Digital Currencies

Digital Currencies

- An “Internet-based medium of exchange”
- No need for a physical representation
- Allow for instantaneous and **borderless** transactions
- Digital Currencies can fall into several categories, including:
    - Virtual Currencies
    - Cryptocurrencies

Digital Currencies - Origins

- Started around the time of the Dot-com bubble in the 1990s
- E-gold was one of the first
  - 1996, Backed by gold
- Liberty Reserve
  - 2006, Allowed conversion from Dollars or Euros to Liberty Reserve Dollars or Euros
  - Shut Down by the US Government for money laundering
- Q (or QQ) Coin
  - A currency based in Tencent’s QQ messaging platform
  - So successful it had a traceable impact on the stability of the Chinese Yuan

Virtual Currency

- Virtual Currencies are Digital Currencies, not necessarily the converse
- Defined by the European Central Bank:
    - A digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.
    - Unregulated digital money, issued and controlled by its developers, and used and accepted among the members of a specific virtual community

Virtual Currency - Origins

- The name Virtual Currency has been in use since around 2009
- Closely tied to the growth of social gaming
- Officially accepted as the name by the US government in 2012-2013

Virtual Currency - Flow

- Closed Currency
    - Fictional Currency, no connection to the real economy
    - Currencies in games that cannot be purchased with real money, for example
- One Direction Flow
    - Currency that can be purchased with real money but not exchanged back
    - Originally coupons that came with a purchase, such as Post's one-cent-off coupons that came in cereal boxes in 1895
    - Microtransaction Currencies would be a more common example now
        - Facebook Credits, Microsoft Points

Virtual Currency - Flow

- Convertible Currencies
  - Can be bought with and sold for legal tender
  - Can be either centralized or decentralized

Virtual Currency as Currency

- Are virtual currencies legally recognized as currency?
  - Currency was defined in 2011 as anything that acts as legal tender and circulates “customarily”
- IRS treated many significant virtual currencies, including bitcoin, as property rather than currency for tax purposes

Centralized Virtual Currency

- Currency with a centralized repository, functioning as a central bank
    - Centralized administrative body
- Relies on confidence in a central authority

Decentralized Virtual Currency

- Currency with no centralized structure
  - No one officially regulating it
- Can be created by anyone with sufficient computational or manufacturing power
- Relies on a distributed system of trust
  - No person or organization to hold accountable
  - Sounds like a good idea, right?

Bitcoin

- Bitcoin was the first decentralized digital currency
  - Classic example of a cryptocurrency
  - Transactions secured and verified using cryptography
- Invented by an unidentified group known as Satoshi Nakamoto
  - Introduced originally in October, 2008, released in 2009
- Currency based entirely on its own ledger
  - A cryptographically secured history of transactions known as the Blockchain

Bitcoin - The Blockchain

- A distributed database recording every bitcoin transaction ever made
  - Consists of blocks, containing timestamps and a link to a previous block
- The Blockchain is the core of bitcoin
  - To keep it secure, the blockchain is constantly verified and added to with a process called mining

Bitcoin - Mining

- In order to maintain security, new blocks must contain a proof-of-work before being added to the blockchain
  - Miners must find a “nonce”, a number such that when the block is hashed with the nonce, the result is smaller than the network’s difficulty target (using SHA-256)
  - The bitcoin network updates its difficulty target roughly once every 2 weeks to keep the time between bitcoin creation roughly 10 minutes
- The proofs created by miners are easy to verify, but take extremely long to produce
  - In March, 2015, the number of nonces miner’s had to attempt was about 200.5 qunitillion per block

Bitcoin - Mining Pools

- Seeing as the amount of work to mine a single block is unfeasibly high for a single person, mining pools formed
  - Shared computational power to try to mine a block, distributing the resulting bitcoins to all those involved in the mining
- Allowed for more consistent income without necessarily earning less than if you mine a block on your own

Bitcoin - Supply

- Where do the bitcoins come from?
  - Mining a block technically simply secures and verifies all the transactions the block represents
- When a block is created, a special coinbase transaction is included, granting some amount of bitcoins plus all the transaction fees encoded in the block to the miner who created it
  - As of July 2016, this amount was roughly 12.5 bitcoins plus the transaction fees

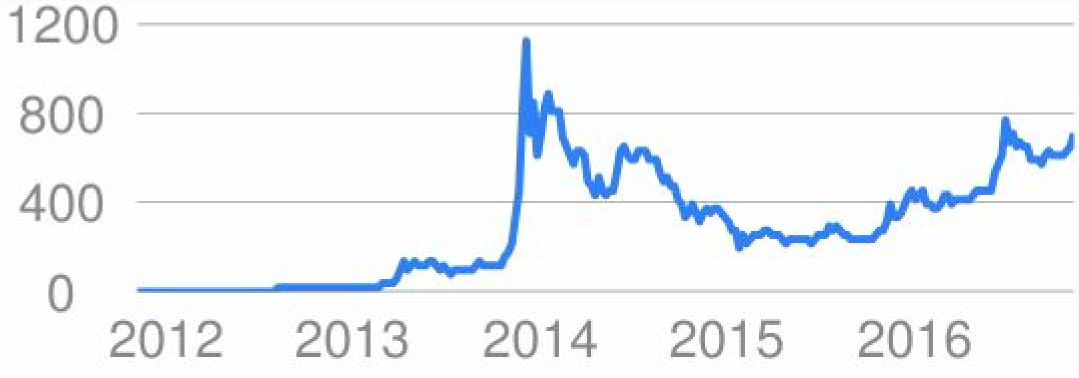
Bitcoin

- The reward in this coinbase transaction changes, such that it halves every 210,000 blocks (roughly 4 years)
  - This means the introduction of new bitcoins will eventually reach 0, and there is a set upper limit on possible bitcoins (about 21 million)
- These bitcoins will eventually be stored in wallets
  - Since bitcoins don't exists outside of unspent transaction results in the leger, all a wallet is is a private key that can sign the transaction of a specific amount of bitcoin
  - Basically the leger says "This person (with this private key) recieved X amount of bitcoins"
  - That private key is necessary to verify any transaction spending those bitcoins, so knowing that key is equivalent to owning the bitcoins

Bitcoin - Economic Value

- Bitcoin as a currency is secure, but its economic value is based entirely on what people are willing to exchange for it
  - There is no centralized authority that can guarantee some service or good in exchange for bitcoins
- This dependence makes the value of bitcoins unstable

Bitcoin - Value over time



Notable Points:

- https://en.wikipedia.org/wiki/History_of_bitcoin
- Huge fluctuation