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); system 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)
Gold vs Fiat: Pros and Cons?

Digital Currency
Why Digital Currency?

• Lower cost
• Resilience (no government interference)
• Can control money supply

The Challenge

Money = Bits

How to prevent
  • Copying a coin, and double spending
  • Money printing
A brief detour into iOwe

The iOwe Protocol

- Domain with a common unit of value (e.g., a vehicle-hour; a MB of download)
- *iota* = “I owe to anyone”
- Iotas can be exchanged
- **A** can sign an iota to **B**, **B** can sign this onto **C**, **C** can later redeem with **A**
Attacks on iOwe

In context of an I_A and transfer chain: A-> B->C

• Whitewashing by A
  – PYDs (*earn trust upon entry through barter*)
• Double spending an I_A by B: B->C and B->D
  – A could propagate “proof of misbehavior”
    (grim trigger on B!)
• But what about: B -> sybil -> double spend
  – need a *chain-of-trust*
• A refuse to honor I_A (a “step omission”)
  – allow C to complain (grim trigger on A!)
Summary: iOwe

- Uses public key infrastructure to support the transfer of an *iota* (a “coin”)
- In effect, anyone can print a their own coin 😊.
  - only valuable if your iota becomes a trusted currency.
- Double spending is possible, but would be eventually caught.

Some undesirable properties:
- hard for IOUs to be readily *transferable*
- hard for IOUs to *sustain value*
- needs *trust along a chain of transfers* (with *barter* to build initial trust)
Bitcoin

• Launched Jan 3 2009 by Satoshi Nakamoto

• Liquid: can convert USD <-> BTC on exchanges
• Can 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)

• 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)

Altcoins

https://coinmarketcap.com/
Bitcoin overview

• Entries in distributed ledger system are costly to make, costly to change.
• This makes the ledger hard to attack. Anyone can check ownership of a coin.
• Workers (“miners”) are paid in coins to do the work to maintain the ledger.
The blockchain

- **Transaction**: A transfer of coins, recorded as an entry in the ledger.
- **Block**: A page in the ledger, containing records of multiple transactions (<= 1MB)
- **Block chain**: The entire ledger. Puts an ordering on transactions.
- New blocks are created by **miners**.

- [http://blockchain.info/charts](http://blockchain.info/charts)
The Bitcoin network

- Nodes “gossip” new Tx data (when it is valid)
- Some nodes are miners, try to form new blocks that contain transactions
- Nodes “gossip” new blocks.

Structure of the Block chain

- Valid block must have a nonce that gives a hash with at least 18 leading 0s

![Diagram of block structure]

- [https://blockexplorer.com/](https://blockexplorer.com/)
Proof-of-work

- Find a nonce that creates a hash of the block with 18 (currently) leading 0s
  - adjusts to have ~10 mins rate of mining
- Can generate a block, add to head of the chain, print 12.5 coins (and collect fees).
- Every 210k blocks (~4yrs), payment halved. Limit of 21 million coins.
- A block must follows rules to be valid.

Handling Forks

- Block chain may accidentally fork if two miners add a block at the same time; OR if the community decides to implement a “hard fork.”
- Protocol for an accidental fork:
  - Miners work to extend the longer chain, also preferring to work on the first new block they hear
  - Eventually the accidental fork is resolved and consensus forms on one chain.
Trust properties of Bitcoin

• Alice pays Bob. Bob sees Tx on the blockchain, gives Alice the items.

• Alice tries to make 2 blocks quickly, and overtake, forking the block with her Tx.
  – If succeeds, Tx disappears from ledger and Alice can spend the coins again.
  – But even with 50% of compute power, Alice will only succeed with $\sim \text{prob} 0.25$
  – Bob gains an exponential advantage by waiting for $k > 1$ blocks (“confirmations”)

Important properties of currency

• Divisible
• Storable
• Exchangeable
• Trusted (no fakes, no double spending)
• Value sustained (control money printing)
Future incentive concern?

• By 2140 no new mining of coins
• Will need to use transaction fees to motivate mining (fees already important, ~$6/transaction as of 2017.)
• A related concern is that miners may not share information about transactions

Bitcoin Incidents

• 9/20/10: Flooding of small (sub 0.01 transactions); a denial of service attack
• 8/15/10: Block 74,638 problem
  – Tx creating 184B bitcoins
  – Overflow problem with code that checks Txs
  – A “good chain” took over by block 74,691
• 9/29/10: A DoS attack on signature verification
• 3/11/13: a 24 block accidental fork, caused by update to bitcoin mining software
Mt.Gox exchange (2011-14)

- 2013 handled 70% of exchange.
- Suspended trade, June 20 2013.
- “lost” 744,408 bitcoins...
- Collapsed in 2014

Infrastructure Problems (2013)

- Wallet attacks
- Exchanges going down

<table>
<thead>
<tr>
<th>Date</th>
<th>Site</th>
<th>Theft amount (BTCs)</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2011</td>
<td>User: Allinvain</td>
<td>25,000</td>
<td>wallet account attack</td>
</tr>
<tr>
<td>March, May 2012</td>
<td>Bitcoinica</td>
<td>61,500</td>
<td>exchange</td>
</tr>
<tr>
<td>Sep 2012</td>
<td>Bitfloor</td>
<td>24,000</td>
<td>exchange</td>
</tr>
<tr>
<td>Oct 2013 (twice)</td>
<td>inputs.io</td>
<td>4,100</td>
<td>wallet</td>
</tr>
<tr>
<td>Dec 2013</td>
<td>Sheep</td>
<td>5,400</td>
<td>marketplace</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>Mt Gox</td>
<td>~ 850,000</td>
<td>exchange</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>Silk Road 2</td>
<td>~ 4,300</td>
<td>marketplace</td>
</tr>
<tr>
<td>Jan 2015</td>
<td>Bitstamp</td>
<td>~ 19,000</td>
<td>exchange</td>
</tr>
<tr>
<td>Aug 2016</td>
<td>Bitfinex</td>
<td>~ 120,000</td>
<td>exchange</td>
</tr>
</tbody>
</table>
US Government actions

• Constitution gives Congress and Treasury right as sole producer of legal tender
• FinCEN ruling (Spring 2013)
  – Bitcoin is not money; it is a decentralized virtual currency
  – Require miners and exchanges to register as money services businesses
• FinCEN ruling (Spring 2014)
  – *Bitcoin is property*

Broader concerns

• The Silkroad marketplace (shut down; money laundering
• Concentration of miners (may have power to threaten to shut down)
• By 2140 no more coins minted. Deflationary?
• Are we in a bubble?
  – *European bank crisis*. Cyprus banking system--from Tue 3/19 to Sat 3/23 rate changed from $47 to $72. $1000 by end 2013. [Coda: Nov 2017, at $6552]
Bitcoin forks (1 of 3)

<table>
<thead>
<tr>
<th>Date</th>
<th>Fork Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 1, 2017</td>
<td>Bitcoin cash (BCH)</td>
<td>Change block size from 1MB to 8MB. Promote “ecash” not “settlement layer.” $19B market cap as of Nov 2017.</td>
</tr>
<tr>
<td>Oct 24, 2017</td>
<td>Bitcoin gold (BTG)</td>
<td>Create “ASIC resistant” bitcoin. Change the cryptotechnology, promote mining on GPUs. $2.7B market cap as of Nov 2017.</td>
</tr>
</tbody>
</table>
Bitcoin forks (3 of 3)

• SegWit2x, scheduled for this Thursday (11/16/17), but called off on Wed 11/8. Plan had been:
  – Go from 1MB to 2MB block size over ~3 months
  – Remove signatures from transactions, handle them in a “segregated witness” hash structure

• Pros: reduce fees, more Txs per block (although some argue the development of ‘fee market’ is good)

• Cons: forks are dangerous, no block size is big enough, network nodes become more costly because need to store entire chain (and thus, push to more centralization).

Altcoins

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Litecoin</th>
<th>Dogecoin</th>
<th>Ethereum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch date</td>
<td>2009</td>
<td>2011</td>
<td>2013</td>
<td>2015</td>
</tr>
<tr>
<td>Market cap (Aug 2016)</td>
<td>US $9.3 B</td>
<td>US $172 m</td>
<td>US $24 m</td>
<td>US $935 m</td>
</tr>
<tr>
<td>Currency</td>
<td>Bitcoin (BTC)</td>
<td>Litecoin (LTC)</td>
<td>Dogecoin (DOGE)</td>
<td>Ether (ETH)</td>
</tr>
<tr>
<td>proof-of-work</td>
<td>SHA-256</td>
<td>scrypt</td>
<td>scrypt</td>
<td>Ethash</td>
</tr>
<tr>
<td>Supply</td>
<td>Deflationary</td>
<td>Deflationary</td>
<td>Inflationary</td>
<td>Inflationary</td>
</tr>
<tr>
<td>Currency cap</td>
<td>21 m</td>
<td>84 m</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Max block size</td>
<td>1 MB</td>
<td>1 MB</td>
<td>1 MB</td>
<td>n/a</td>
</tr>
<tr>
<td>Block generation time</td>
<td>10 min</td>
<td>2.5 min</td>
<td>1 min</td>
<td>15 sec</td>
</tr>
<tr>
<td>New coins per block</td>
<td>12.5 f</td>
<td>25 f</td>
<td>10,000</td>
<td>5</td>
</tr>
<tr>
<td>Exchange rate (Aug 2016)</td>
<td>US $585</td>
<td>US $83.65</td>
<td>US $0.00023</td>
<td>US $11.2</td>
</tr>
</tbody>
</table>

• Proof-of-work in these new coins is memory based (making ASICs less easily designed…)

• Ether has faster generation time, no limit on block size.
Ethereum

- 2nd largest coin by market cap ($30B vs $20B Bitcoin cash, $109B Bitcoin)

Ethereum Charts

- A “World computer”: nodes can be programmed to step through a scripting language
- Have a decentralized computer that can run programs. Instructions are paid “gas” (=10^{-5} Ether); e.g., addition is 3 gas, multiplication is 5 gas.
- Facilitates smart contracts; e.g., “pay Dad when Mom says I used car.” Build “distributed autonomous organizations.”
Etherereum

- A “World computer”: nodes can be programmed to step through a scripting language
- Can run programs. Instructions are paid “gas” (=10^-5 Ether); e.g., addition is 3 gas, multiplication is 5 gas.
- Facilitates smart contracts; e.g., “pay Dad when Mom says I used car.” Build “distributed autonomous organizations.”
- Caution: The DAO June 17 2016 attack. 3.6m Ether transferred to a “child DAO.” Loophole in code.
  - This caused a July 20, 2016 hard fork, reverting Ether back to original owners. Ethereum Classic remained ($1.5B cap).

Other uses of Blockchain

- Seems to have potential (a trusted way to transact)
- But one issue is the “gateway problem” (getting things to trade onto the block chain).