Just NOT a guide for investment

Lecture 11 Blockchain and Bitcoin

7 Dec 2017

Yang Ye
MFE FE8828

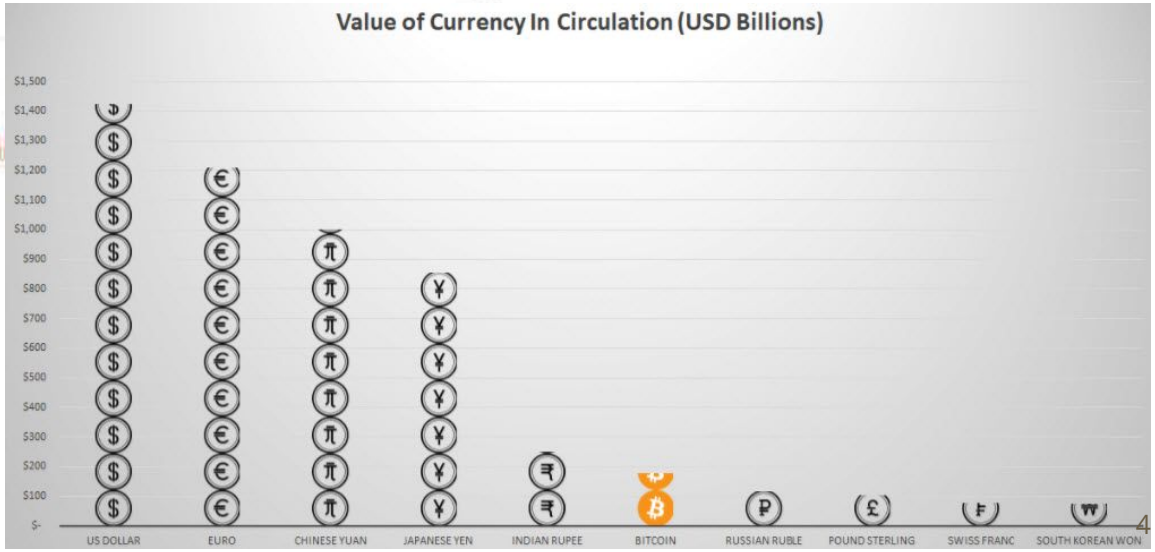
Since Jan this year, I have been collecting news for Bitcoin

- I imagined what to come by the end of the year when the courses starts.
- Bust? Boom?
- “We have known the beginning but never guessed about the future.”
- Anything but just pales to recent movement.

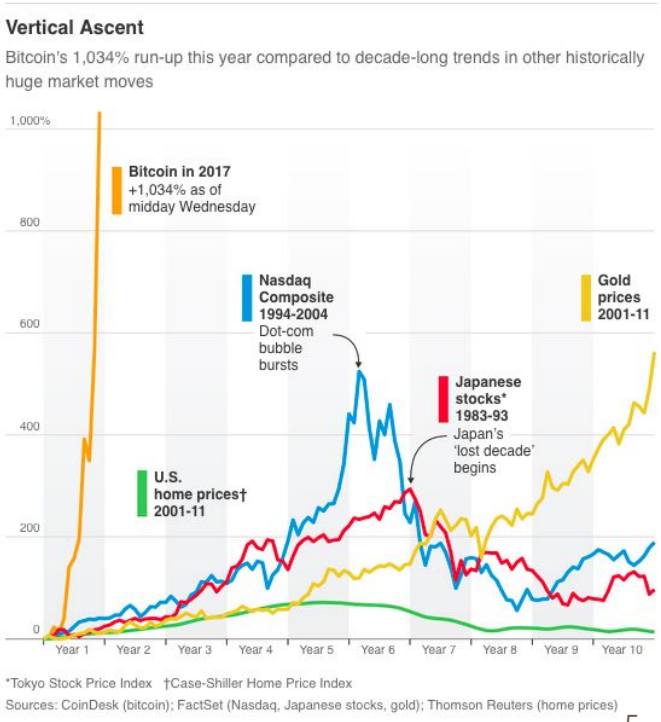
2017-11-29, Bitcoin > 10k

https://www.bloomberg.com/news/articles/2017-11-29/for-bitcoin-skeptics-the-question-is-what-will-pop-this-bubble

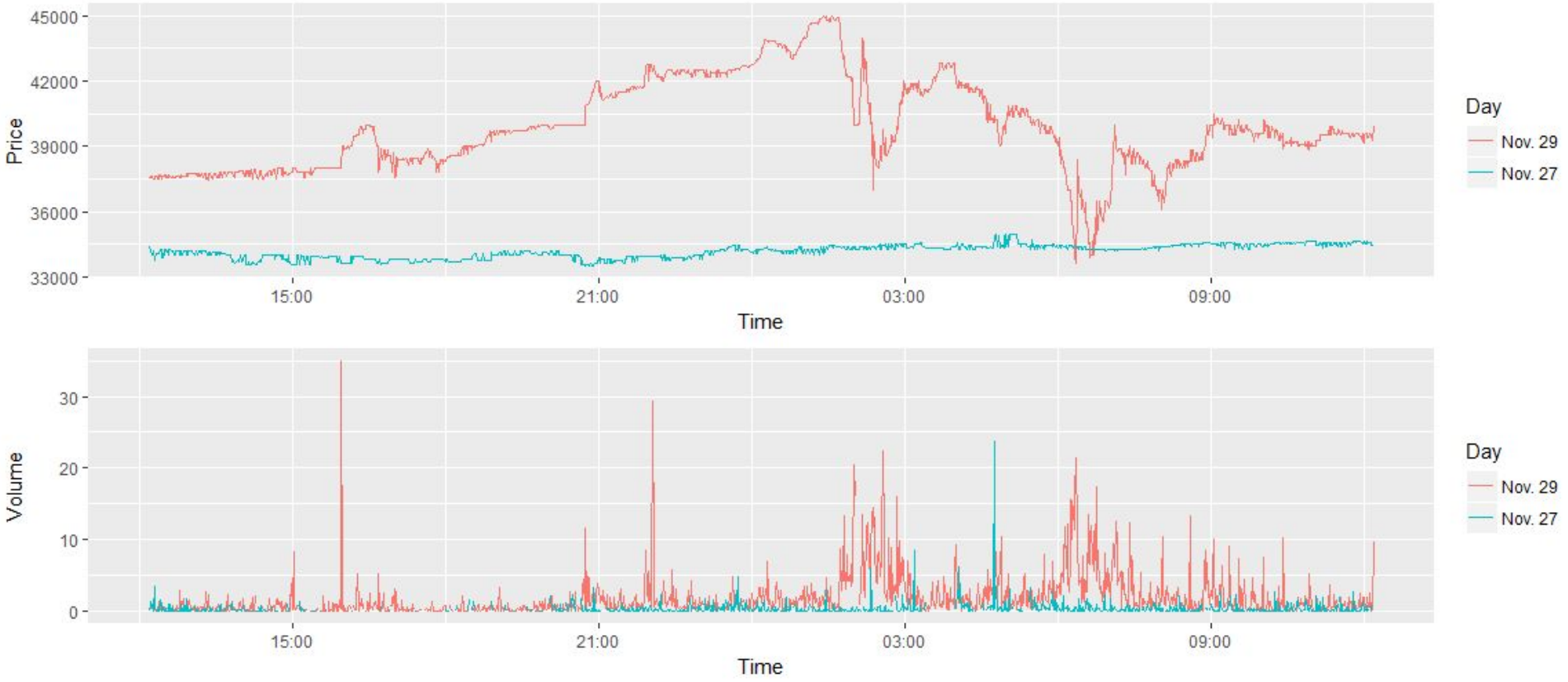
B$: Sixth largest currency in the world.



Bitcoin had, by all accounts, a remarkably volatile week, losing $3 bln in market cap in just 90 minutes as the price slid from $11,400 to close to $9,000 (on some exchanges it flash-crashed to the low $8,000s). Nevertheless, within 36 hours, the cryptocurrency has rebounded to over $11,000.



2017-11-29, a volatile day for Bitcoin ever since. Below is in Brazil Rs. About 4:1 to USD.



???

ʃʃʃ

???

ʃʃʃ


How Newton's fortune fell to earth
South Sea Company share price
£
1,000
800
600
400
200
0
Newton re-enters with a lot
Newton's friends get rich
Newton exits happy
Newton invests a bit
Newton exits broke
1718
1719
1720
1721
Source: Marc Faber, Gloom Boom Doom

What is it?

- **Bitcoin** is a peer to peer electronic cash system.
- **Blockchain** is a type of distributed ledger created to trace the use of a decentralized application.
- **Mining** is the process of creating new coins in exchange for validating the ledgers and verifying their accuracy.
- **Cryptocurrency** refers to any of the coins being created to incentivize the mining for various blockchains and their corresponding applications.

Some cryptography

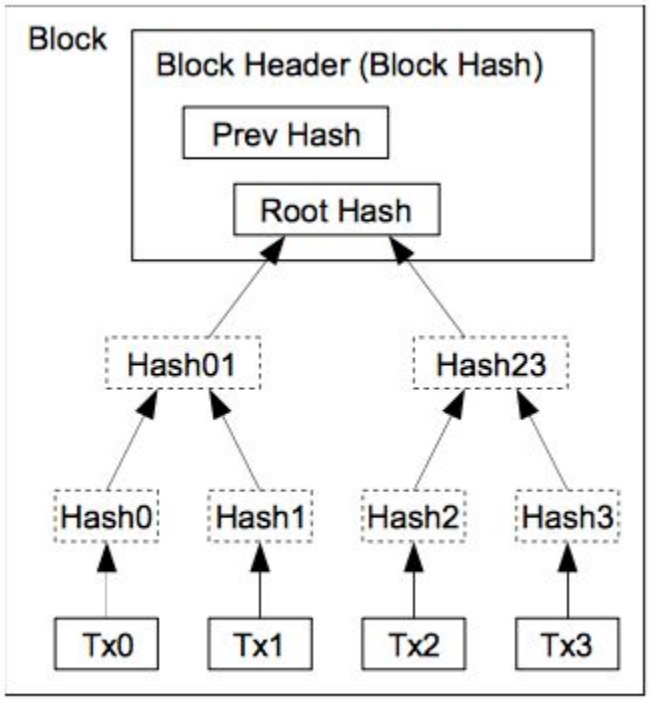
- Hash function: one-way encryption. Difficult to get original data.

Hash function is to generate an abstract/digest of information.

R:
```
install.packages("openssl")
library(openssl)
sha256("123")
# a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
sha256("1234")
# a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

Python
```
import hashlib
hash = hashlib.sha256("123").digest()
```

Merkle Tree: How information is stored in Blockchain is via hash



Transactions Hashed in a Merkle Tree

Ralph Merkle

Merkle at the Singularity Summit 2007

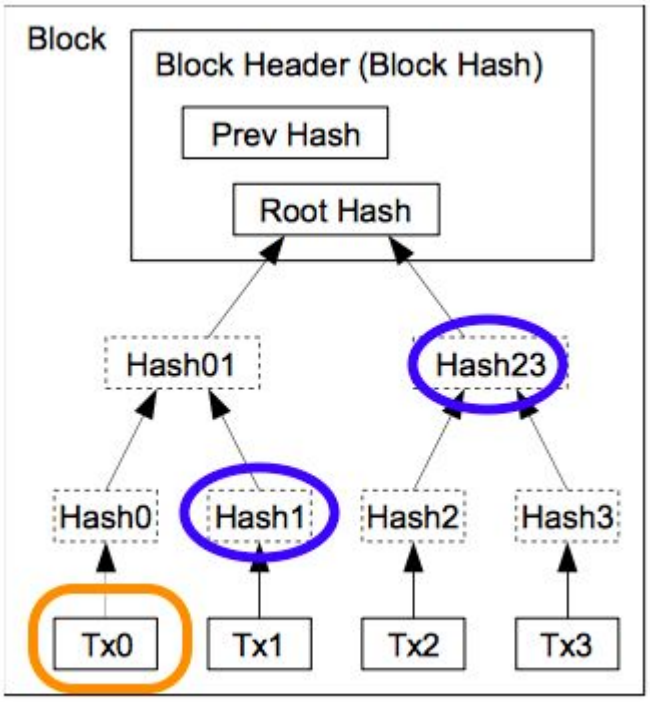
Born	February 2, 1952 (age 65) Berkeley, California
Nationality	American
Citizenship	American
Alma mater	UC Berkeley (B.A., 1974; M.S., 1977) Stanford University (Ph.D., 1979)
Known for	Co-inventor of public key cryptography Merkle tree[1] Merkle's puzzles Merkle–Hellman knapsack cryptosystem Merkle–Damgård construction

Merkle not Merkel

Angela Merkel

Chancellor of Germany

Merkle Tree in a Block of “Blockchain”



Transactions Hashed in a Merkle Tree

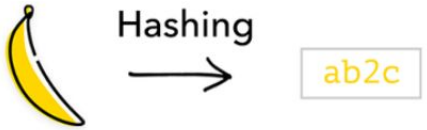
- Transaction records records action and our balance.
- Example of our records
  - F gives A 50 BTC
  - A => B 25 BTC, => C 25 BTC
  - What’s in A’s balance?
    - 0 (Zero)
    - It depends.

- Note: Design of bitcoin
  - A/B/F is wallet address
  - One person can own unlimited number of wallets.
  - A must sends all its holding out. If A just wants to spend 25BTC to B. A will send 25 BTC to B and 25 BTC to C. C is a new wallet address created by the owner of A.

Why Merkle Tree?

Q 1:

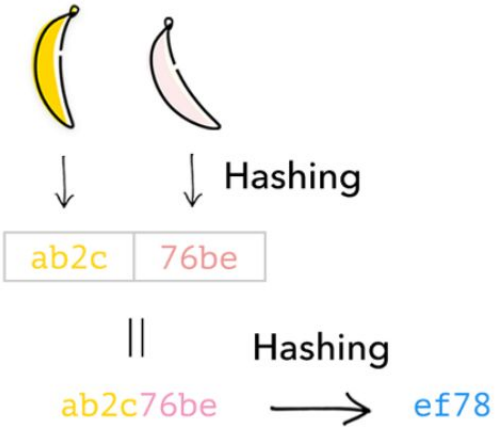
How to encode a banana ?



Representing a small piece of information

Q 2:

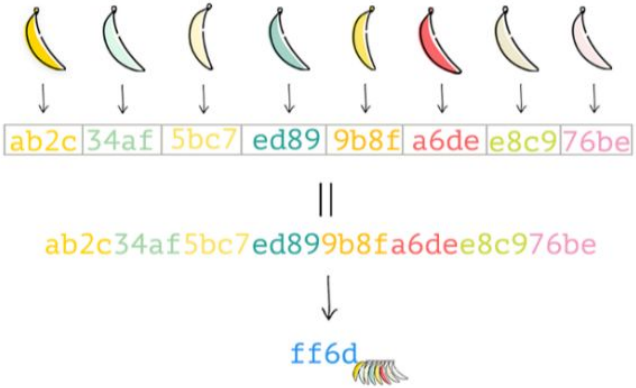
How to encode 2 bananas ?



Naïve Approach

Q3.

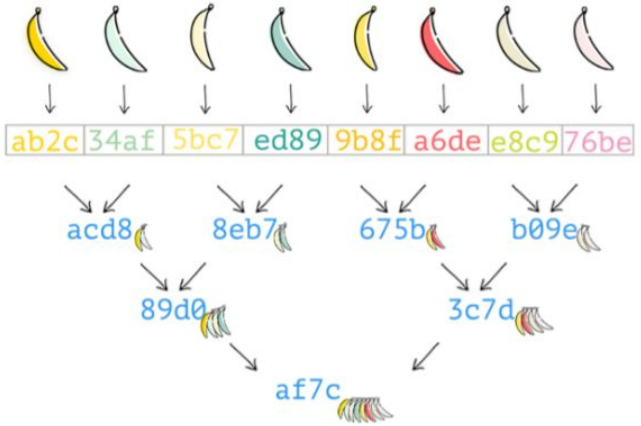
How to encode 8 bananas ?



Merkle Tree

Q3.

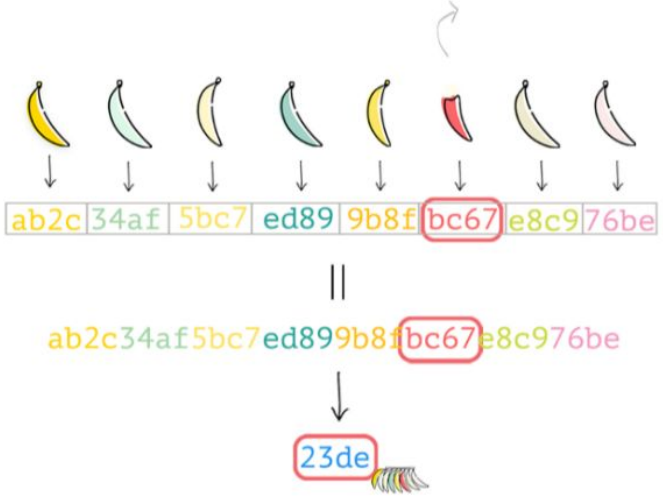
How to encode 8 bananas ?



Q4.

What if a banana has been bitten ?

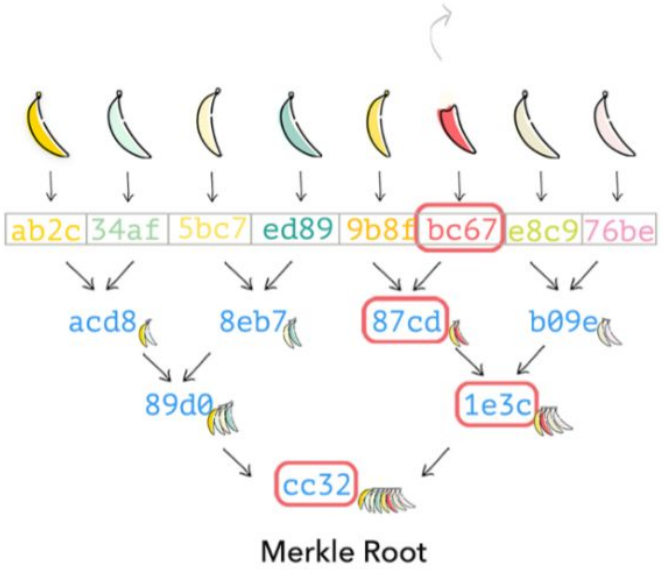
Or a small piece of a large dataset has changed



Q4.

What if a banana has been bitten ?

Or a small piece of a large dataset has changed



Q5.

How to verify that (data chunk) is part of the bunch represented by the Final Hash `ff6d` ?

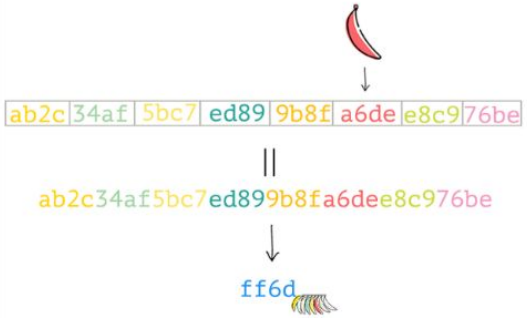
There is no way without the entire bunch (dataset)

Q5.

How to verify that (data chunk) is part of the bunch represented by the Merkle Root `af7c` ?

We only need the banana and a handful of hashes!

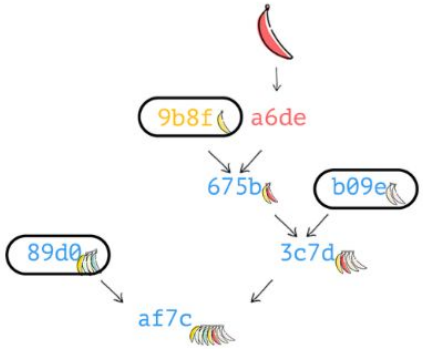
Verifying membership in the bunch requires rerunning the entire proceures



And verify that it's consistent with the Final Hash!

ff6d ✓

Verifying membership in the bunch requires only a few computations



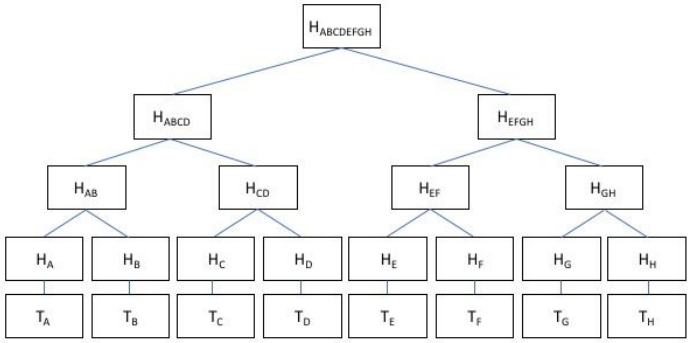
And verify that it's consistent with the Mekle Root!

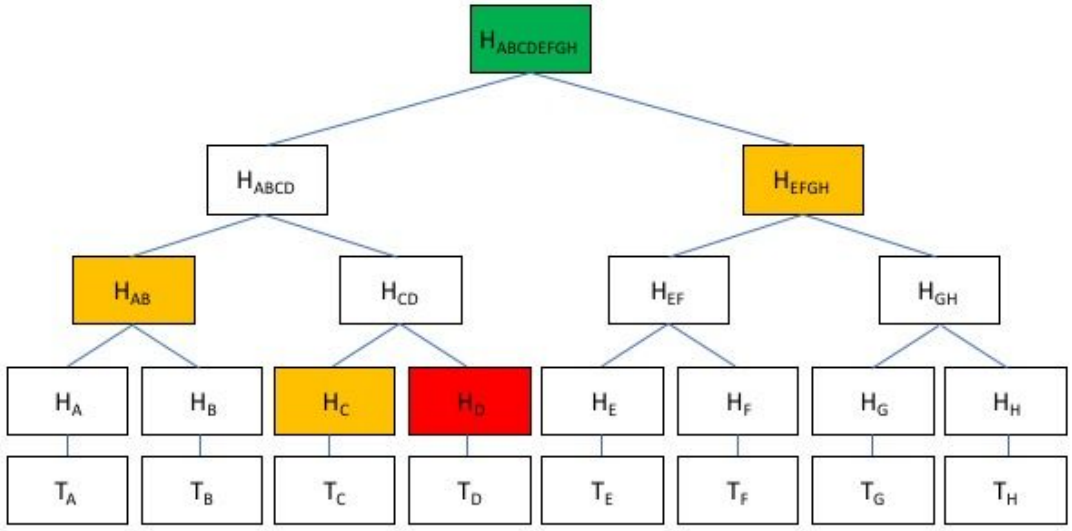
af7c ✓

Note how Merkle Tree requires much less information and fewer computations!

This is the most important advantage of the Merkle Tree!

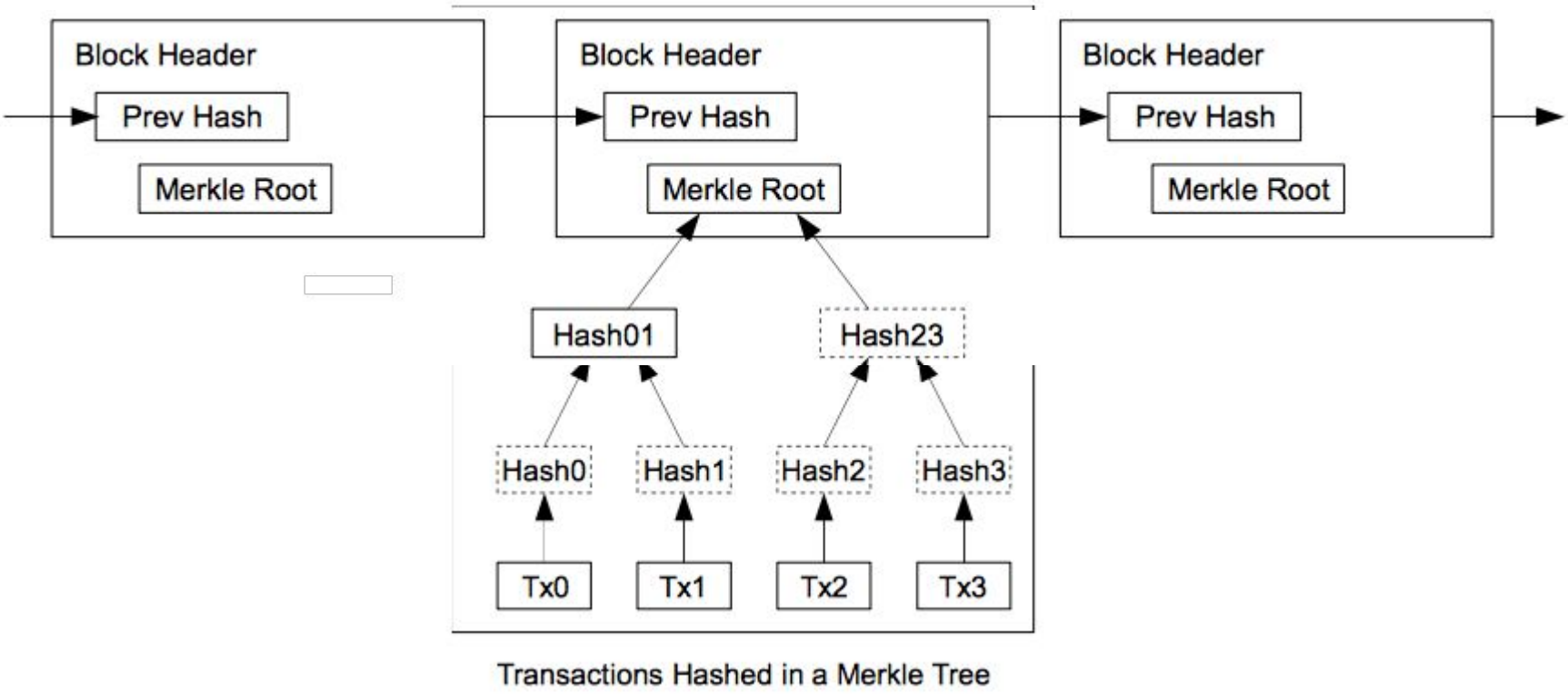
Transactions in Merkle Tree





Merkle Tree is to combine all transactions into one hash.

Blockchain: link Block by Hashes



Transactions Hashed in a Merkle Tree

Blockchain

New information can only be added to the file in blocks that refer to their predecessor in the chain.

The blockchain was designed so these transactions are immutable, meaning they cannot be deleted. The blocks are added through cryptography, ensuring that they remain meddle-proof.

With this link, in a blockchain, if any transaction is altered or corrupted, then the hash of that block will change.

Bitcoin's Blockchain

https://blockchain.info

#497959 is the latest block of now.
hash:
00000000000000000013f779c1c823ba7845c89c81ebdad4d278303279f10eb8

I can store all hashes of bitcoin as 497959 * 256 bits = 15,934,688 Bytes = 15.19 MB. And I can verify whether a block is in the blockchain easily.

A blockchain has three core distinguishing ideas:

1. *Everywhere the same*
2. *The record is permanent.*
3. *No one is in charge, everyone has a piece of it.*

Some cryptographic 2

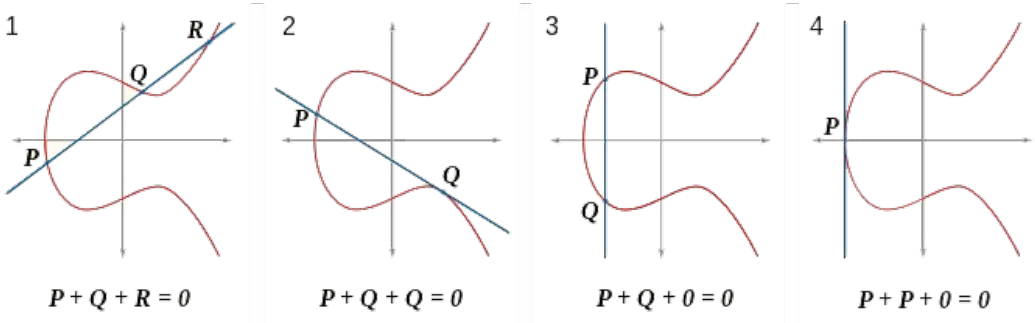
- Asymmetric encryption

There are some mathematics problems are not easily reversible. Such as **big integer factoring.**

https://en.wikipedia.org/wiki/Integer_factorization

When the numbers are sufficiently large, no efficient, non-quantum integer factorization algorithm is known. An effort by several researchers, concluded in 2009, to factor a 232-digit number (RSA-768) utilizing hundreds of machines took two years and the researchers estimated that a 1024-bit RSA modulus would take about a thousand times as long.[1] However, it has not been proven that no efficient algorithm exists.

Elliptic Curves is the current standard, due to space-efficient.



Asymmetric Cryptography to Public Key Infrastructure

How to use big integer to build a public key/private key pair:

p * q = R, R is a very big integer

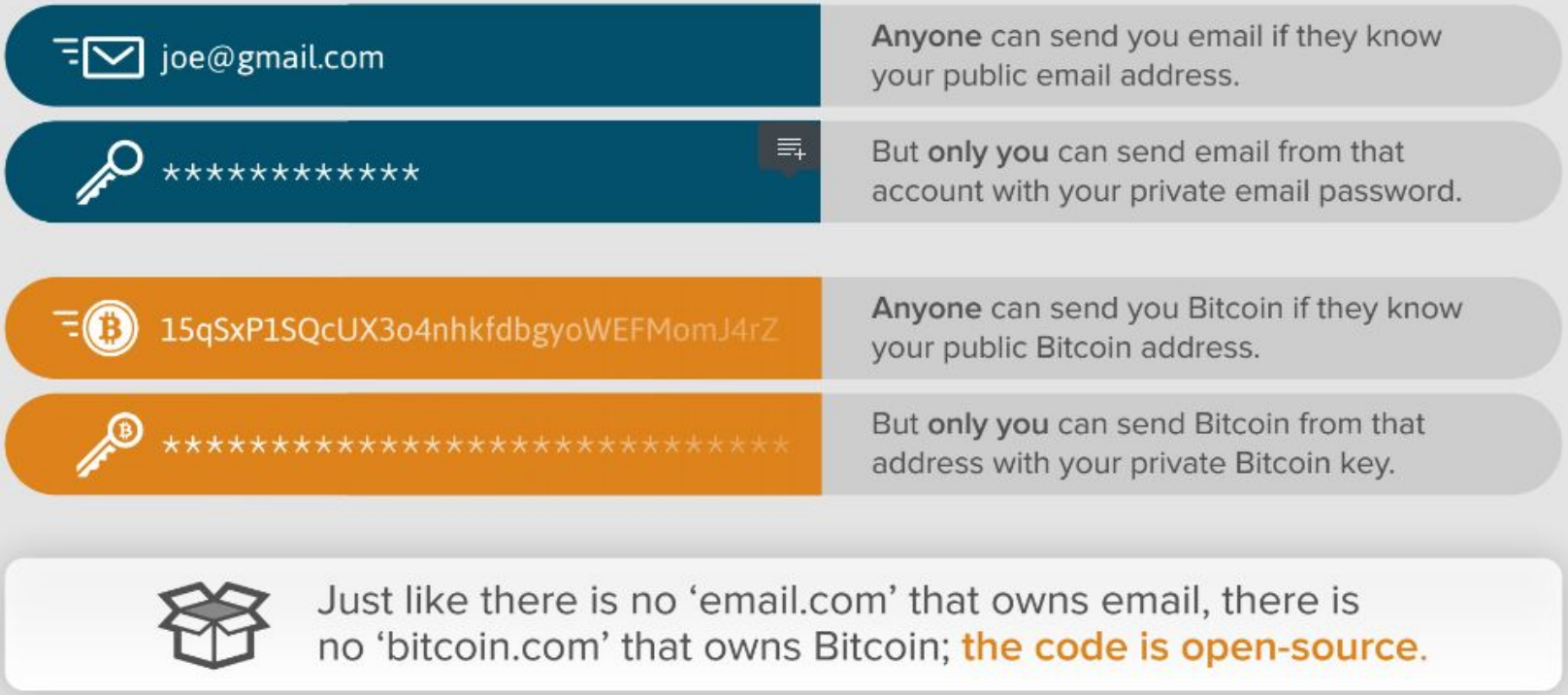
R is my public key to be shared to everybody. p is my private key.

Some one can use my public key to encrypt a message. Only I can decrypt it.

This is how blockchain network to recognize instruction of transactions. If I want to send money out, I need to encrypt my instruction with my private key. The public key can be used to verify whether its my instruction.

To the end user, Bitcoin is like email

Like email, others can send to your public Bitcoin/email address - but only you can send out w/ your private key.



Part 3 Consensus

After talking about Blockchain and Instructions, what happens afterwards is the most innovative thing that Satoshi invented.

I can call it social-economics-science-engineering.

Centralized way: current way

- Alice tells Charlie that she wants to pay Bob $1
- Charlie debits Alice's account by $1
- Charlie credits Bob's account by $1

Charlie maintains the ledger of who has what money. The fact that Alice and Bob both trust Charlie to hand out credits and debits - to validate transactions by updating a ledger - is the way that scarcity can be re-introduced into the digital realm.

Charlie is our bank system today.

The problem, of course, is that **Charlie must be trusted with immense power**: the power over Alice and Bob's bank accounts.

De-Centralized way: current way

Alice and Bob took the pseudonyms 1F2gspw7 and 3MVBBzaD

1F2gspw7 then broadcast to the entire Internet (**~Not just Charlie~**) that it was paying 1 BTC (1 bitcoin) to 3MVBBzaD

A miner listening to the network hears that transaction, ensures 1F2gspw7 owns at least 1 BTC, and adds a record to a database (the Blockchain) such that 1F2gspw7's account is debited by 1 BTC and 3MVBBzaD is credited by 1 BTC.

The miner then in turn broadcasts this database update to all other miners, such that their transaction databases are now in sync.

Mining: How instruction is recorded on Blockchain

Solution:

- Transactions are grouped into blocks.
- About every 10 minutes a new block of transactions is generated and broadcasted, becoming part of the transaction log known as the blockchain, which indicates the transaction has been made (more-or-less) official.
- Bitcoin mining is the process that puts transactions into a block, to make sure everyone has a consistent view of the transaction log.
- Miner needs to “work” hard to be able to generate a block.

This solution is called “proof-of-work”.

Mining and Miner

- Miner earns bitcoin from creating new block.
- In addition, the miner gets any fees associated with the transactions in the block.
- Because of this, mining is very competitive with many people attempting to mine blocks.
- The difficulty and competitiveness of mining is a key part of Bitcoin security, since it ensures that nobody can flood the system with bad blocks.

Mining: How instruction is recorded on Blockchain

Requirements:

- Avoid double-spending, only can appear once, one record.
- Keep everybody updated.
- No forge of record.

Mining: How instruction is recorded on Blockchain

How does the solution solves the issues?

- To mine a block, miners must find an extremely rare solution to an (otherwise-pointless) cryptographic problem. Finding this solution generates a mined block, which becomes part of the official blockchain. => Only one truth can survive.
- Miner is rewarded with bitcoin. This is the only place that new bitcoin is issued. => Everyone wants to get the most updated to work on the next block.
- Forge of record is difficult because it needs to re-do all the calculation that the whole network of computing power has done before.
- Double-spending is avoided.

Why Science-Engineering?

Satoshi's game of number.

The mechanics of the puzzle are fairly simple. Every miner has a block containing a list of transactions that should be published. The miner's goal is to find a value called a nonce, such that the hash of {nonce + block} is less than a target value.

The current target is 440 billion (at the time of writing). And because SHA-256 is a specially constructed cryptographic hash function, miners can't do better than guesswork when it comes to finding a nonce that wins the hash puzzle. So every nonce has a 440 billion / 2^256 = 3.7999142e-66 chance of winning the hash puzzle—meaning a Bernoulli trial.

Mining

```
# Mining with Python
import hashlib, struct
ver = 2
prev_block = "000000000000000117c80378b8da0e33559b5997f2ad55e2f7d18ec1975b9717"
mrkl_root = "871714dcbae6c8193a2bb9b2a69fe1c0440399f38d94b3a0f1b447275a29978a"
time_ = 0x53058b35 # 2014-02-20 04:57:25
bits = 0x19015f53

# https://en.bitcoin.it/wiki/Difficulty
exp = bits >> 24
mant = bits & 0xffffff
target_hexstr = '%064x' % (mant * (1<<(8*(exp - 3))))
target_str = target_hexstr.decode('hex')
```

Mining 2

```
nonce = 0
while nonce < 0x100000000:
    header = ( struct.pack("<L", ver) + prev_block.decode('hex')[::-1] +
          mrkl_root.decode('hex')[::-1] + struct.pack("<LLL", time_, bits, nonce))
    hash = hashlib.sha256(hashlib.sha256(header).digest()).digest()
    print nonce, hash[::-1].encode('hex')
    if hash[::-1] < target_str:
        print 'success'
        break
    nonce += 1
```

Mining - result

0	5c56c2883435b38aeba0e69fb2e0e3db3b22448d3e17b903d774dd5650796f76
1	28902a23a194dee94141d1b70102accd85fc2c1ead0901ba0e41ade90d38a08e
2	729577af82250aaf9e44f70a72814cf56c16d430a878bf52fdaceeb7b4bd37f4
3	8491452381016cf80562ff489e492e00331de3553178c73c5169574000f1ed1c
39	03fd5ff1048668cd3cde4f3fb5bde1ff306d26a4630f420c78df1e504e24f3c7
990	0001e3a4583f4c6d81251e8d9901dbe0df74d7144300d7c03cab15eca04bd4bb
52117	00006424117 33cd63264d3bedc046a5364ff3c77d2b37ca298ad8f1b5a9f05ba
1813152	00000c94a85b5c06c9b06ace1ba7c7f759e795715f399c9c1b1b7f5d387a319f
19745650	000000cdccf49f13f5c3f14a2c12a56ae60e900c5e65bfe1cc24f038f0668a6c
243989801	0000000ce99e2a00633ca958a16e17f30085a54f04667a5492db49bcae15d190
856192328	00000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50

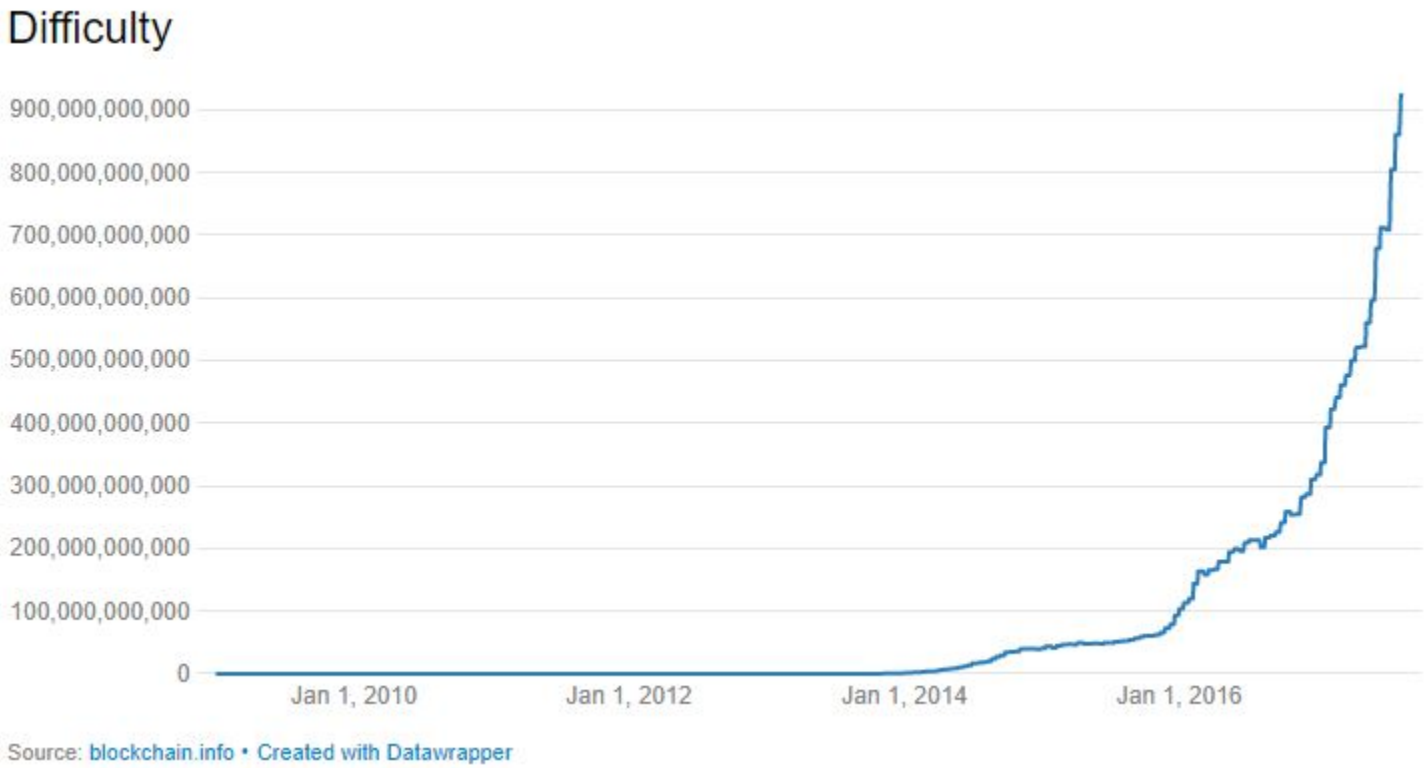
Satoshi thought of increasing computing power

The time between blocks in the Bitcoin blockchain is Poisson distributed with an expected value of 10 minutes between blocks.

Since millions of these Bernoulli trials are happening every second, across the global compute power of miners, we end up with a Bernoulli distribution where a miner wins the hash puzzle (and can then publish a block) every 10 minutes, on average.

Since the global compute power of miners changes, so does the target value in the hash puzzle. Thus, the expected time between blocks remains 10 minutes, even as global mining power changes over time.

Mining Difficulty



Genesis Block - https://goo.gl/oXh38t

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Block information

Block #480504

Summary	
Number Of Transactions	2779
Output Total	27,697.98433914 BTC
Estimated Transaction Volume	3,818.00804544 BTC
Transaction Fees	2.33243867 BTC
Height	480504 (Main Chain)

Hashes	
Hash	000000000000000000c2c4d562265f272bd55d64f1a7c22ffeb66e15e826ca30
Previous Block	000000000000000000a08e6f7a955e49de1c4efffbcb7fbe348d8a3f3d155b50
Next Block(s)	000000000000000000005ebdb5fe9e24266bb673416879c5ca28ce1153fccfec9e
Merkle Root	ee527ad6598161318c74a88f3006ae08c6ec16d470082b30a09038f82a0292ef

https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Why this solution is also Social-Economical

- Satoshi designs that bitcoin is issued to miner. If you can create a block, you earn bitcoin. This is the only way that bitcoin is issued.
- Once a new block is created, miner broadcasts to the network. All receivers will stop working on this block and switch to work on next block for new transactions.
- No one wants to lag behind. So only the longest chain will survive.
-

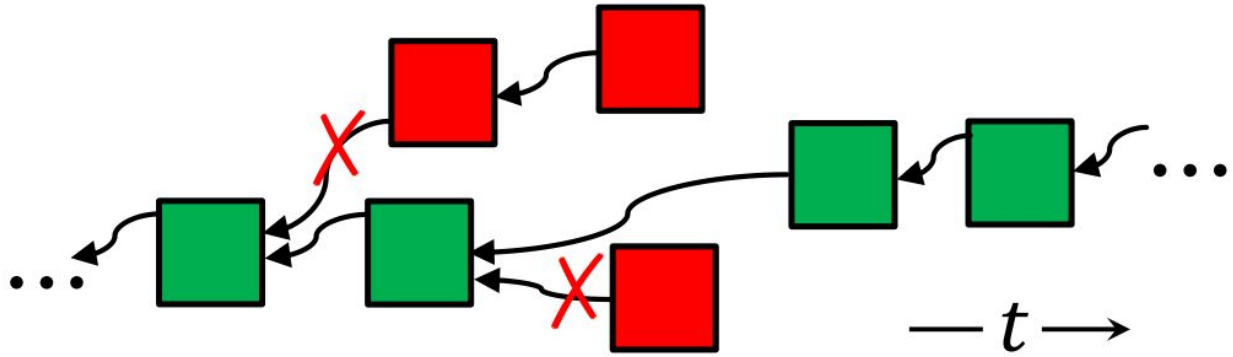
Bitcoin - the great social experiment

- For bitcoin, it happened several times that two solutions are found almost at the same time, almost half-half in the network. It survived.
- Once it was due to a software bug.
- Once it was due to half-user upgraded, half-user not upgraded.
- Bitcoin has survived all these tests.

Mining Power Utilization

17

Measure of robustness against rollback



$$\frac{\sum \blacksquare}{\sum (\blacksquare + \blacksquare)}$$

https://cyber.stanford.edu/sites/default/files/efegencer.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

http://fermatslibrary.com/s/bitcoin

Bitcoin paper: abstract 1

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, **but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.**

Bitcoin paper: abstract 2

The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, **forming a record that cannot be changed without redoing the proof-of-work**.

The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Future World with Blockchain and Smart Contract

A blockchain has three core distinguishing ideas:

1. *Everywhere the same*
2. *The record is permanent.*
3. *No one is in charge, everyone has a piece of it.*

Use blockchain to store records and logic.

- Major business activities involves credit:
  - Verification of ownership
  - Verification of identity
  - Loan
  - Delayed payment
- Many middlemen are hired to act as witness or authority

Smart Contract

- It’s a beautiful thing the more you think about it. You can cut out tons of middlemen here.
-
- All public records of ownership are stored in **Country Recorder**.
- If I want to buy a house, I will search it. Find one and verify the house with the seller’s public key in **Country Recorder**.
- I might go peer-to-peer with the seller and we’ll transfer the title after a few meetings in exchange for some crypto-currency. I’ll pay the seller.
- The **County Recorder** is instantly notified and tax records updated. My title gets properly recorded and seamlessly transferred and my crypto wallet is updated with the new house title.
- Who won’t be involved in all of this? The brokers, title companies, laywers, etc with all their crazy fees and paper pushing.
- And in the end we’ll have achieved the same basic process without incurring all these middleman steps along the way

Bitcoin disintermediates banks

Similarly, Bitcoin disintermediates Fedwire/ACH/SWIFT, replacing with programmable packet-based money.

BEFORE

Deal with bank to deploy code related to value in the banking system

AFTER

Anyone can programmatically send value to anyone (or many anyones) via Bitcoin

Bitcoin has a four-sided network effect

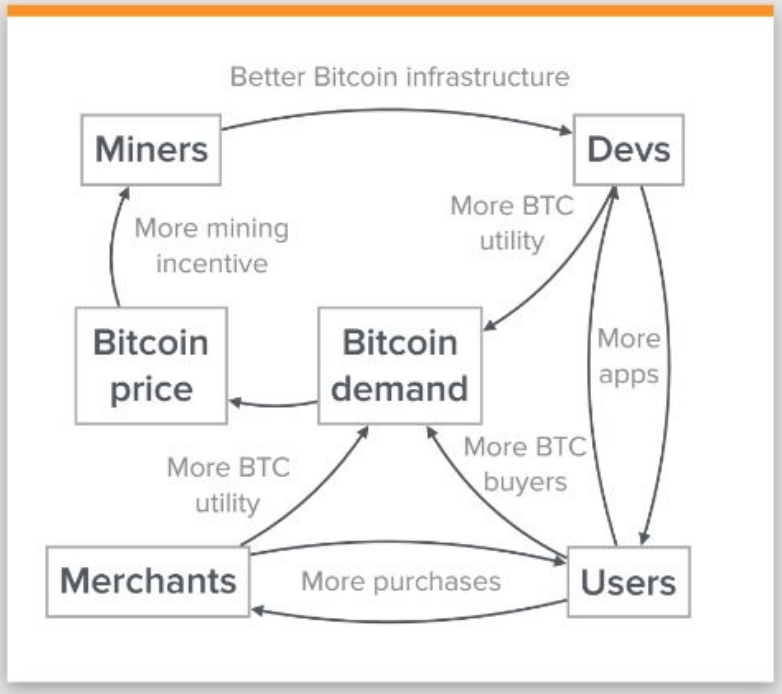
Four groups: miners, developers, users, and merchants.

Miners
Verify transactions, receive BTC.

Devs
Write Bitcoin apps.

Merchants
Accept Bitcoin for goods.

Users
Use Bitcoin for goods & apps.



The 4-Sided Network Effect
Every node increases value for other nodes.

Application of Blockchain: fine-grained database and control

https://qz.com/929833/googles-goog-deepmind-is-using-blockchain-technology-to-handle-nhs-medical-data/

As part of its projects with Britain's National Health Service, Google's artificial intelligence unit DeepMind announced last week it's developing a new way to protect confidential health data—from itself. Its problem: How to assure hospitals, and the public at large, that patient confidentiality isn't compromised as it processes the sensitive medical health records entrusted to it.

DeepMind's proposed solution is to create an indelible data log that can't be tampered with. It would show when a piece of data was used, and for what purpose. Importantly, DeepMind itself wouldn't be able to modify logs to use the data nefariously. The solution bears resemblance to the "distributed ledger technologies" or "private blockchains" that the financial world has been trying to create in recent years. While loathe to call it "blockchain"—DeepMind prefers the term "verifiable append-only ledger" to describe its health data system—it is interested in one property that the technology can confer upon its users: trust.

While the banks want blockchains to slash back-office costs while staying compliant, DeepMind needs blockchains to shore up public trust. Last year, DeepMind's work with the UK's health service was dragged into the public by a *New Scientist* investigation. The publication found that 1.6 million patient names, addresses, and other information from three London hospitals had been shared with Google's artificial intelligence subsidiary. It triggered an investigation by the UK's privacy regulator that is ongoing. DeepMind and the hospitals say they followed the rules.

http://www.chinadaily.com.cn/business/2017-10/14/content_33235955.htm

PBOC inches closer to digital currency

By Wang Yanfei | China Daily | Updated: 2017-10-14 09:10

The People's Bank of China (PBOC) is seen in this photo taken on June 12 in Beijing. [Photo/Xinhua]

The People's Bank of China, China's central bank, has completed trial runs on the algorithms needed for digital currency supply, taking it a step closer to addressing the technological challenges associated with digital currencies, according to a top official associated with the project.

Yao Qian, director-general of the Institute of Digital Money at the PBOC, said China's central bank has successfully designed a prototype that can regulate the supply of its future digital fiat

The successful simulation of money supply paves the way for the central bank to become the future sole regulator and policymaker governing the value of digital fiat currency, said Yao.

Digital fiat currencies are the digital forms of a sovereign currency that is backed by the central bank.

Unlike Bitcoin or other digital money issued by the private sector, the digital fiat currency has the same legal status as the Chinese yuan, the only fiat currency issued by the People's Bank of China.

There is no timetable for the introduction of the currency, but once introduced, China is likely to become the first country that would deploy a digital fiat currency.

China's central bank has been actively preparing for digital fiat currencies since last year.

Earlier in June, the central bank finished several digital money trials involving fake transactions between it and some of the country's commercial banks.

"China has been at the forefront in digital payment technology development," said Di Gang, a senior engineer of the institute.

"However, it would still be some time before the currency goes public," said Di, adding that, "the central bank is proceeding very cautiously."

Apart from solving the technology challenges, there are a number of other concerns that are yet to be solved such as managing risks and improving efficiency, according to Di.

The government also needs to factor whether the public would use the new currency, he added.

"The central bank might be able to start trials in some developed regions such as Beijing, Shanghai and Guangdong province, and see how citizens respond to the digital currency," he said.

The development of a digital currency comes at an opportune time for China, said Yao.

Various (Social) Topics of Bitcoin

Energy Consumption of Bitcoin network

Source: https://digiconomist.net/bitcoin-energy-consumption

Each Bitcoin transaction uses 271kWh of electricity—enough to power a typical American home for nine days.

What does cause Bitcoin's energy usage to rise however, is when Bitcoin's price goes up. A higher price means the 12.5 bitcoin reward becomes more valuable, and so miners spend more resources to capture the larger prize.

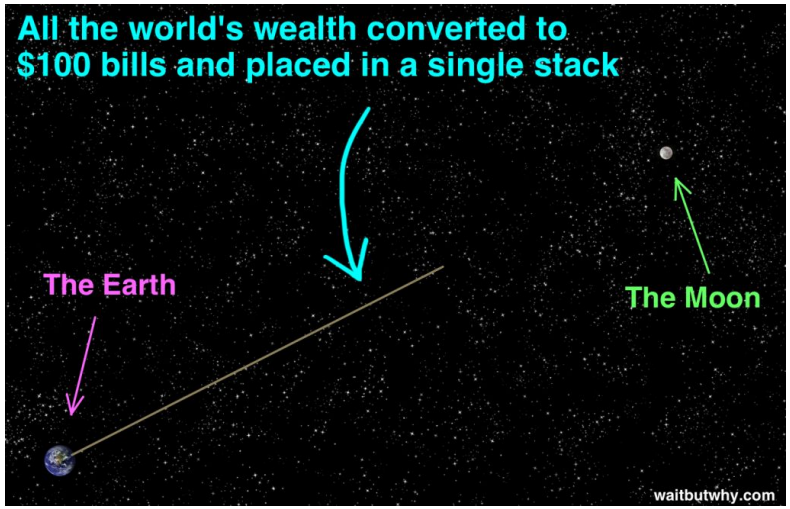
Per-block reward has fallen twice—it started out at 50 bitcoins in 2009—and is scheduled to fall to 6.25 bitcoins per block some time in 2020, then to 3.125 bitcoins per block around 2024. I hope, as the per-block reward falls, the network's energy consumption will fall proportionately.

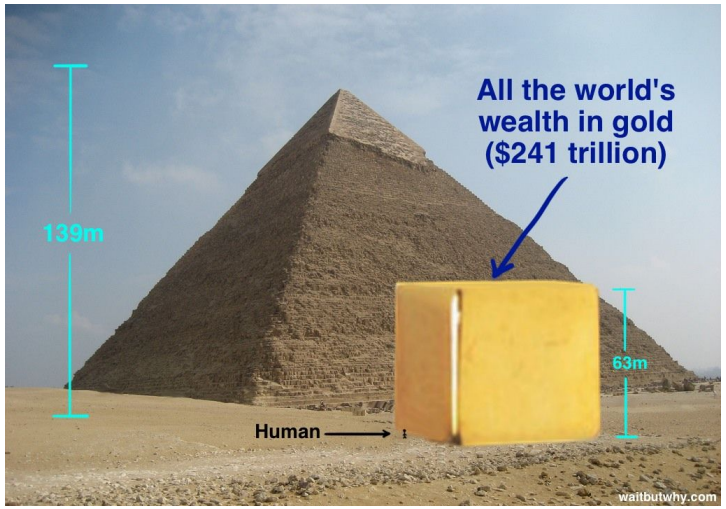
Valuation of Bitcoin - Fundamental View

- Asset pricing is that price = expected present value of dividends.
- Bitcoin will never has cash dividends. Like as gold.
- Asset pricing is also affected by "convenience yield," or a "rational bubble."
  - If the price is greater than zero, either people see some "dividend," some value in holding the asset, beyond its cash payments; like AMZN equity.
  - Or, buyer/holder think the price will keep going up forever, so that price appreciation alone provides a competitive return. There is no such thing, “Greater fool” or “Ponzi scheme”.
- Price surges only happen with 1) restricted supply, 2) and accompany price volatility, 3) large trading volume, and 4) short holding periods.
-

Valuation of Bitcoin - World Asset allocation

- Some estimates that there is $241 trillion of wealth in the world
- If you imagine people wish to hold one quarter of one percent of that in crypto form, that gets you to about $600 billion in value. Currently crypto assets (on good days) hover near $300 billion in market capitalization. Is that so crazy?





Valuation of Bitcoin - World Asset allocation

- Total market cap of cryptocurrency has exceeded $300bn. Bitcoin's market cap is about $168bn, Ethereum, 2nd largest cryptocurrency, has a market cap of $42bn, followed by Bitcoin cash at $23bn.
- In comparison, total size of gold ETFs at $90bn. Bitcoin > Gold?

Valuation of Bitcoin - World Asset allocation

- First, gold ETFs is not the main way wealth is stored via gold. Wealth is mostly stored via gold bars and coins the stock of which, excluding those held by central banks, amounts to 38,000 tonnes or $1.5tr. **In other words, the market cap of cryptocurrencies would have to rise five times from here to match the total private sector investment to gold via ETFs or bars or coins.**
- Second, cryptocurrencies derive value not only because they serve as store of wealth but also due to their utility as means of payment. The more economic agents accept cryptocurrencies as means of payment the higher their utility and value. **I am bit skeptical that now it takes 15% to do money remittance with bitcoin. Bitcoin trading is mostly speculative.**

Bitcoin as a descendant of technologies in the last 30 years.

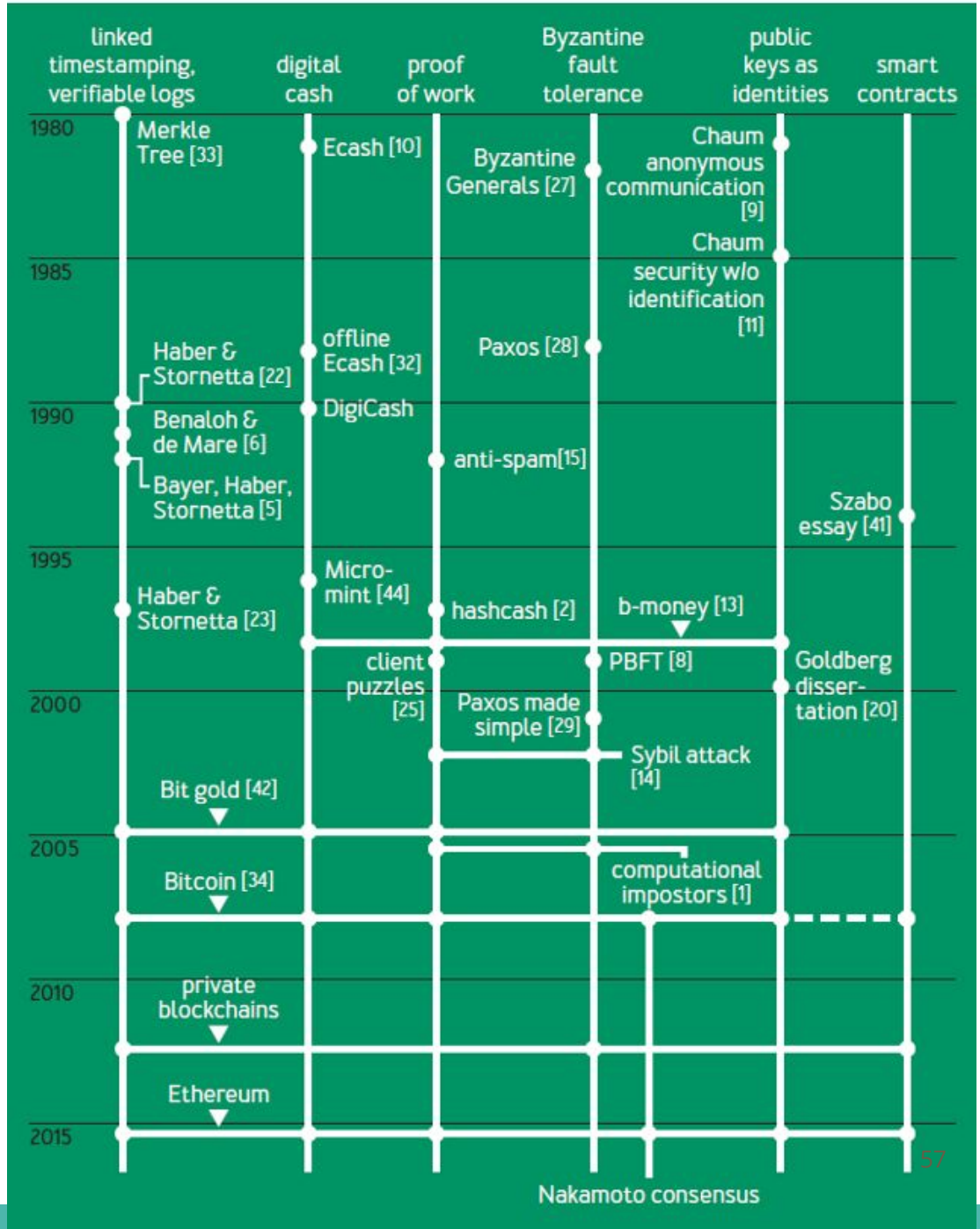
Bitcoin's Academic Pedigree

The concept of cryptocurrencies is built from forgotten ideas in research literature.

Arvind Narayanan and Jeremy Clark

http://queue.acm.org/detail.cfm?id=3136559

FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN



Summary

- Hash function - merkle tree - block and blockchain.
- Asymmetric cryptography - identity
- Mining/consensus process - Proof of work - Nakamoto Consensus
- Smart Contract

Summary

- Buying bitcoin is the least you can do.

1. Study Bitcoin, bunch of books and online tutorial
   a. E.g.
   b. E.g. http://davidederosa.com/basic-blockchain-programming/
2. Study Ethereum - smart contract project. Program in Solidity language
3. Work with open source blockchain platform.

MultiChain

Adjoint