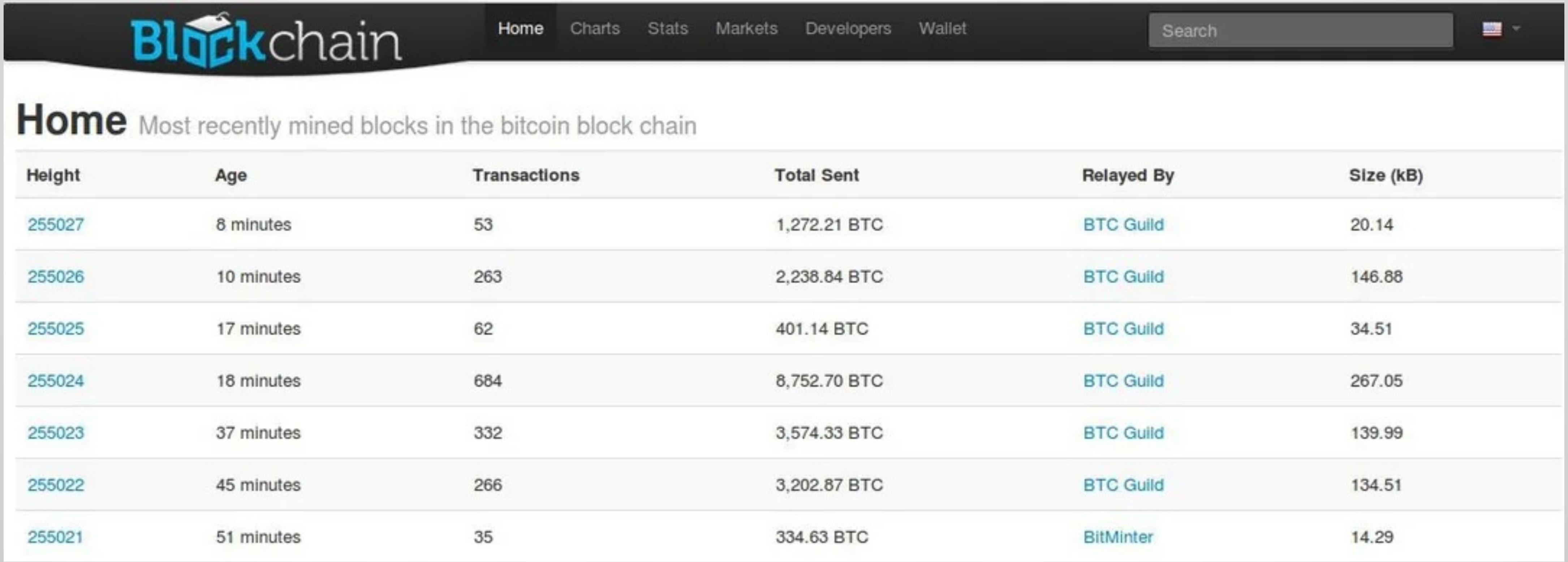
The Potential Danger of Mining Pools



(Bitcoin.com - Q1 of 2022)

The Potential Danger of Mining Pools

In 2012, BTC Guild mined 6 blocks in a row, and this was not the first time!



Home Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
255027	8 minutes	53	1,272.21 BTC	BTC Guild	20.14
255026	10 minutes	263	2,238.84 BTC	BTC Guild	146.88
255025	17 minutes	62	401.14 BTC	BTC Guild	34.51
255024	18 minutes	684	8,752.70 BTC	BTC Guild	267.05
255023	37 minutes	332	3,574.33 BTC	BTC Guild	139.99
255022	45 minutes	266	3,202.87 BTC	BTC Guild	134.51
255021	51 minutes	35	334.63 BTC	BitMinter	14.29

https://www.reddit.com/r/Bitcoin/comments/1le3rq/btc_guild_mines_six_blocks_in_a_row_again/

What Comes Next …

- We saw how transactions are ordered when branches happen and how a global consensus is reached on that.
- We learned how Bitcoin, and blockchains in general, protect themselves from double spending.
- In the next video, we explain other features of Bitcoin like anonymity and its scripting language.

See you in the next video …