Finance Matters Lecture 6 (Part 1)

By Dr. Monia Mazigh, 2019©

Cryptocurrencies: Bitcoins and others

Bitcoins

- A cryptocurrency is a digital or a virtual currency that uses cryptography for security
- It's like an online version of cash
- A Peer-to-Peer Electronic Cash System
- Bitcoins started in 2009
- It follows an idea released in a white paper by an anonymous and mysterious person **Satochi Nakamoto**

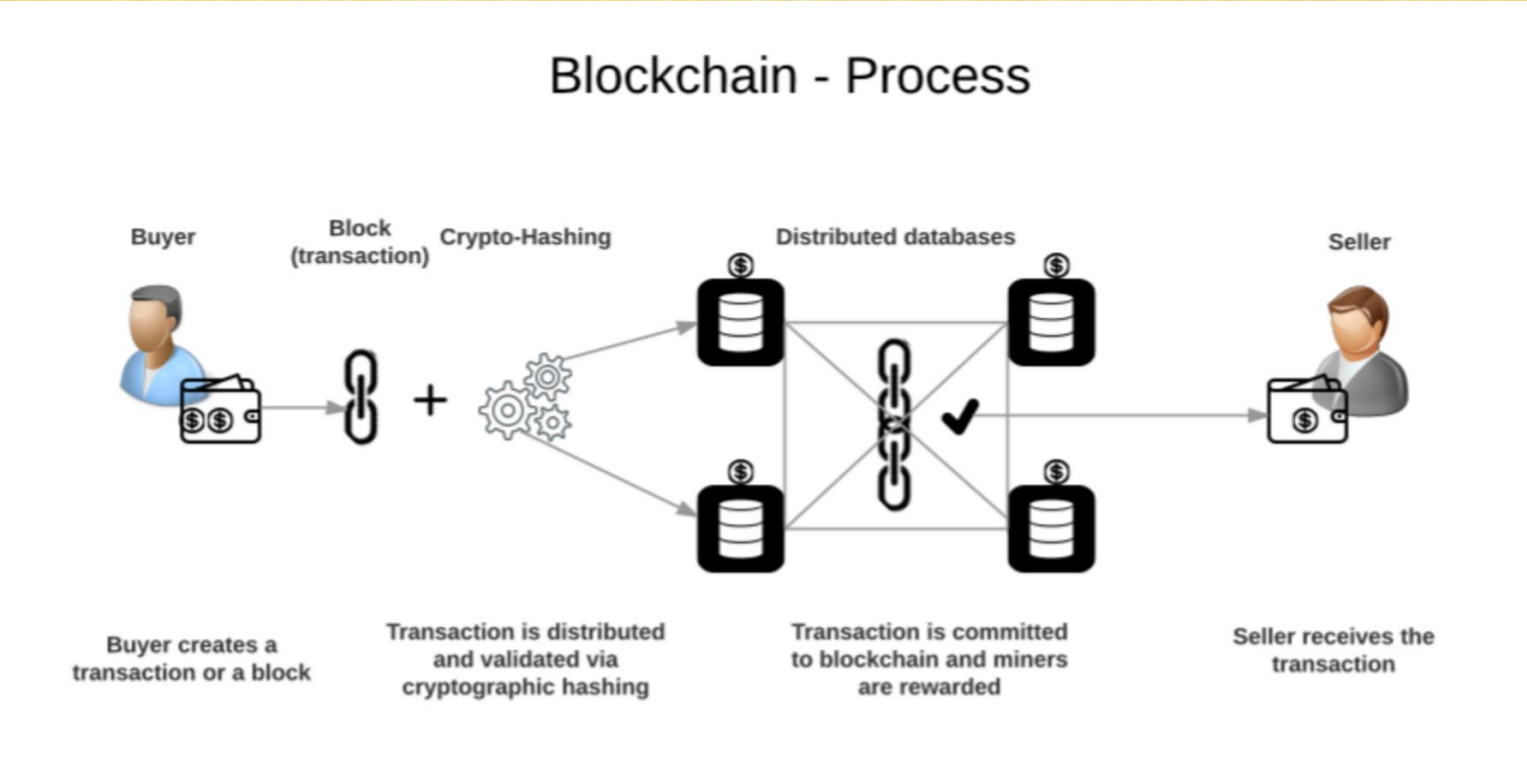
- There are no physical bitcoins
- There are only balances associated with public addresses
- These addresses can be viewed on the blockchain
- Blockchain keep track of the transaction
- The blockchain are made public so it stops people from spending coins they do not own, making copies or undoing transactions
- Each address has an authorized private key used to authorize transaction
- Each key should be known only to the owner

- Cryptocurrencies (Bitcoins) are legal in many countries
- They are accepted by some businesses and by some retailers
- New bitcoins are released through a process called **mining**
- Anyone who owns a free open source software can participate in the process

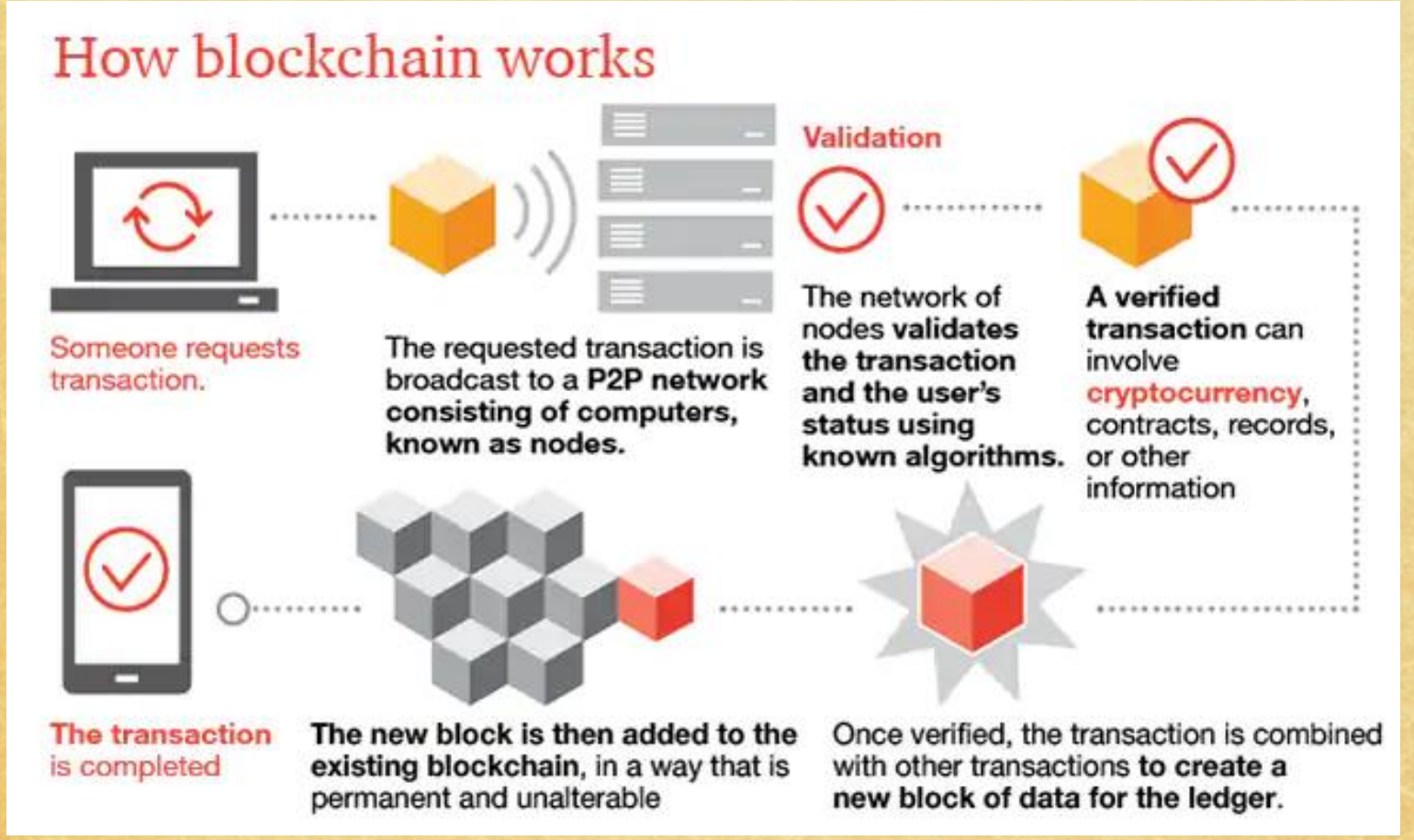
- There are three ways for people to get Bitcoins
- You can **buy Bitcoins** using “real” money.
- You can **sell things** and let people pay you with Bitcoins
- Or they can be **created** using a computer
- The computers are made to work out incredibly difficult computations. Occasionally they are rewarded with a **Bitcoin**
- People set up powerful computers just to try and get Bitcoins. This is called **mining**

- A cryptocurrency is not issued by any central authority, rendering it theoretically immune to government interference or manipulation
- The confirmation is **key** in this system. The **miners** need to solve the puzzle in order to confirm the transaction. By solving the puzzle, you receive a reward in forms of a “bitcoin”

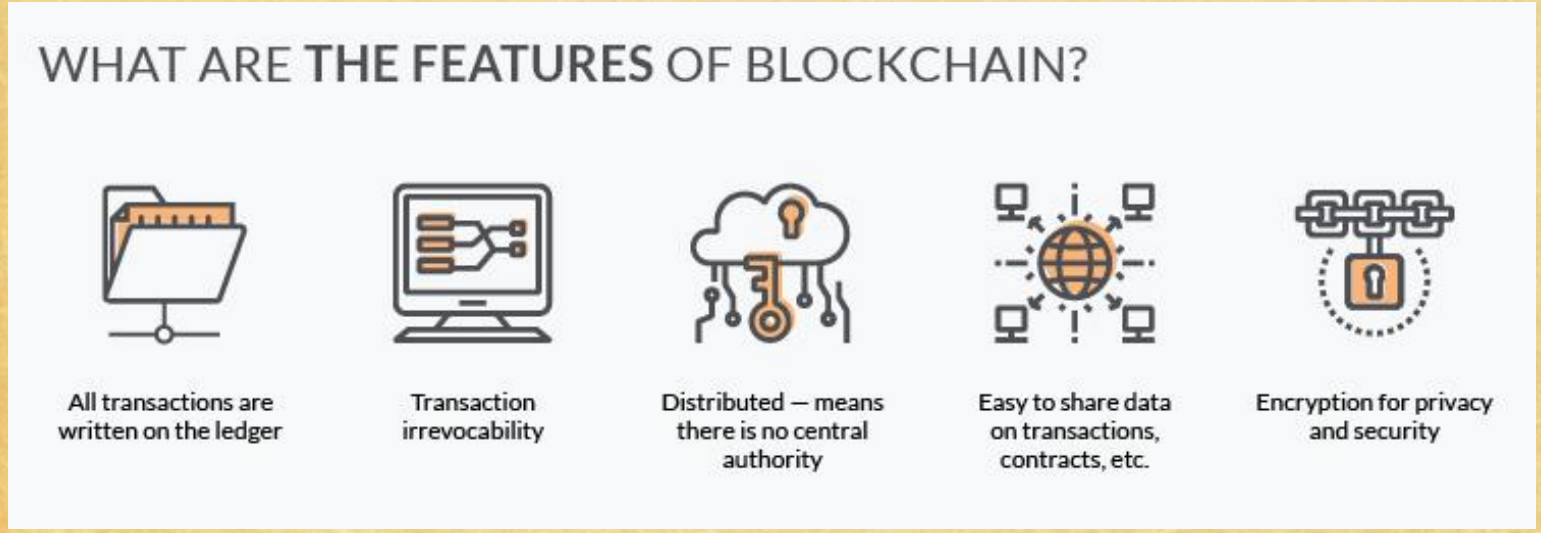
How it works


Blockchain - Process
Buyer
Block (transaction)
Crypto-Hashing
Distributed databases
Seller
Buyer creates a transaction or a block
Transaction is distributed and validated via cryptographic hashing
Transaction is committed to blockchain and miners are rewarded
Seller receives the transaction

Blockchain


How blockchain works
Someone requests transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information
The transaction is completed
The new block is then added to the existing blockchain, in a way that is permanent and unalterable
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

Blockchain


WHAT ARE THE FEATURES OF BLOCKCHAIN?
All transactions are written on the ledger
Transaction irrevocability
Distributed — means there is no central authority
Easy to share data on transactions, contracts, etc.
Encryption for privacy and security

Keys

- Balances are kept using public and private "keys"
- Keys are are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them.
- The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins.
- The private key (comparable to an ATM PIN) is meant to be a guarded secret and only used to authorize Bitcoin transmissions.

- Once verified the transaction is publicly stored on a public ledger
- This is known as the blockchain
- Transactions fee for Bitcoins are relatively low compared to traditional transaction fees

Bitcoin Mining

- It is the process through which bitcoins are released to come into circulation
- It involves solving a computationally difficult puzzle to discover a new block, which is added to the blockchain
- The miner would receive a reward in the form of a few bitcoins
- The block reward was **50 new bitcoins in 2009**
- It decreases every four years. As more and more bitcoins are created, the difficulty of the mining process – that is, the amount of computing power involved – increases.

Miners

- The independent individuals and companies who own the governing computing power and participate in the Bitcoin network, also known as **miners**
- They are motivated by rewards (the release of new bitcoin) and transaction fees paid in bitcoin
- These miners can be thought of as the decentralized authority enforcing the credibility of the Bitcoin network

Easy Step

- First, they must verify 1 megabyte (MB) worth of transactions, which can theoretically be as small as 1 transaction but are more often several thousand, depending on how much data each transaction stores.

Hard Step

- Miners must solve a complex computational math problem, also called a "**proof of work".**
- They try to come up with a 64-digit hexadecimal number, called a **"hash"** that is less than or equal to the target hash
- A miner's computer spits out hashes at a rate of megahashes per second (MH/s), gigahashes per second (GH/s), or even terahashes per second (TH/s) depending on the unit, guessing all possible 64-digit numbers until they arrive at a solution. In other words, it's a gamble.

- There are currently 17, 300, 900 BTC in existence.
- This number changes about every 10 minutes when new blocks are mined.
- The reward for mining each block started at 50 BTC (2009) and has since “halved” twice. The current reward sits at 12.5 Bitcoins per block.

- New bitcoin are being released to the miners at a fixed, but periodically declining rate, such that the total supply of bitcoins approaches **21 million by year 2140**
- Crypto inventor Satoshi Nakamoto set a monetary policy based on artificial scarcity at bitcoin's inception that there would only ever be 21 million coins in total.

Mining Difficulty

- As of February 2019, the mining difficulty is over 6.06 *billion*.
- Once, an ordinary desktop computer sufficed for the mining process; now, to combat the difficulty level, miners must use faster hardware like Application-Specific Integrated Circuits (ASIC), more advanced processing units like Graphic Processing Units (GPUs),

Cryptocurrency Mining Difficulty