Bitcoin: A New Internet Currency

The opinions expressed are solely those of the presenters and do not reflect the opinions of the Federal Reserve Bank of Dallas or the Federal Reserve System.

Economic Education at the Dallas Fed

What is Bitcoin?

- A **peer-to-peer** internet currency that allows **decentralized** transfers of value between **individuals and businesses**.

Economic Education at the Dallas Fed

Bitcoin vs. bitcoins

- **Bitcoin** is the system
- **bitcoins** are the units

Economic Education at the Dallas Fed

Creating a currency from scratch

- Motivation
  - Distrust of financial institutions
  - Transaction costs
- Primary concerns
  - Transaction security
  - Double spends

Economic Education at the Dallas Fed

Distrust of financial institutions

- Any noncash transaction requires a trusted third-party administrator—commonly a bank or financial service provider.
- The system forces participants to trust financial institutions that are not always trustworthy.

Transaction costs

- Traditional payments are revocable, even on irrevocable services.
- Financial institutions act as an arbitrator between counterparties in disputed claims.
- Arbitration costs are passed on to consumers.

Transaction security

- Two levels of verification
  - Source is legitimate
  - Coins are legitimate
- Public/private key verification ensures the legitimacy

Double spends

- If the money is just digital codes, why not copy and paste to make more money?
  - Timestamps
  - Hashes
  - Block chain

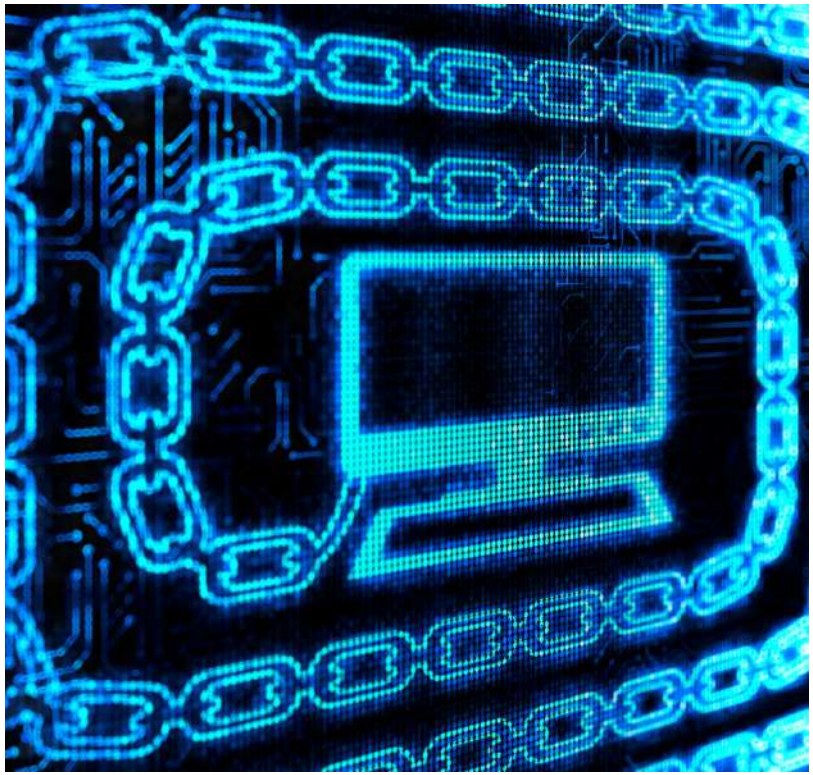
Double spends

- Timestamp
  - Each transaction is packaged and publically recorded in the order it was carried out.
- Hash
  - The time-stamped group of transactions are given a unique algorithmically derived number

Economic Education at the Dallas Fed

Double spends

- Block chain
  - Transactions are recorded in a community-built record of all transactions that acts as a proof-of-work.
  - Computers connected to the network accept the longest chain as accurate.



Economic Education at the Dallas Fed

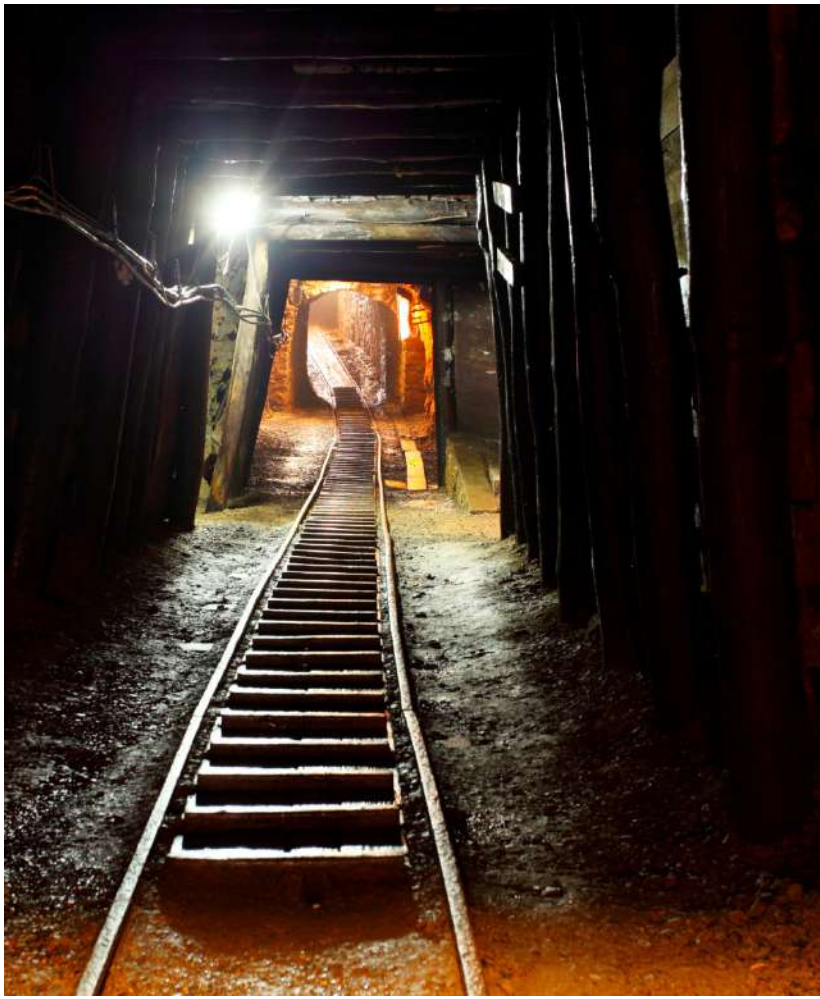
Where do bitcoins come from?

- They’re mined, silly.
- High-powered computers solve complicated math problems.
- Each time a problem is solved, the finder is paid a bounty.

Economic Education at the Dallas Fed

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.



Economic Education at the Dallas Fed

Mining bitcoins

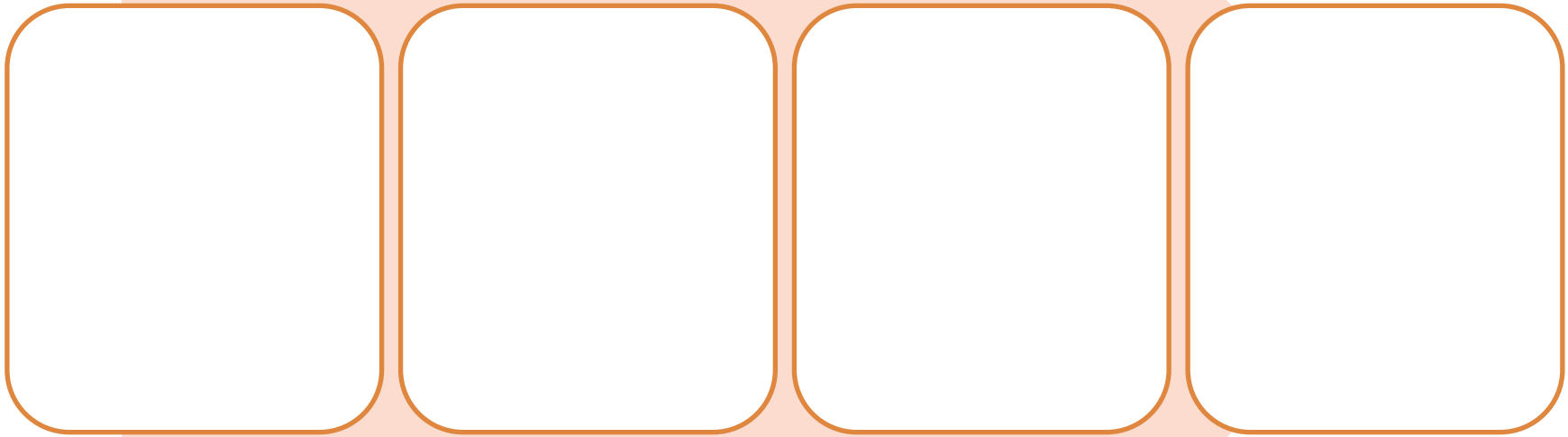
- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount paid per hash goes down by half about every 4 years.

Owning bitcoins

- Users create accounts called wallets.
- Wallets are secured using passwords and contain the private keys used for transferring bitcoins.

Economic Education at the Dallas Fed

Spending bitcoins



Bitcoin security

- Computers accept the longest block chain, which inhibits hacking.
  - Hackers would have to create a longer chain of fraudulent information faster than the combined effort of all other computers.
- Public/private cryptography means individual bitcoins are secured when not being transacted.

Is it money?

- Store of value
- Medium of exchange
- Unit of account

Is it money?

Economic Education at the Dallas Fed