NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CC0007 Science and Technology for Humanity

Blockchain Revolution

Asst Prof Li Yi, NTU

The Bitcoin Revolution

What is Money?

A medium of exchange
for buying things

A unit of account
for pricing

A store of value
for saving

MONEY = VALUE = TRUST

Fiat Money

(*Latin fiat - 'let it be done' or 'so it be')*

- **Fiat money**
  - The dollars, or euros, or any other currency for that matter have value because the government orders it to.
- **Drawbacks**
  - It is centralised.
  - It is not limited in quantity (e.g., unlimited QE).

Beigel, O. (2022, January 13). *What is bitcoin? A complete beginner's guide*. 99Bitcoins. Retrieved July 20, 2022 from https://99bitcoins.com/bitcoin/#centralization

Digital Money and “Double-Spending” Problem

- Digital money is a type of currency available in digital form in contrast to physical, such as banknotes and coins.
  - Allow for instantaneous transactions and borderless transfer-of-ownership
- **Double-spending:** A potential flaw in a digital cash scheme in which the same single digital token can be spent more than once.
- This is possible because a digital token consists of a digital file that can be **duplicated or falsified**.
- Banks’ solution:
  - Keep a computer ledger to keep track of who owns what
    ⟶ **Centralised computer system**

PayPal

Double-spending. (2022, June 19). In *Wikipedia*. Retrieved July 20, 2022 from https://en.wikipedia.org/wiki/Double-spending

Hello Bitcoin! (Oct 2008)

Proposed by Satoshi Nakamoto

- A **peer-to-peer (P2P)** electronic cash system
- This system claimed to create **digital money** that solves the **double-spending problem** without the **need for a central authority**.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

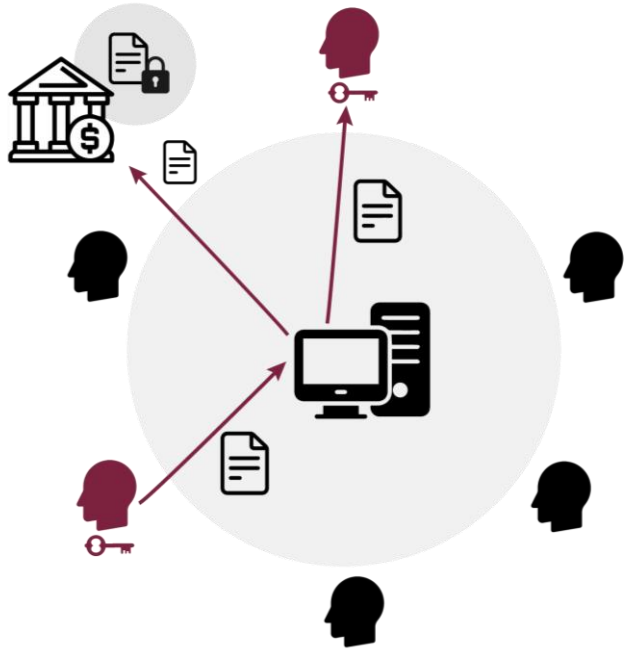
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system* [White paper]. Bitcoin. Retrieved July 20, 2022 from https://bitcoin.org/bitcoin.pdf

Centralised or Decentralised

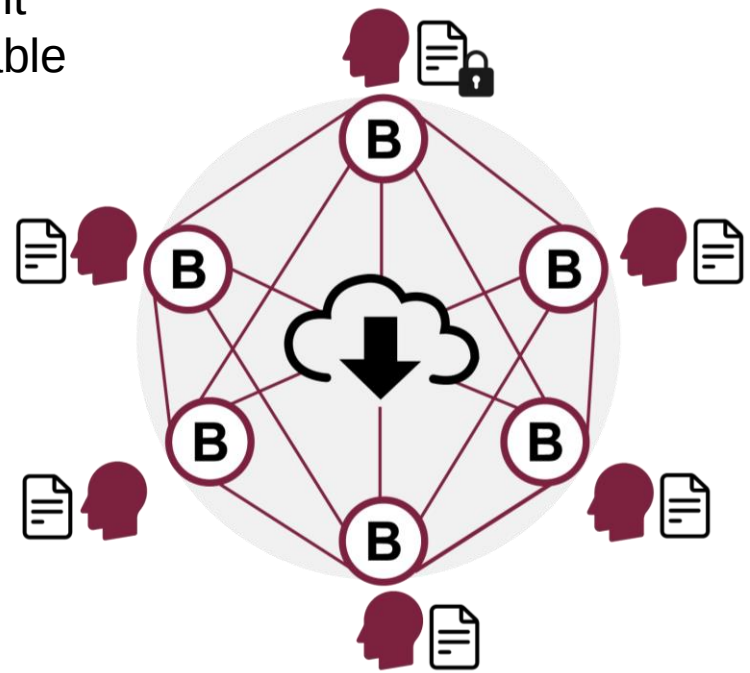
Centralised system:

- Bookkeeper fee
- Availability
- Power corruption
- Single point of failure
- Non-resilient



Decentralised system:

- Trusted
- Transparent
- Shared
- Resilient
- Immutable



Why is Bitcoin a Big Thing?

Internet is the information superhighway

is the Internet of Value (Trust)