Why is money useful?
Why is money useful?

avoid *double coincidence of wants*

Important properties
Important properties

• Divisible
• Storable
• Exchangeable
• Hard to fake
• Sustains its value

Gold standard vs Fiat currency
Gold standard

• First gold coins minted around 610 BC. Why gold?

• Later: paper currency. Countries adopt “gold standard” in 1800s to build trust

• But pressure in wars (sell gold, want to print money).

• *Bretton Woods System* 1946 (DM -> USD -> Gold); collapsed during Vietnam war

• Swiss Franc on gold standard until 2000
Fiat currency

• “fiat” = “let it be done”
• Government declares it to be a legal medium of exchange
• Value unrelated to any physical quantity
• Originated in 11th Century China

(Wikipedia)
Pros and Cons?

Electronic Currency
Electronic Currency

- Lower transaction fees
- Privacy
- No government interference

The challenge

Money = Bits

How to prevent
  - Double spending
  - Copying
A brief detour into iOwe

The iOwe Protocol

- Domain with a common unit of value (e.g., my car for one hour; KB of download)
- iota = “I owe to anyone”
- Can be exchanged
- A can sign an iota to B, B can sign this onto C, C can later redeem with A
Attacks?

• Whitewashing by A
  – Need to first earn trust through barter
• Double spending by B: B-> C and B->D
  – A could propagate “proof of misbehavior”
     (grim trigger!)
• B -> sybil -> double spend
  – need chain-of-trust
• A refuses to provide resource ("step omission")
  – allow C to complain; grim-trigger

Attacks?

• Whitewashing by A
  – Need to first earn trust through barter
• Double spending by B: B-> C and B->D
  – A could propagate “proof of misbehavior”
     (grim trigger!)
• B -> sybil -> double spend
  – need chain-of-trust
• A refuses to provide resource ("step omission")
  – allow C to complain; grim-trigger (threats)
Summary: iOwe

- Uses PK/SK to support the transfer of an iota “coin”
- Copying, double spending possible, but would be eventually caught.
- Anyone can print a their own coin 😊

But, does not satisfy many properties. Fails:
- Not very exchangeable
- Does not sustain value
- Not trusted (barter initially)
Bitcoin

• Launched Jan 3 2009 by Satoshi Nakamoto

• Liquid: can convert USD <-> BTC on exchanges
• Transfer BTCs to anyone with a public key

• Key innovation: a trusted, shared ledger of all transactions.
Bitcoin Properties

- Fiat currency
- Total number of coins bounded, rate of new coin printing controlled
- Coins can be copied. But ledger system prevents double spending.
  - 1 BTC = US$2.33 (2011)

- $76 (2013)
Bitcoin Properties

• Fiat currency
• Total number of coins bounded, rate of new coin printing controlled
• Coins can be copied. But ledger system prevents double spending.
  • 1 BTC = US$2.33 (2011)
  • $76 (2013)
  • $420 (2014)
  • $221 (2015)
Bitcoin Properties

• Fiat currency
• Total number of coins bounded, rate of new coin printing controlled
• Coins can be copied. But ledger system prevents double spending.
  • 1 BTC = US$2.33 (2011)
  • $76 (2013)
  • $420 (2014)
  • $221 (2015)
  • $424 (2016)

Basic idea

• Entries in distributed ledger system costly to make, costly to change
• Makes the system hard to attack
• Workers (“miners”) are paid to do the work to maintain the ledger
• Anyone can check ownership of a coin; transfer of a coin
Main components

- **Transaction**: Transfer of currency, recorded as entry in block chain (ledger)
- **Block**: A page in the ledger
- **Block chain**: A book
- New blocks created by **miners**

Bitcoin Charts

- [https://blockchain.info/charts](https://blockchain.info/charts)
A Transaction

Transactions

A

Transaction

Owner 1’s Public Key

Hash

Owner 0’s Signature

Owner 1’s Private Key

B

Transaction

Owner 2’s Public Key

Hash

Owner 1’s Signature

Owner 2’s Private Key

C

Transaction

Owner 3’s Public Key

Hash

Owner 2’s Signature

Owner 3’s Private Key

(Nakamoto ’08)
The Block Chain
Costly to make a new block

• Have to find a nonce that creates a hash with $l (=17$ currently) leading 0’s
  – Adjusted to keep rate approx every 10 mins
• Success: generate block, add to chain, claim 25 BTCs as payment
• Every 210k blocks (~4yrs), payment halved
• Limit of 21 million coins
• Blocks that don’t follow rules are rejected
Handling Forks

• If two users generate a block at around same time, block chain may fork
• Workers will extend the first block they hear about
• Later, resolve fork by preferring longer chain (TXs in other chain then invalid)
  • [Fall’11] 154,358 blocks.
  • [Spring’13] 230,437 blocks
  • [Spring’14] 296,138 blocks
  • [Spring’15] 352,217 blocks
  • [Spring’16] 470,000 blocks

Trust

• Alice pays Bob. Tx recorded in Block. Bob gives Alice the goods or services.
• Alice tries to make two blocks quickly, before next block on main chain
  – If succeeds, the transfer to Bob is removed and Alice can spend the BTCs again
  – Even with 50% of compute power, roughly prob 1/2 * 1/2 = 1/4 to succeed
• Bob can wait for more blocks to be added to the main block chain to be more secure
Important properties of currency

• Divisible
• Storable
• Exchangeable
• Trusted (no fakes, no double spending)
• Value sustained (control on money printing)

Future incentive concern?

• By 2140 no new mining of coins
• Will need to use transaction fees to motivate mining
• May be an issue with miners not sharing information about transactions
Bitcoin Incidents

• 9/20/10: Flooding of small (sub 0.01 transactions). DoS.
• 8/15/10: Block 74,638 problem
  – Tx creating 184B bitcoins
  – Overflow problem with code used to check Txs
  – Good chain took over by block 74691
• 9/29/10: DoS attack on signature verification
• 3/13/13: 24 block bitcoin form

Mt. Gox exchange incident

• 2013 handled 70% of exchange.
• Suspended trade, June 20 2013.
• “lost” 744,408 bitcoins…
Infrastructure Problems (2013)

• Wallet attacks
• Exchanges going down
• Bubble?
  – European bank crisis
    • E.g., Cyprus Friday 3/15
    • Tue 3/19 1 BTC = $47
    • Sat 3/23 1BTC = $72
• By end of 2013 up to $1000!

Problems in 2014

• MtGox Collapse
• Government policies
  – Constitution gives Congress and Treasury right as sole producer of legal tender in US
  – FinCEN ruling (Spring 2013)
    • Bitcoin is not money; it is a decentralized virtual currency
    • Require “miners” and exchanges to register as “Money services businesses”
    • Later ruling that Bitcoin is property
Broader concerns

- Silkroad marketplace (shut down)
- Money laundering
- Concentration of miners (may have power to threaten to shut down)

Discussion

- Deflation? 2140 no more coins minted.
- Build contract technology onto the Blockchain.
- ASICs; concentration of miner power
- Litecoin, Dogecoin
  - http://en.wikipedia.org/wiki/Dogecoin (block time 1 min; no limit to # new coins)
  - http://en.wikipedia.org/wiki/Litecoin (block time 2.5 mins; limited # coins; memory hard computation to prevent concentration; new arms race)