Bitcoin: In the News

Stephen Clayton
Community Engagement Director
Federal Reserve Bank of Dallas

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.

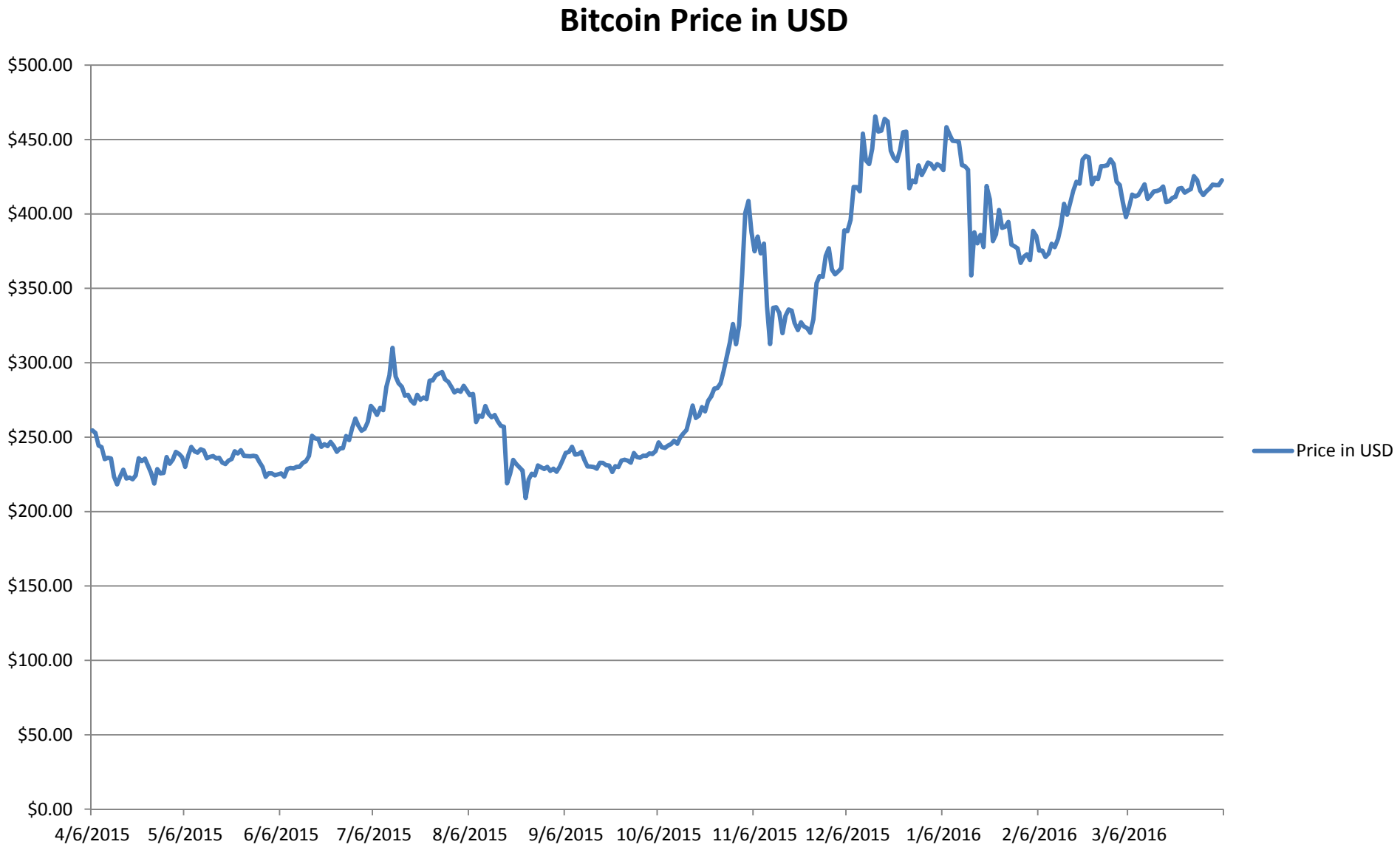
What is Bitcoin?

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

Is Bitcoin Money?

- Anything that is generally acceptable as payment for goods and services or for repayment of debts
- Store of Value
- Medium of Exchange
- Unit of Account

Let's (pretend) to buy something


Bitcoin Price in USD
$500.00
$450.00
$400.00
$350.00
$300.00
$250.00
$200.00
$150.00
$100.00
$50.00
$0.00
4/6/2015
5/6/2015
6/6/2015
7/6/2015
8/6/2015
9/6/2015
10/6/2015
11/6/2015
12/6/2015
1/6/2016
2/6/2016
3/6/2016
Price in USD

What are people talking about?

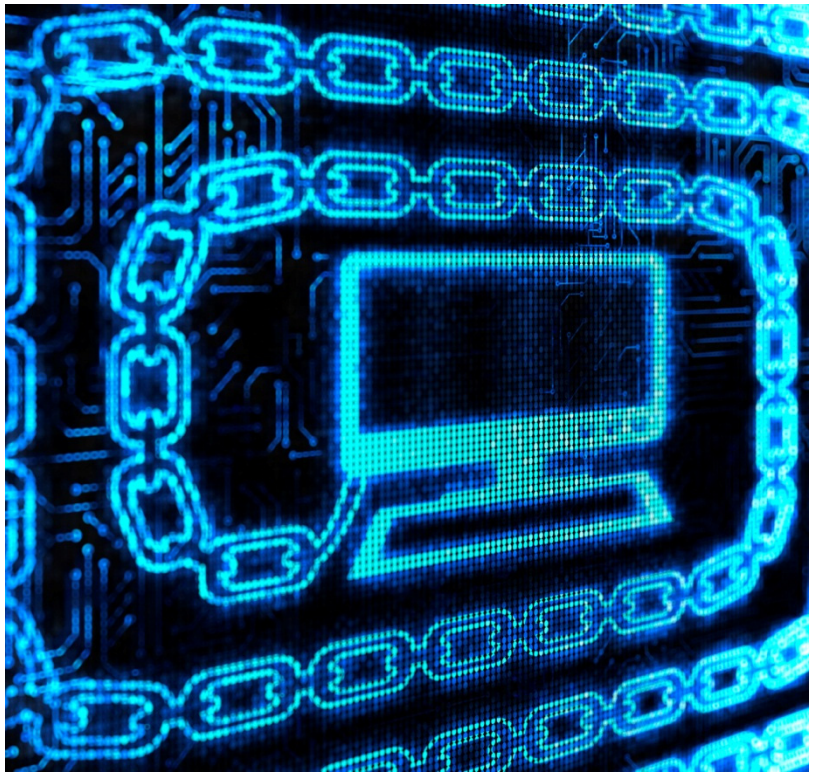
- Bitcoin Scaling
  - The system is running up against current capacities
  - Changes in the system require a near consensus
  - Differing opinions on how to scale the system up
  - A coming “Hard Fork”

What are people talking about?

- The Blockchain may persist, even if bitcoin doesn't
  - What does the blockchain offer outside of Bitcoin?
    - Securities Settlements
    - Foreign Exchange
  - Who can adopt blockchain technology?
    - Nasdaq
    - Banks
  - This is where the capital is going.

Blockchain

- 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.



What are people talking about?

- Governance
  - How does Bitcoin adjust to changes?
  - In consensus the right answer?
  - Can anonymous cryptocurrency exist with governance?

What are people talking about?

- Regulation
  - How do sovereign nations and states respond?
  - How will the internet be regulated?
  - What is Bitcoin to governing institutions?

What are people talking about?

- Can Bitcoin go “Mainstream”
  - Financial Tech firms are interested in becoming national banks
  - Currency exchangers are complying with anti-money laundering regulations
  - Transactions are moving to the “light” web.
  - Some Financial Tech firms are getting easier access to banking and capital

Bitcoin: Where it Goes

Stephen Clayton

Community Engagement Director

Federal Reserve Bank of Dallas

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.

What is a non-national currency?

- Not run through a central bank or government
- Not tied to national economic goals

Examples of non-national currency

- Eurozone
- Milltowns
- Prisons
- Internet

Who benefits?

- Unstable countries
- People with large multinational operations
- Internet based service providers

What are the risk?

- Not anchored in domestic economy
- If they are decentralized, no monetary oversight
- May not be regulated
- May not be trustworthy

Why would you want one?

- Exchange rate risk
- Ease of multi-national transactions
- Stability in unstable nations

Why wouldn't you want one?

- Lack of oversight can facilitate black markets
- Lack of regulation can allow for fraudulent systems
- Might not be a tangible asset

How does the internet fit in?

- Exists (for the most part) across borders
- Allows for transmission of services across borders
- Transfer information and opportunities to low cost producers

What is Bitcoin?

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

Where does Bitcoin fit in?

- "Native" currency to the internet
- Low-cost international payments
- "Anonymous"

What is Bitcoin's Future?

- Laid foundation for a secure non-national payment
- Pioneered the Blockchain
- Highlighted, in practice the advantages and risks
- Is beginning the address scalability

What is non-national currency's future?

- Some view as an inevitability
- National borders are already breaking down
- Globalization as a whole is progressing
- Resistance?

Bitcoin: How It Functions

Stephen Clayton

Community Engagement Director

Federal Reserve Bank of Dallas

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.

What is Bitcoin?

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

Bitcoin vs. bitcoins

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

Creating a currency from scratch

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

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

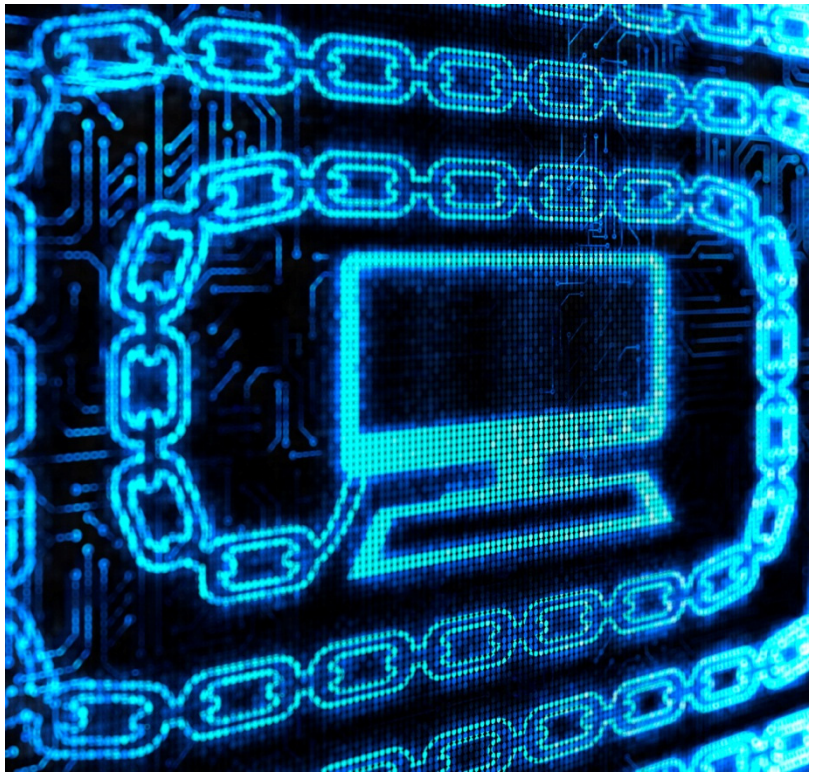
- If the money is just digital codes, why not copy and paste to make more money?
  - Timestamps
  - Hashes
  - Block chain

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

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.

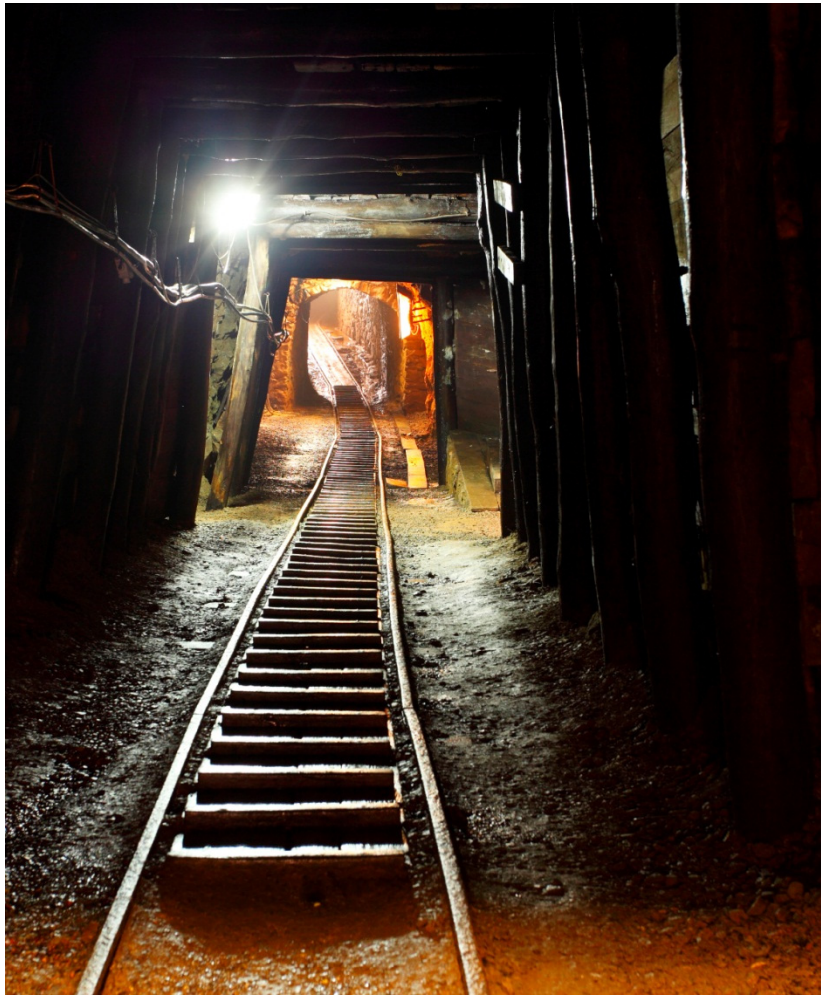


Where do bitcoins come from?

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

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.



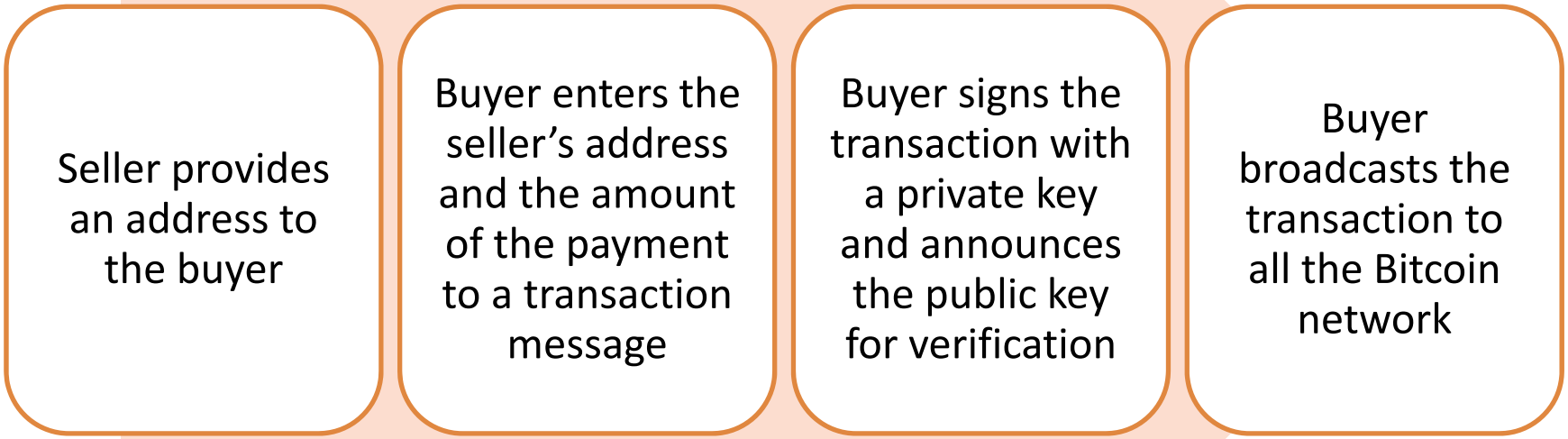
Mining bitcoins

- 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.

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?


1
2
2
3
2
SCARCE


$20!
$20!
$20!
1¢!
1¢!
1¢!
1¢!
UNIFORM


FIELD TRIP!
PORTABLE


LOOKIN' GOOD!
THANKS
DURABLE


GOT CHANGE?
WE ARE CHANGE!
DIVISIBLE


WANNA TRADE PLACES?
ACCEPTABLE