School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 14

Cryptocurrency Basics

Last Updated: 20/11/2021

2

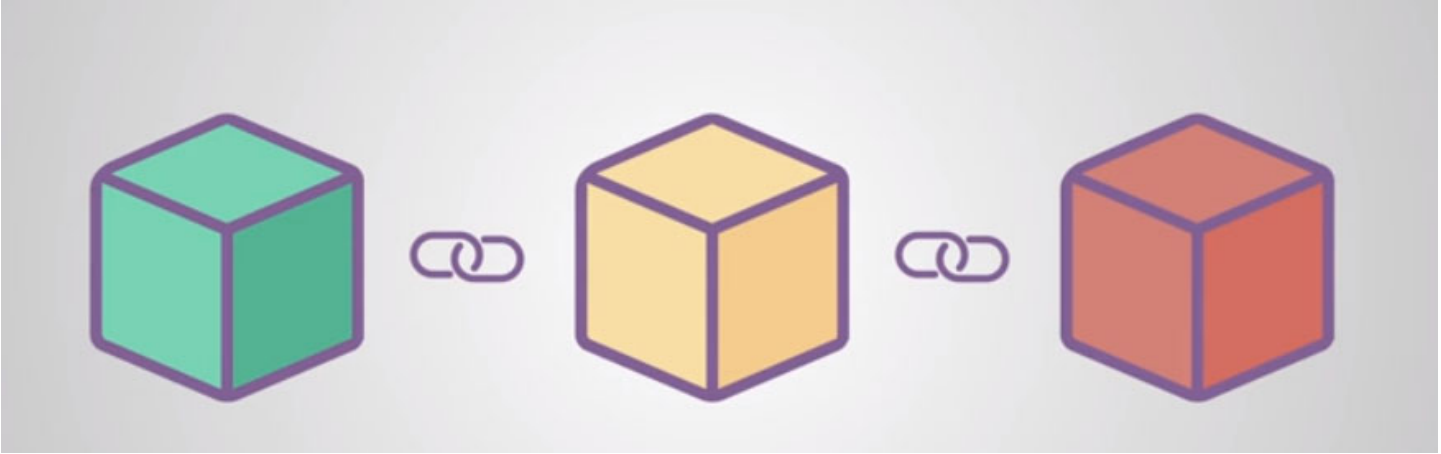
Cryptocurrency Basics

Blockchain

Cryptocurrency - Bitcoin

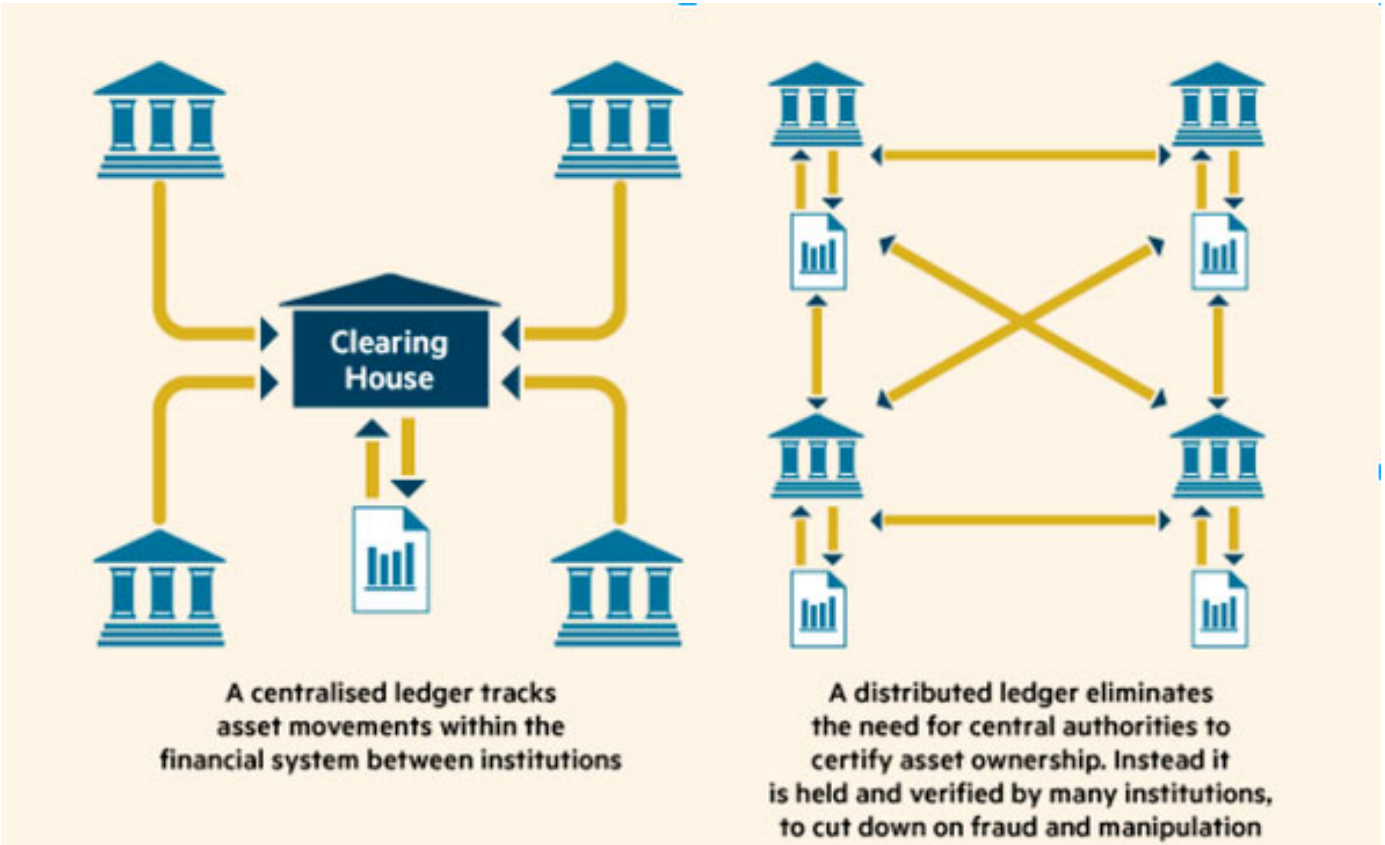
Blockchain

- A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.
- Blockchain is the technology behind cryptocurrencies.



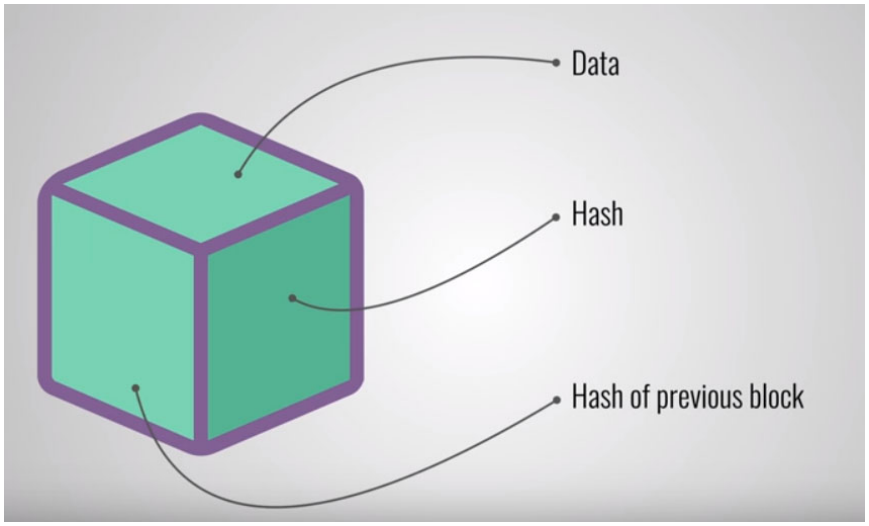
Blockchain

- Blockchains are Distributed Ledgers.
  - Ledgers are historically centralized and private
  - Blockchains are Decentralized or Distributed



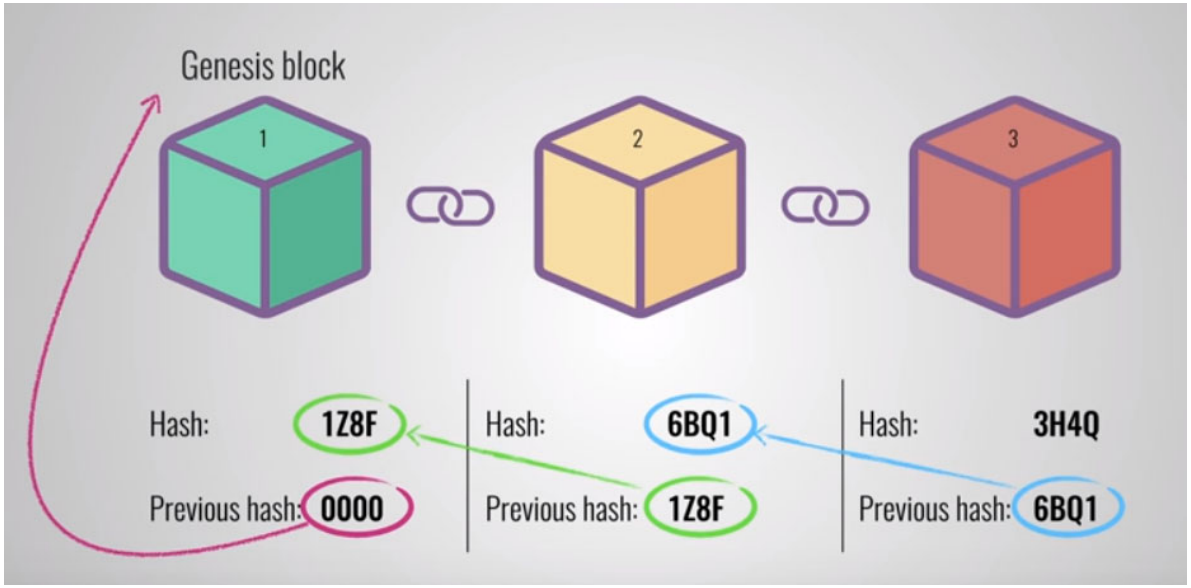
How Blockchain Works?

- Each block typically contains a transaction data, hash values of the current and the previous block, and also additional information like timestamp and etc.



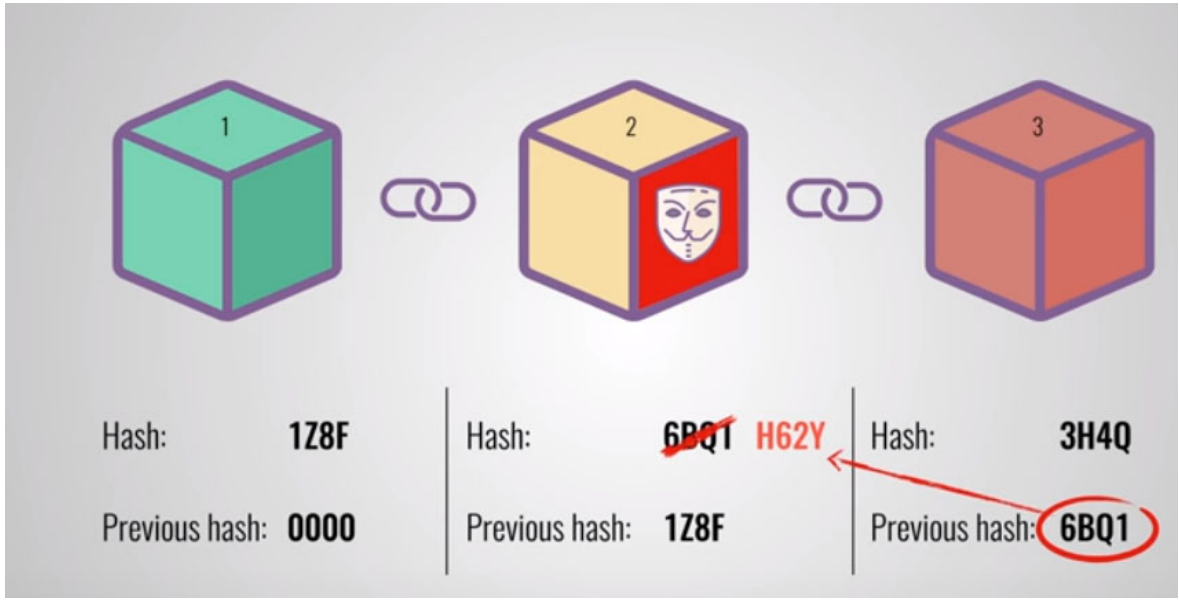
How Blockchain Works?

- The first block has no previous hash value, it is called a Genesis block.
- Subsequent blocks contain the hash value of the previous blocks.



How Blockchain Works?

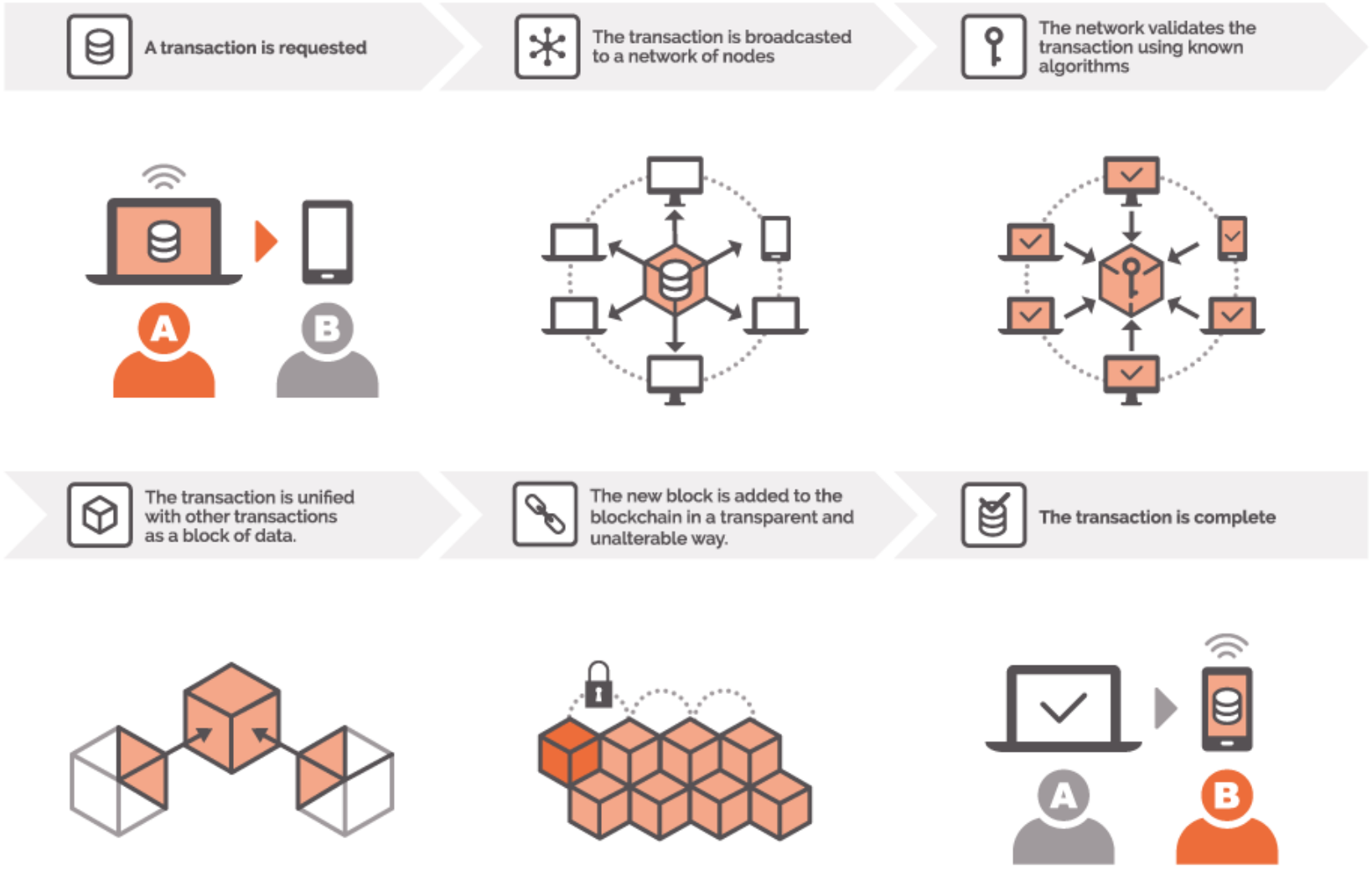
- Blockchain has great security because if a hacker changes one block, the new hash value will not match to the value stored in the next block, which makes all the subsequent blocks invalid.



How Blockchain Works?

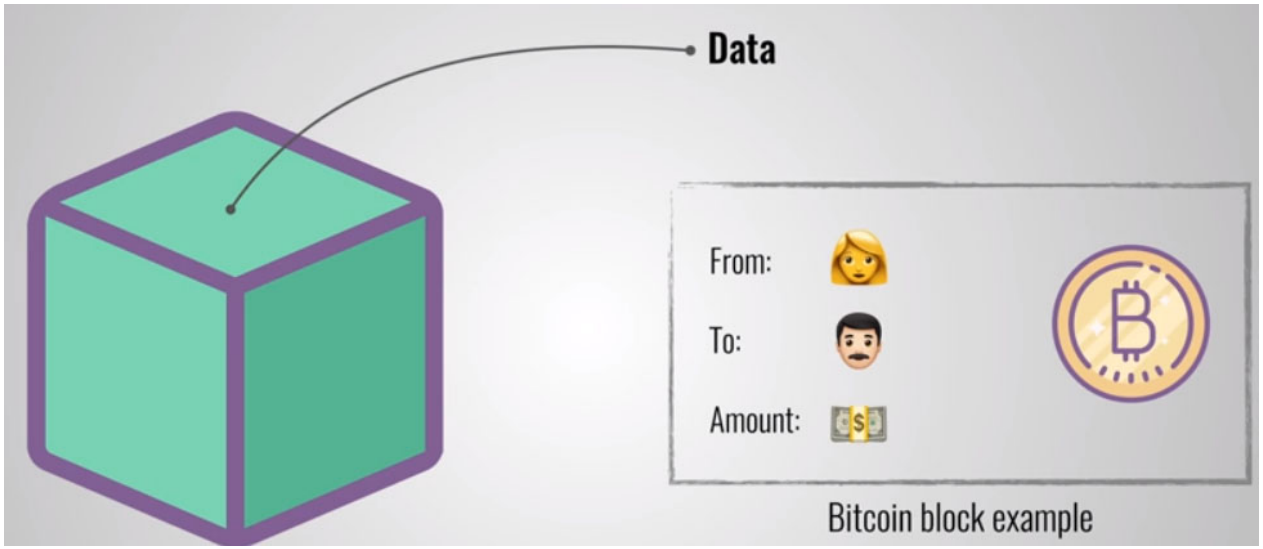
- Blockchain uses a P2P network where everyone can join.
- Everyone in the network has a full copy of the block chain.
- When a new block is created, everyone verifies the block to make sure it has not been tampered with.
- When everything checks out, each node add the new block to their blockchain.

How Blockchain Works?



Bitcoin

- Bitcoin (₿) is the world's first cryptocurrency.
- Bitcoins are sent from user to user on the peer-to-peer bitcoin network directly, without the need for intermediaries. These transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a **blockchain**.



Bitcoin block example

Bitcoin ≠ Blockchain

- Bitcoin - is an application of blockchain technology
- Blockchain - is the underlying data structure, which can be used for many things, including cryptocurrencies

Bitcoin

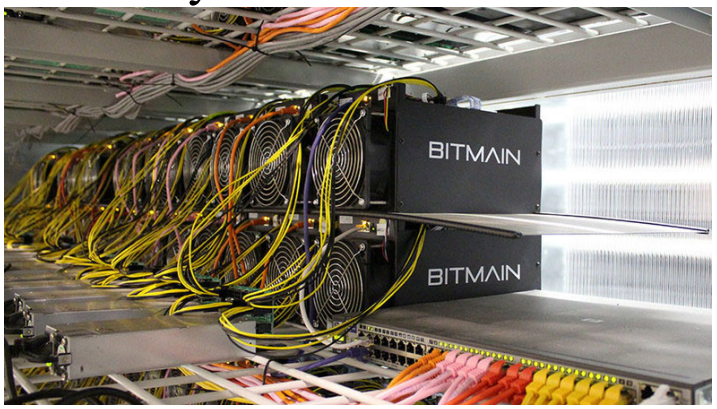
- The individuals who maintain and update the Blockchain are "miners," and they are paid a reward.
- Bitcoins are created as a reward for a process known as mining.
- The Miners process transactions by:
  - Solving a complex mathematical problem (Bitcoin hash puzzle).
  - Sending transactions to other nodes to be verified.
- When all miners agree the problem has been solved correctly, the block is added to the chain and is visible to the entire network.
- The unbroken Hash (seal) confirms that the block, and therefore every block before it, is legitimate.

Bitcoins: Mining vs Buying

- Bitcoins are ‘mined’ into existence. Mining is the process of bringing them into circulation.
- Bitcoins can also be bought either from exchanges or directly from market places through other people.

Bitcoins: Mining

- The process of mining involves an accumulation of recent transactions into blocks and trying to solve a hash puzzle.
- The **first** participant to solve the hash puzzle gets to place the next block on the blockchain and claim his rewards.
- In the early days, it was possible for the average person to mine Bitcoin, but that's no longer the case.
- Today, Bitcoin mining requires powerful computers and access to massive amounts of cheap electricity to be successful.



What Are the Miner's Mining?

- Recall a hash function such as SHA256, it means is whenever an SHA-256 algorithm is applied to any length of string or text, it will give back a unique 256-bit string.
- Assume there are 4 recent transactions accumulated in a block, such as:
  - Address10 (sender) transfers 1 bitcoin to address23 (receiver), and etc.

```
address10 -> 1 btc -> address23
address23 -> 0.5 btc -> address50
address21 -> 100 btc -> address200
address36 -> 0.001 btc -> address214
```

- It will be very straightforward to hash the above 4 lines. But Bitcoin increases the difficulty of the hash puzzle by setting a requirement.

What Are the Miner's Mining?

- You are required to add a new line on top of the transactions called Nonce.
- The Nonce can be any number example 123456 or 94857, for your trial and error.
- With your selected Nonce and the 4 transactions, the hash value should start with 5 leading 0s.

```
Nonce: 123456
address10 -> 1 btc -> address23
address23 -> 0.5 btc -> address50
address21 -> 100 btc -> address200
address36 -> 0.001 btc -> address214
```

What Are the Miner's Mining?

Nonce: ?????
address10 -> 1 btc -> address23
address23 -> 0.5 btc -> address50
address21 -> 100 btc -> address200
address36 -> 0.001 btc -> address214

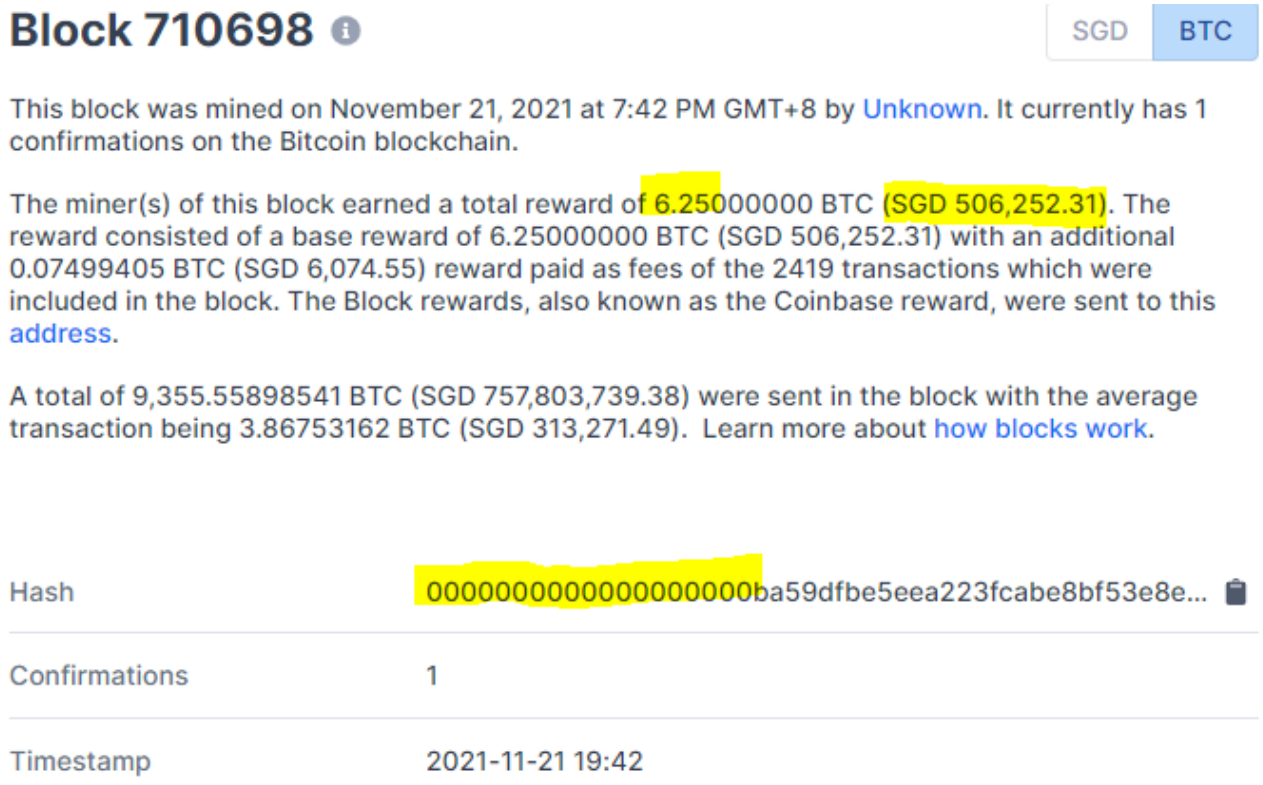
- Since a good hash outcome is not predictable, so you have to try a lot of times to find a good nonce.
- Only the first person who work the puzzle out is winner and get the Bitcoin rewards.
- In the actual world, Bitcoin may increase the difficulty by requiring you to obtain more leading 0s.

Bitcoin Network

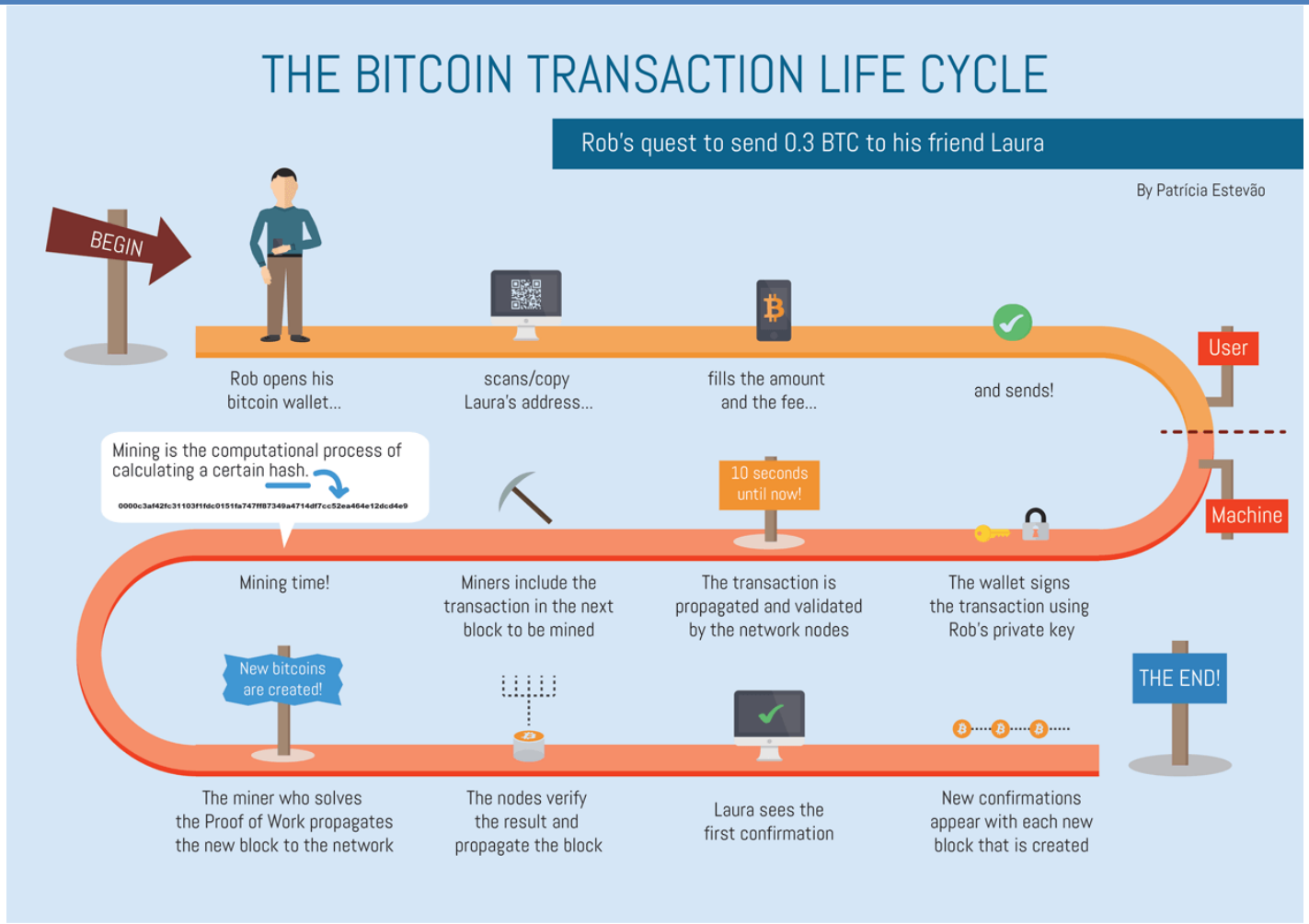
- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block.
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions, prevent double spending).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Reading a Bitcoin Block

- You can access the Blockchain's block explorer to read all the mined blocks. You may also notice that the current number of leading 0s is 19. And the reward for the winner is 6.25BTC, worth SGD 506,252.31.
- https://www.blockchain.com/explorer



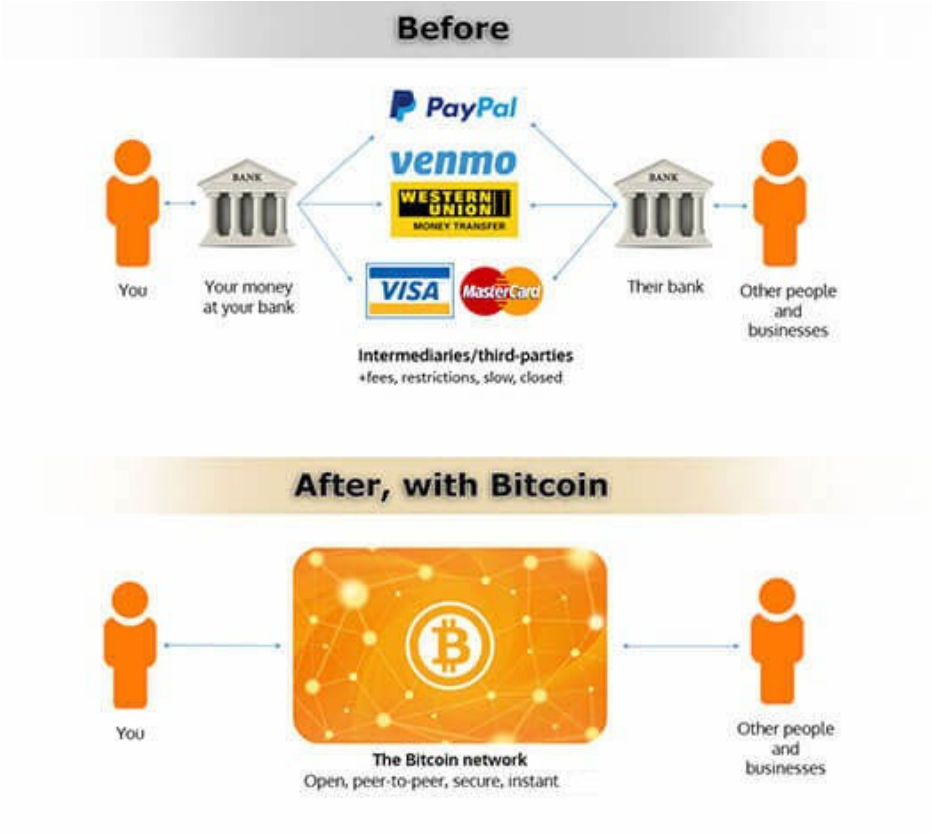
Bitcoin Transaction Life Cycle



Bitcoins: Buying

Bitcoin Transaction

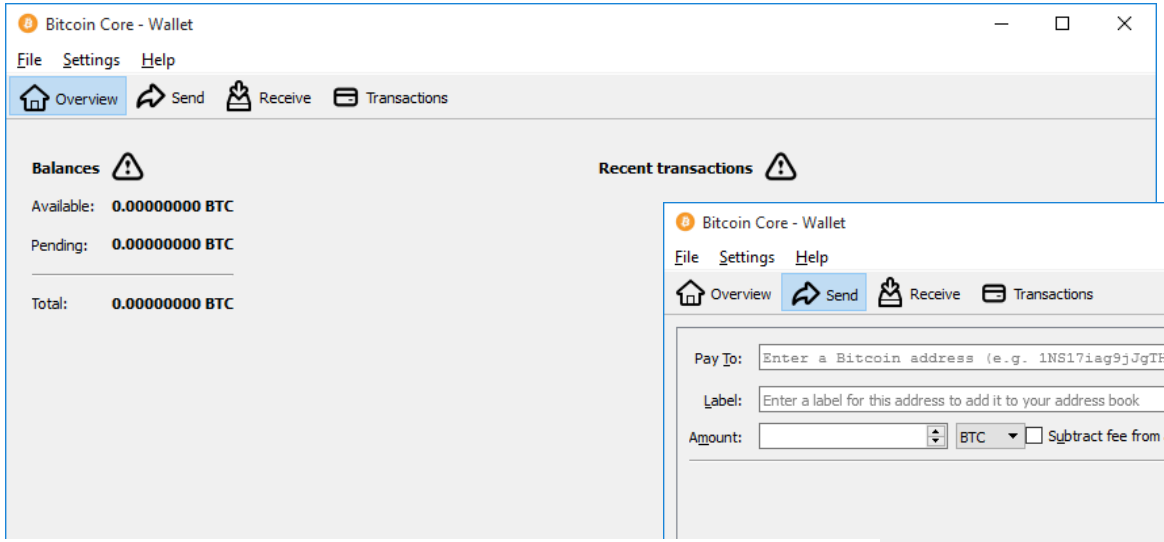
- Peer-to-peer and de-centralized transactions.

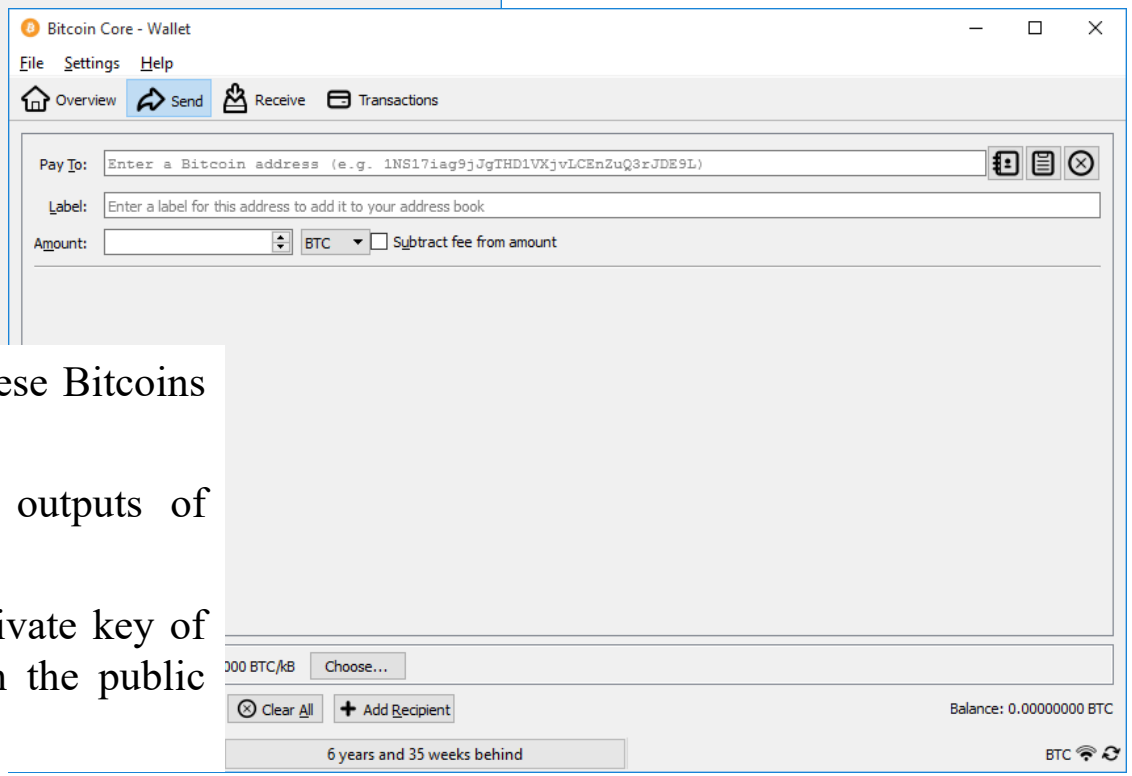


Bitcoin Wallet

- There are software applications available for you to create a Bitcoin wallet (see https://bitcoin.org/en/choose-your-wallet)
- The wallet holds the private keys you use to prove your own specific Bitcoins.
- The software creates public/private key pairs for you as needed.
  - For each pair, there is a corresponding bitcoin address, which is a 160-bit hash of the public key. Bitcoins are sent to addresses.
- The wallet also contains software that allows you to send and receive bitcoins.
  - You send bitcoins by registering your payments in the block chain, which is bitcoin's public ledger containing all transactions since the beginning of bitcoin.

Bitcoin Wallet Transaction





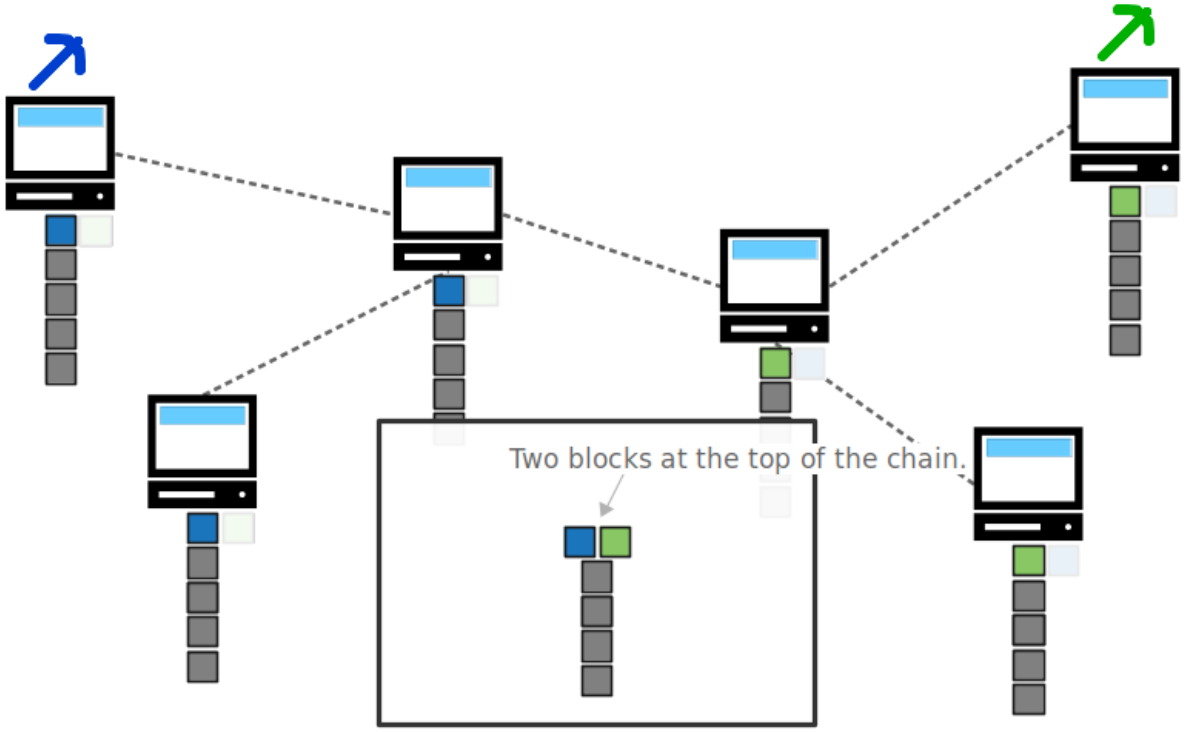
- A transaction is of the form “send these Bitcoins from address X to address Y”
- Specific Bitcoins are described as outputs of previous transactions.
- The transaction is signed with the private key of address X and broadcast, along with the public key of X, to the payment network.

Bitcoin Transaction Verification

- For the same transaction: “send these Bitcoins from address X to address Y”
- The miner first checks the signature using the public key for address X.
- Then the miner checks the public ledger to verify that X hasn’t already sent these Bitcoins to someone else.
- After the above steps, a transaction is verified.

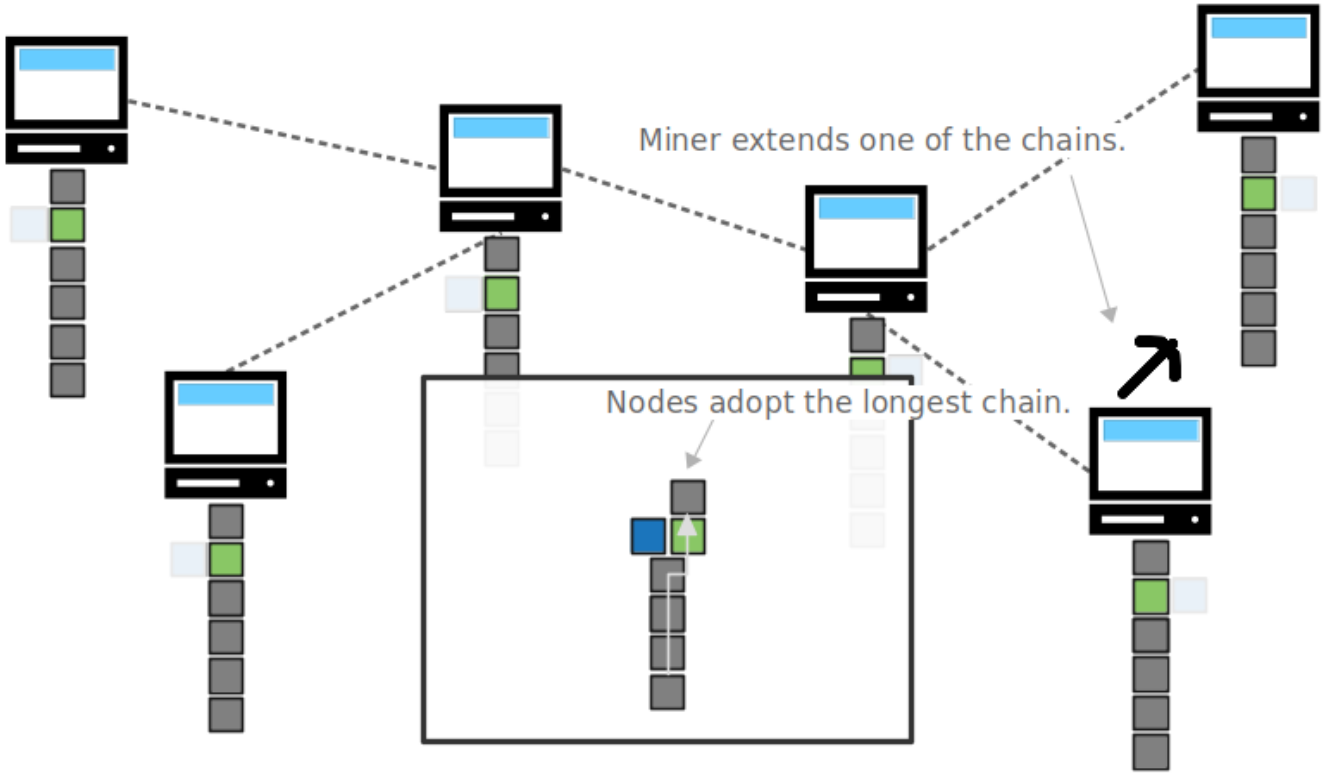
Bitcoin Transaction Problem- Blockchain Forks

- Due to the fact that bitcoin operates on a network, it's possible that two independent computers will mine a block at the same time. In this situation, nodes across the network will end up being in disagreement about which of these two blocks should be at the top of the blockchain.

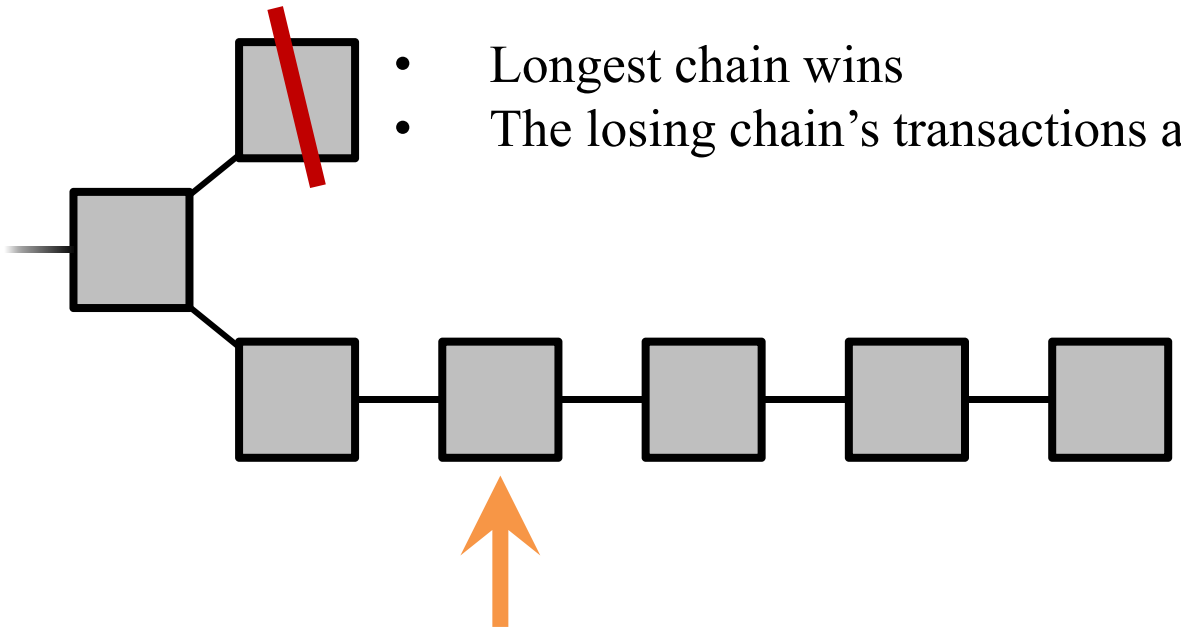


Bitcoin Transaction Problem- Blockchain Forks

- However, this situation can be resolved by having nodes adopt the longest chain of blocks. This is because the next block to be mined will build upon one of these two blocks, creating a new longest chain that all nodes on the network will be happy to adopt.



Transaction Confirmation



- Longest chain wins
- The losing chain's transactions are reverted

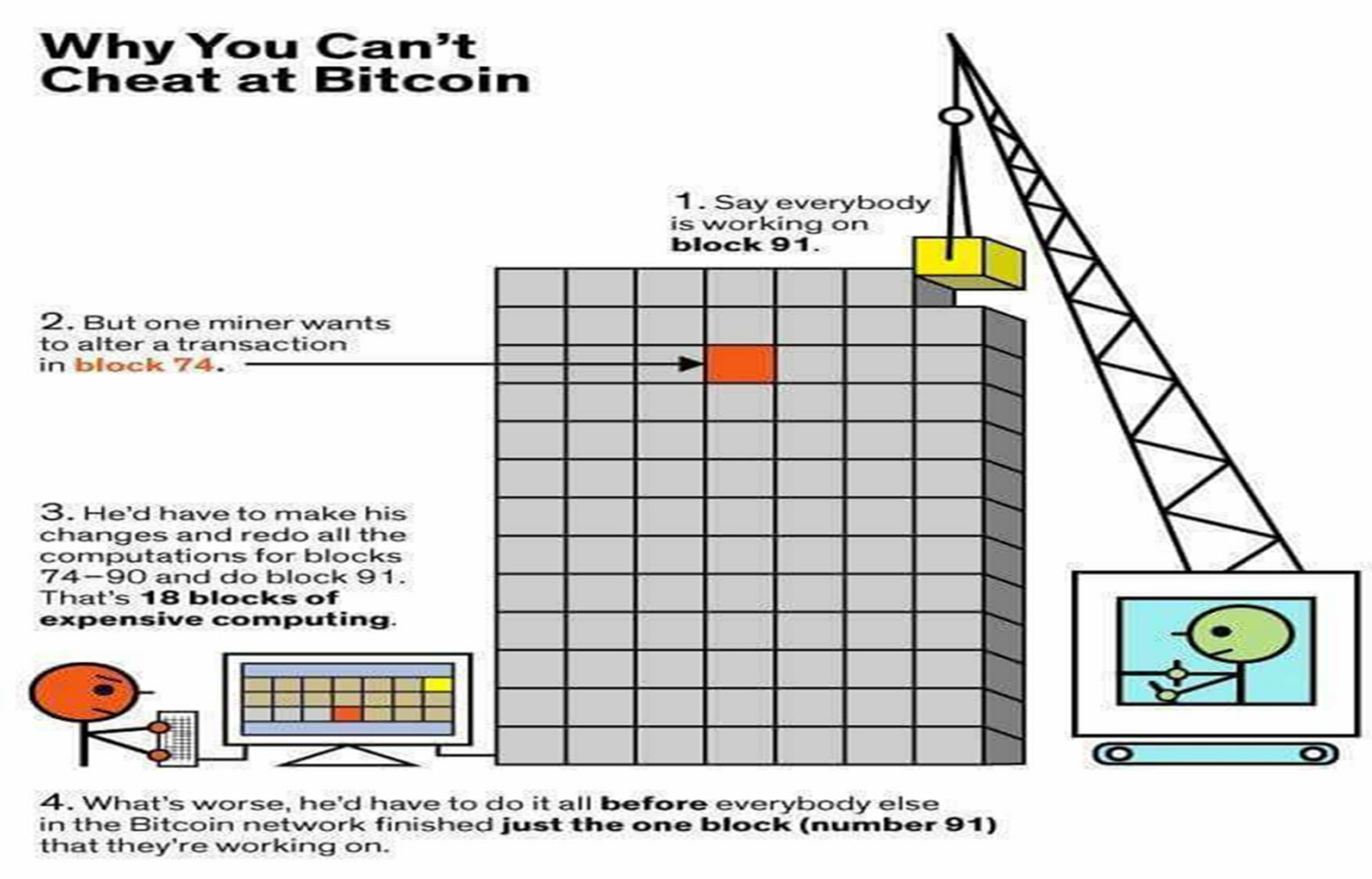
A transaction is **confirmed** when it is **buried** deep enough

Transaction Confirmation

- How many Bitcoin Confirmations are Enough?

0	Payments with 0 confirmations can still be reversed! Wait for at least one.
1	One confirmation is enough for small Bitcoin payments less than $1,000.
3	Enough for payments $1,000 - $10,000. Most exchanges require 3 confirmations for deposits.
6	Enough for large payments between $10,000 - $1,000,000. Six is standard for most transactions to be considered secure.
60	Suggested for large payments greater than $1,000,000. Less is likely fine, but this is to be safe!

Bitcoin Security



Transactional Properties

- **Irreversible**: After confirmation, a transaction can't be reversed.
- **Pseudonymous**: Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters.
- **Fast** and global: Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes.
- **Secure**: Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency.
- **Permissionless**: You don‘t have to ask anybody to use cryptocurrency. It‘s just a software that everybody can download for free.

References - Videos

- https://youtu.be/dcQCa4Ctkcc
- https://youtu.be/l9jOJk30eQs
- https://youtu.be/Lx9zgZCMqXE

Summary

Summary

What is Cryptocurrency?

Cryptocurrency is a digital money, created from code.

Free of all governmental oversight, The cryptocurrency economy is monitored by a peer-to-peer internet protocol .

Cryptocurrency is an encrypted string of data or a hash, encoded to signifyone unit of currency

Examples of Cryptocurrency

Bitcoin Market Cap
$11,322,347,786

Ethereum Market Cap
$928,068,434

Ripple Market Cap
$293,888,278