Cryptocurrency & The Blockchain

Matt Motherway

Why do we use money?

- transaction medium
- to store value
- to measure value

Properties

- Who issues the currency?
- Who accepts it as payment?
- Is there any instrinsic value? (e.g. can use it as something else or it's backed by gold)
- What's the cost of holding? Transacting?

Bitcoin

https://bitcoincore.org/bitcoin.pdf

A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto Jan. 3, 2009

Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the network.

Bitcoin uses public-key cryptography, peer-to-peer networking, and proof-of-work to process and verify payments. Bitcoins are sent (or signed over) from one address to another with each user potentially having many, many addresses. Each payment transaction is broadcast to the network and included in the blockchain so that the included bitcoins cannot be spent twice. After an hour or two, each transaction is locked in time by the massive amount of processing power that continues to extend the blockchain. Using these techniques, Bitcoin provides a fast and extremely reliable payment network that anyone can use.

- Bitcoin Transactions are:
  - **Permissionless and borderless**. The software can be installed by anybody worldwide.
  - **Do not require any ID to use**. Making it suitable for the unbanked, the privacy-conscious, computers or people in areas with underdeveloped financial infrastructure.
  - Are **censorship-resistant**. Nobody is able to block or freeze a transaction of any amount.
  - **Irreversible** once settled, like cash. (but consumer protection is still possible.)
  - **Fast**. Transactions are broadcasted in seconds and can become irreversible within an hour.
  - Online and available **24 hours a day, 365 days per year.**

- Stored Bitcoins:
  - Cannot be printed or debased. Only 21 million bitcoins will ever exist.
  - Have no storage costs. They take up no physical space regardless of amount.
  - Are easy to protect and hide. Can be stored encrypted on a hard disk or paper backup.
  - Are in your direct possession with no counterparty risk. If you keep the private key of a bitcoin secret and the transaction has enough confirmations, then nobody can take them from you no matter for what reason, no matter how good the excuse, no matter what.

Nearly all other digital currencies are centrally controlled. This means that:

- They can be printed at the subjective whims of the controllers
- They can be destroyed by attacking the central point of control
- Arbitrary rules can be imposed upon their users by the controllers

Being decentralized, Bitcoin solves all of these problems.

Unlike gold, bitcoins are:

- Easy to transfer
- Easy to secure
- Easy to verify
- Easy to granulate

Unlike fiat currencies, bitcoins are:

- Predictable and limited in supply
- Not controlled by a central authority (such as The United States Federal Reserve)
- Not debt-based

Unlike electronic fiat currency systems, bitcoins are:

- Potentially anonymous
- Freeze-proof
- Faster to transfer
- Cheaper to transfer

How do I get some?

Buy it with dollars or mine it.

Exchanges

https://www.coinbase.com/

https://www.gdax.com/trade/BTC-USD

https://gemini.com/

Mining

https://www.coindesk.com/information/how-bitcoin-mining-works/

People are sending bitcoins to each other over the bitcoin network all the time, but unless someone keeps a record of all these transactions, no-one would be able to keep track of who had paid what. The bitcoin network deals with this by collecting all of the transactions made during a set period into a list, called a block. It's the miners' job to confirm those transactions, and write them into a general ledger.

This general ledger is a long list of blocks, known as the 'blockchain'. It can be used to explore any transaction made between any bitcoin addresses, at any point on the network. Whenever a new block of transactions is created, it is added to the blockchain, creating an increasingly lengthy list of all the transactions that ever took place on the bitcoin network. A constantly updated copy of the block is given to everyone who participates, so that they know what is going on.

Learn Blockchains by Building One

https://hackernoon.com/learn-blockchains-by-building-one-117428612f46

- ported to node.js
- added a simple react ui
- todo: simulate larger network, add ledger & visualizations