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”

• Traditionally: Government declares 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
- Cannot be stopped (send anywhere)
- Can control money supply
- Transact via code
- Private

The Challenge

Money = Bits

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

The iOwe Protocol

- *iota* = “I owe to anyone” e.g., bandwidth, miles, etc.
- iotas can be exchanged
Cryptography: Review

• Public-key infrastructure
  – Public key $PK_A$, secret key $SK_A$
  – $SM = \text{Sign}(X)_{SK_A}$: hard to spoof
  – $\text{Verify}(SM, X, PK_A) = T/F$

• Cryptographic hash function
  – One way function
  – $Y = \text{Hash}(X)$
  – Cannot go from $Y$ to $X$

The iOwe Protocol

• *iota* = “I owe to anyone” e.g., bandwidth, miles, etc.
• Iotas can be exchanged
• A can sign an iota to B, B can sign this onto C, C can later redeem with A
iOwe: Generate Credit

• User A can issue IOU “A -> B”

• Generate iota
  • \( I = (A, \text{resource}, \text{exp-time}, nonce) \)

• Generate promise to B:
  • \( I_{AB} = \text{Sign}(I, PK_B)_{SK_A} \)

• Anyone can verify

iOwe: Redeem Credit

• B can now spend with A
  • \( \text{Sign}(I_{AB}, PK_A)_{SK_B} \) to prove identity
    – “Hey, you said you’d do work for me!”

• A can check they created \( I_{AB} \), and not yet been spent
iOwe: Transfer Credit

• B can also spend with C
• Transfer the promise from A:
  – \( I_{AC} = \text{sign}(I_{AB}, PK_C)_{SK_B} \)

iOwe: Redeem Credit

• C can now spend with A
• \( \text{sign}(I_{AC})_{SK_C} \) to prove identity
  – “Hey, you said you’d work for B, and B said they’d let you work for me instead!”
Attacks on iOwe

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

- Whitewashing by $A$
  - need to 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 “chain-of-trust” for transfers
- $A$ can refuse to honor $I_A$
  - $C$ can complain (grim trigger on $A$!)

Summary: iOwe

- PKI to support creation and transfer of an *iota* (a “coin”)
- Money printing encouraged. Anyone can have their own coin!
- Double spending possible, eventually caught
  
  • But, needs **trust** along a chain of transfers, and barter to **build initial trust 😊**
Bitcoin

• From: Satoshi Nakamoto <satoshi <at> vistomail.com>
  Subject: Bitcoin P2P e-cash paper
  Newsgroups: gmane.comp.encryption.general
  Date: Friday 31st October 2008 18:10:00 UTC

  “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

May 22, Bitcoin Pizza Day

• May 18, 2010 Laszlo Hanyecz on bitcointalk.org:
  "I'll pay 10,000 bitcoins for a couple of pizzas"
• May 21, 2010 "So nobody wants to buy me pizza? Is the bitcoin amount I'm offering too low?"
• May 22, 2010 "I just want to report that I successfully traded 10,000 bitcoins for pizza...Thanks jercos!"
A New Layer? Programmable Transactions

- 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)
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)

Market cap, various coins

https://coinmarketcap.com/
As The Bitcoin Price Plummets, Its Dominance Is On The Rise

Bitcoin has had a terrible month, but not as bad as many other major and minor cryptocurrencies. It would seem, with bitcoin’s share of the total cryptocurrency capitalization, known as its dominance, moving higher throughout November.

The bitcoin price has fallen some 45% so far this month after rival cryptocurrency, bitcoin cash, split in two due to developers and miners failing to reach an agreement over its future, triggering a cryptocurrency sector-wide sell-off that has caused some to question bitcoin’s chances of survival.

Bitcoin’s dominance has ticked up over the course of the month, however, from lows of 51% in early November to 53% today—highlighting bitcoin’s enduring appeal to investors and cryptocurrency miners.

---

**Bitcoin overview**

- Entries in distributed ledger system are costly to make, costly to change.
- Makes 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 Bitcoin Blockchain

- **Transaction**: A transfer of coins, recorded as an entry in the ledger.
- **Block**: A page in the ledger, containing records of transactions (<= 1MB)
- **Block chain**: The entire ledger. Puts an ordering on transactions.
- New blocks are created by **miners**.
- If a Tx not in blockchain it is unconfirmed
- [http://blockchain.info/charts](http://blockchain.info/charts)
The Bitcoin network

- Nodes “gossip” new transactions
- Miners try to form blocks that contain transactions, suggest new blocks to the rest of the network
- If the block is valid, then nodes “gossip” the new block

Structure of the Block chain

- At present, valid block must have at least 18 leading 0s
Proof-of-Work

• Find *nonce* that hashes block to 18 zeros
  – Difficulty adjusts to ~10 mins/block
• A valid block (follows rules) can be added to the head of the chain
• Get to print 12.5 coins, and collect transaction fees
• Every 210k blocks (~4yrs), payment halved. Next time is May 2020.
• Limit of 21 million coins

Structure of the Block chain

• At present, valid block must have at least 18 leading 0s

*https://blockexplorer.com/*
Double spending attack?

• Alice pays Bob
• Bob sees bitcoin Tx on the blockchain, gives Alice the items.
• Alice makes 2 blocks quickly, forking chain
  – Tx no longer on consensus chain, can spend coin again
  – Even with 50% of compute power, Alice will only succeed with ~ prob 0.25
  – Bob gains an exponential advantage by waiting for $k > 1$ blocks (“confirmations”)

Branches

• May also be accidental branches
• Bitcoin consensus protocol:
  – Miners extend the longer chain, accept first new block they hear
  – Eventually the fork is resolved, consensus forms on one chain
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, ~$0.50/transaction as of 2017).
• Tragedy of commons? Will transactions move to “sidechains”?
A Concern: Mining Pools

- One computer takes several years to solve a block
- For more steady income, join groups, form pools, collectively work to solve blocks
- Distribute rewards
- Leads to concern about chain instability
Forks; Collective Action

• Protocol needs to be updated from time to time (bugs, larger blocks, etc.)

• Soft fork: old nodes still recognize new transactions

• Hard fork: need to update software to be able to recognize new txs
  • Literally “forks” the blockchain

Hard forks: BCH; BTG


Security Vulnerabilities

- 9/20/10: Flooding of small (< 0.01 BTC) transactions; denial of service attack
- 8/15/10: block 74,638
  - 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

• June 19, 2011. Exchange hacked. BTC/USD rate fell to US 1c.
• 2013 handled 70% of BTC/USD exchange.
• Suspended trade, June 20 2013.
• “Lost” 744,408 BTC
• Collapsed in 2014
Additional Infrastructure Problems

• 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>

U.S. Government Actions

• U.S. Constitution makes Congress and Treasury the sole producer of legal tender

• FinCEN ruling (Spring 2013)
  – Bitcoin is a decentralized virtual currency
    • Miners, exchanges need to register as money services businesses

• FinCEN ruling (Spring 2014)
  – Bitcoin is property
Broader concerns

• Illegal transactions, money laundering (e.g., The Silkroad marketplace)
Bitcoin: The Essence of a Bubble

Source: Jeremy Grantham based on data from Philip Pilkington
Hash Rate and Energy Expenditure (Log Scale!)

Energy Expenditure
- 200 million Kwh/day
  - 7 million U.S. homes
  - Austria

How to elect a leader without PoW?

- Leaders gain profit (block rewards, fees, censor enemies?)
- Need to commit something of which there is a limited quantity, else will make Sybil accounts
- For example:
  - Computational power
  - Coins in escrow
Proof of Stake

- No mining cost
- Leader candidates commit some stake, form a committee
- Randomized, weighted election
- Leader proposes new block, a committee votes on validity
- If bad stake, then stake is “slashed”. Need some committee members to be honest
- Versions beginning to be seen (Dash, NEO, Tezos; Casper)

Ethereum

- 3rd largest coin by market cap ($11B vs $64B BTC, $14B Ripple)
- A “World Computer”
- Source of ERC-20 tokens
- ICOs
- dApps
- Smart contracts
- …
Etherereum

- Normal accounts, and smart-contract accounts (contain code, key-value storage, hold ETH)
- Code can send ETH to other accounts; read/write; expose APIs; call APIs of other contracts
- Commit to code
- Ethereum provides a virtual machine; “mining” involves running scripts and writing to blocks
- Instructions paid for in “gas”; e.g., addition is 3 gas, multiplication is 5 gas.
- In place of Tx fees, bid a “gas to ETH rate”

Create a Contract

- Submit Tx to blockchain:
  - To: empty
  - Value: ETH value
  - Data: code of contract
  - Gas
  - Signature
- If succeed, Ethereum returns the address of the new contract
- Enables smart contracts (e.g., “pay Dad when Mom says I used car.”)
Augur: Prediction Market

- ERC-20 tokens, ICOs

Other dApp Examples

- EOS ($2.6B cap).
  - Building a network that can utilize inter-blockchain communication

- TRON ($750M cap).
  - Open source protocol for the digital entertainment industry

- VeChain ($233M cap).
  - An enterprise-level public blockchain platform, with IoT integration.
Caution: The 2016 DAO attack

• The DAO was a kind of VC

• June 17 2016
• 3.6m ETH transferred to a “child DAO.”
• Loophole in code.
• Led to a July 20, 2016 hard fork, reverting ETH back to their original owners.
• Ethereum Classic remained ($454M cap).