Just NOT a investment guide

Lecture 11: Blockchain and Consensus

MFE FE8828 Cryptocurrency Technologies /1

2018/11/26

Yang Ye

Overview

Lecture 11 Blockchain and Consensus

- Part 1: Blockchain
    - Block
    - Has
    - Merkle Tree
- Part 2: Consensus
    - Nakamoto consensus, "Proof-of-Work"
    - Mining

Part 0: Introducing Bitcoin

Do I need to?

B$: Sixth largest currency in the world.

BTCUSD

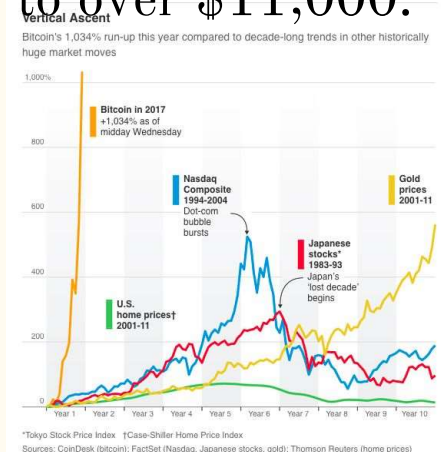CFTC

Value of Currency In Circulation (USD Billions)

5

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.

Bitcoin price milestones

- 1 week to **$9,000**
- 2 weeks, 3 days to **$8,000**
- 1 week, 6 days to **$7,000**
- 1 month, 2 weeks, 4 days to **$6,000**
- 3 weeks to **$5,000**
- 2 months, 1 day to **$4,000**
- 3 weeks, 1 day to **$3,000**
- 3 years, 5 months, 2 weeks, 5 days to **$2,000**
- 4 years, 10 months, 4 weeks to **$1,000**

'09 '10 '11 '12 '13 '14 '15 '16 '17

ATLAS | Data: Coindesk

Vertical Ascent
Bitcoin's 1,034% run-up this year compared to decade-long trends in other historically huge market moves

Bitcoin in 2017 +1,034% as of midday Wednesday

Nasdaq Composite 1994-2004 Dot-com bubble bursts

Gold prices 2001-11

Japanese stocks* 1983-93 Japan's 'lost decade' begins

U.S. home prices† 2001-11

*Tokyo Stock Price Index †Case-Shiller Home Price Index
Sources: CoinDesk (bitcoin); FactSet (Nasdaq, Japanese stocks, gold); Thomson Reuters (home prices)

6

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.

7

Part 1: Blockchain

Part 1: Blockchain and Bitcoin

- First blockchain was implemented in Bitcoin.
- Blockchain and bitcoin, which one appears the first?
- Your would answer Bitcoin appeared first.
- Anwer: First is the **block** "Genesis Block", Second is the **coin**, Third is the **Blockchain**. This order is the key to understand cryptos.
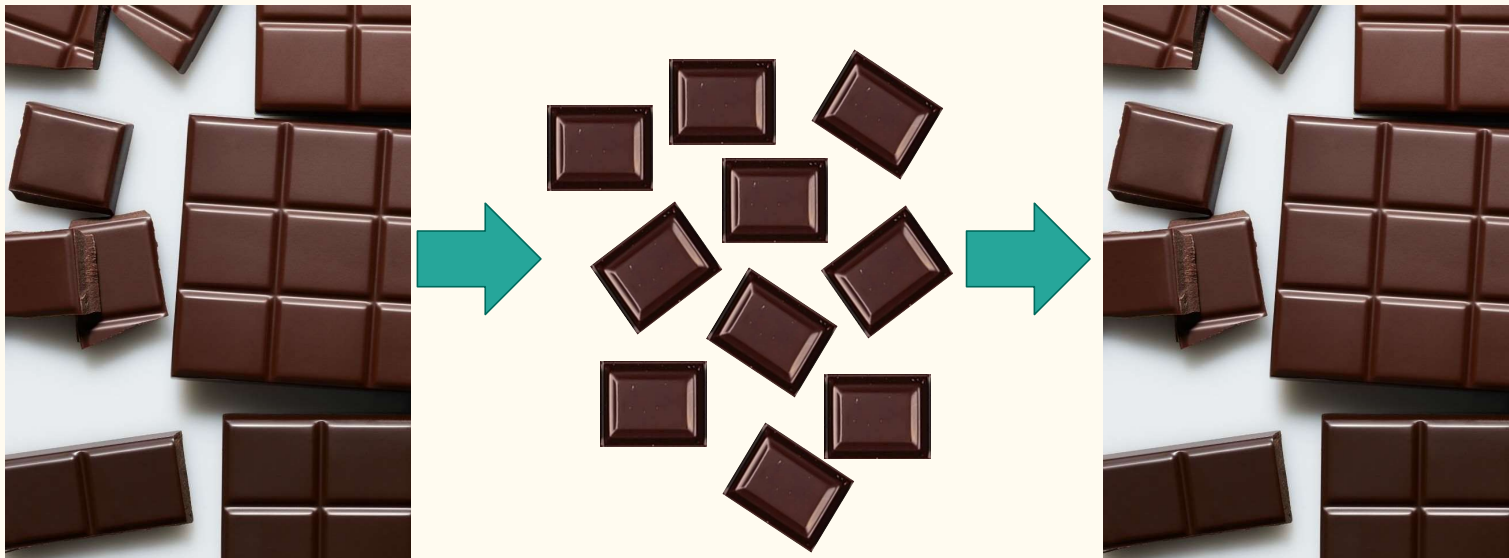- After this lecture, you shall know why and how
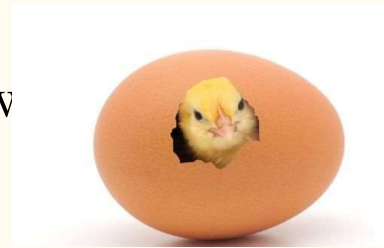
Data structure

- Inside computer memory, we design certain ways to store and retrieve data.
- They are called **data structure**.
- The simplest data structure is an **array**.
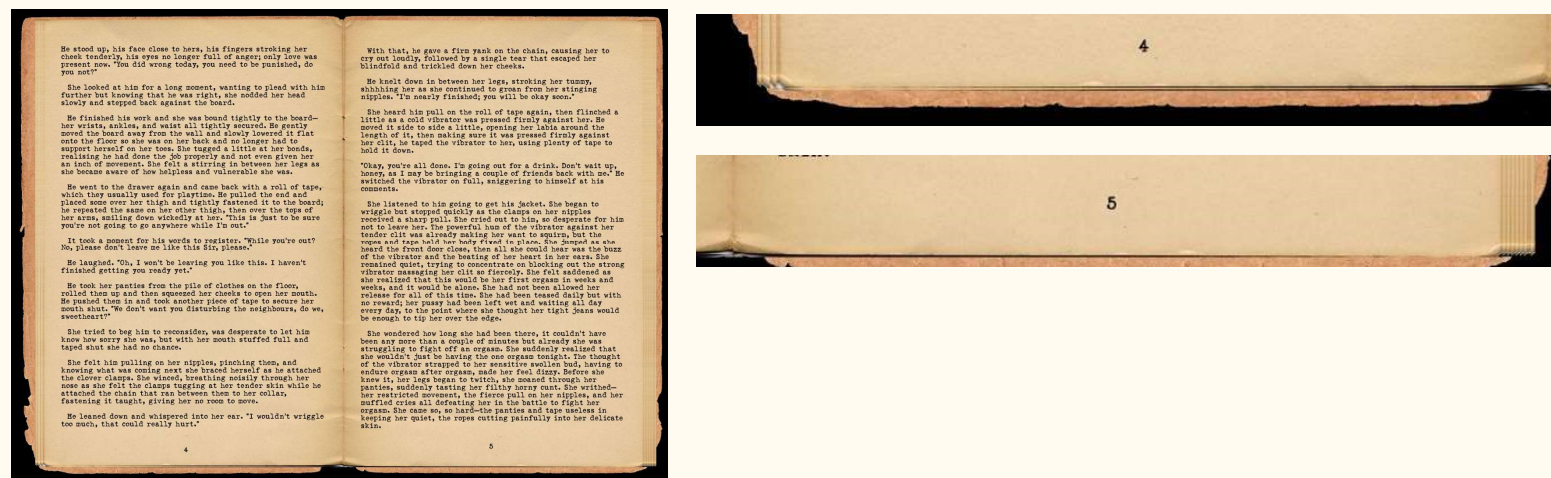- **Element** are inside array.

Distribute the Array (Chocolate)

Labelled Array (Book)

It's still not good enough

Page number is still not good enough.

Watermark/special color of paper/... are ways to ensure we get back what we distributed earlier.

The digital watermark is from cryptography:
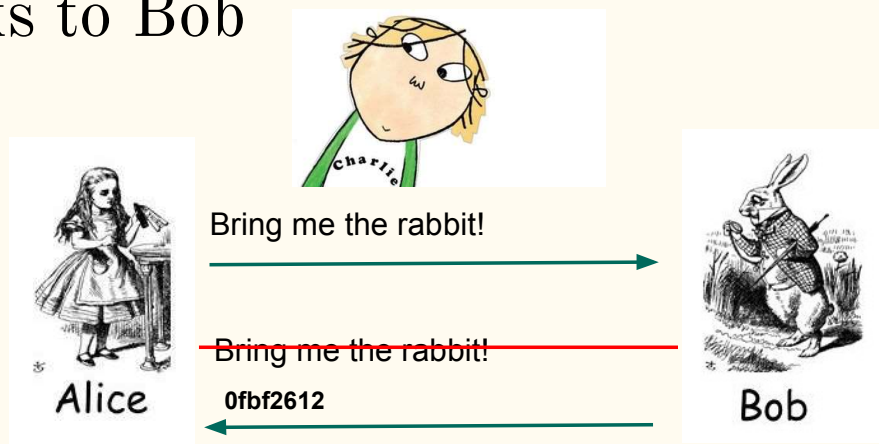
Cryptographic Hash

In short, **"Hash"**

Cryptographic Hash

Cryptographic hash was about to solve the problem of data verification.

Hash can map data of arbitrary size to data of fixed size. The fixed size is much shorter than the original data.

256bit hash = 2 power 256

Alice talks to Bob

Bring me the rabbit!

Bring me the rabbit!

0fbf2612

Alice

Bob

Both Alice and Bob know a certain hash algorithm to compute a hash from a message.

Bob doesn't need to send the original message ("Bring me the rabbit") but just the hash ("0fbf2612").
So Alice can know that Bob has received her message.

hash("bring me the rabbit") = "0fbf2612".
Alice needs to know what crytographic hash that Bob used.

Cryptographic Hash

Cryptography has created a number of very good hash functions.

- We can't easily find another data with the same hash
- A small change in the original data would result in another hash and such change is not predictable.
- "Bring me the rabbit" => "Bring me the Rabbit"
- Brute-force, "rainbow attack".

$$2^{95} = 39,614,081,257,132,168,796,771,975,168$$

Bitcoin uses double SHA-256

Sounds "Sharp-256"

It's 256 bits of data to represent data. Double means it hashes twice.

Long and hard to crack. Within current limit, they are safe to use. Quantum computing may crack it.

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()
```
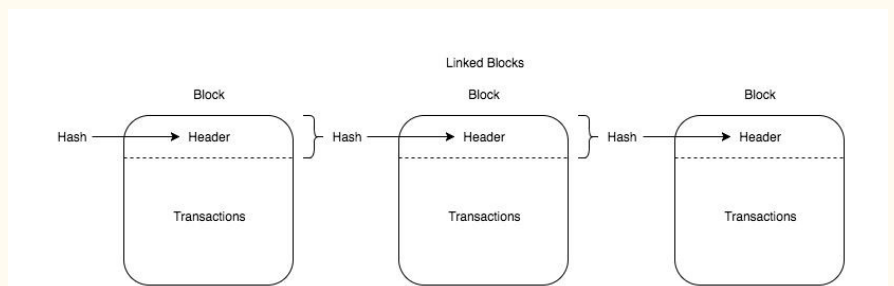
Book with Hash

So, if we generate **a hash** the content of a page and put the **hash value** on **the next page**. In this way, we can determine whether a page is the original page by checking the hash on its next page.
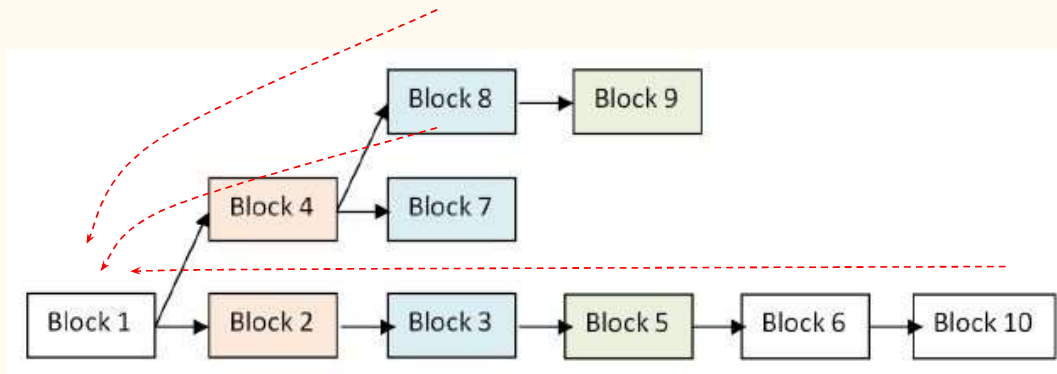
This is blockchain.

"Chain of blocks"

Blockchain can grow

So, there could be only one chain if we trace **back** from Block N to Block 0. Blocks can be **distributed stored**, old data **can't be modified**, and, more importantly, chain **can grow**. By now, you shall understand fully about the definition of blockchain and why it's useful.

One way to trace back

Merkle Tree: Store data in Blockchain
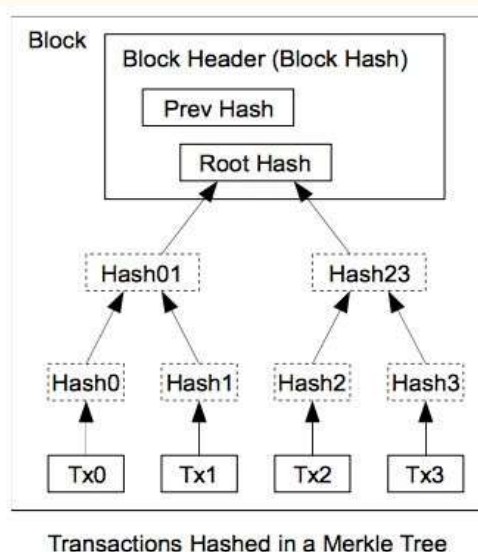
Transactions Hashed in a Merkle Tree

Merkle not Merkel

# Grouped Hash

Merkle tree is a grouped hash of data. Binary tree is combine two-record per hash. One Merkle tree contains N data and $1 + 2 + 4 + ... N / 2$ hashes. Merkle tree provides simplified verification, $\log 2(N)$ for N transactions.
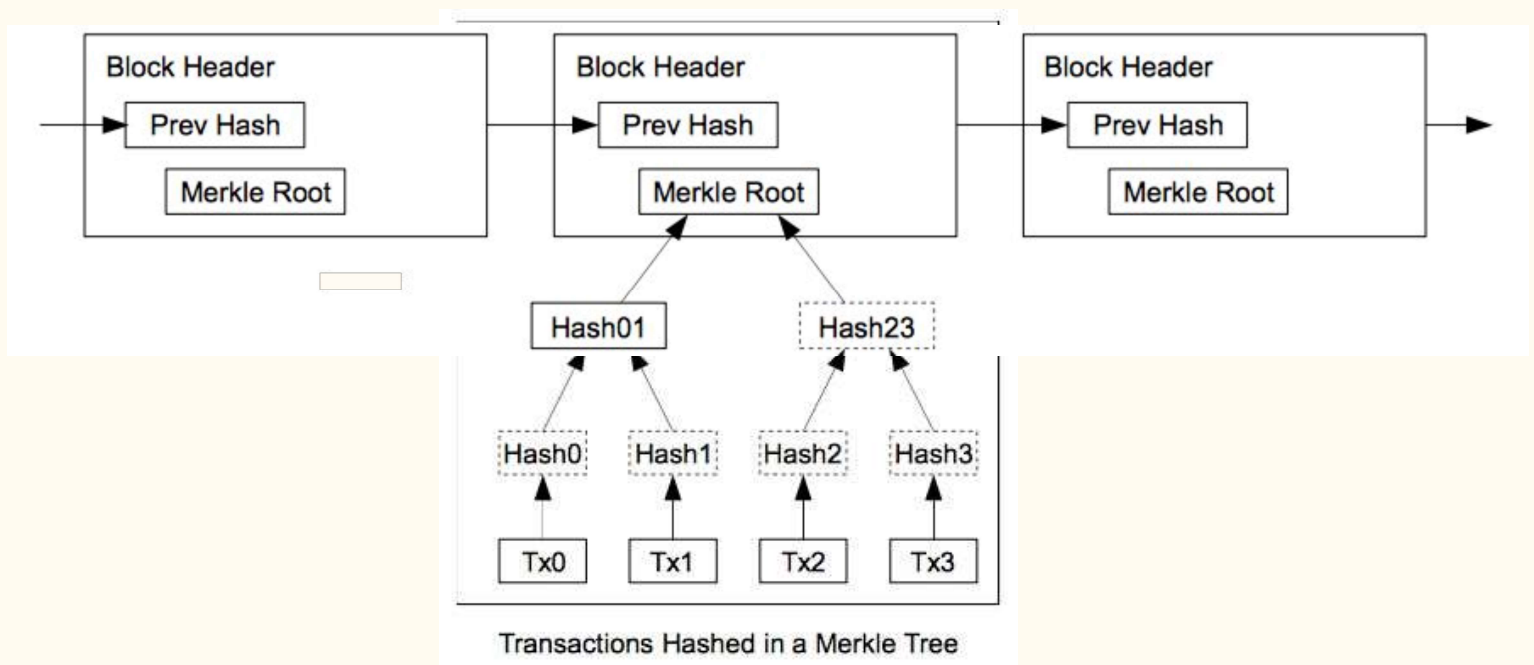
In-and-out block, there are hashes. Hash offers verification and also a space-saving. Full Bitcoin blockchain is close to 200G till now but hashes only takes less than 100MB.

$HAB = hash(HA + HB)$
$HA = 0fbf2912$
$HB = 0fab1259$
$HA + HB = 0fbf2912ab1259$
2 power $10 = 1024$
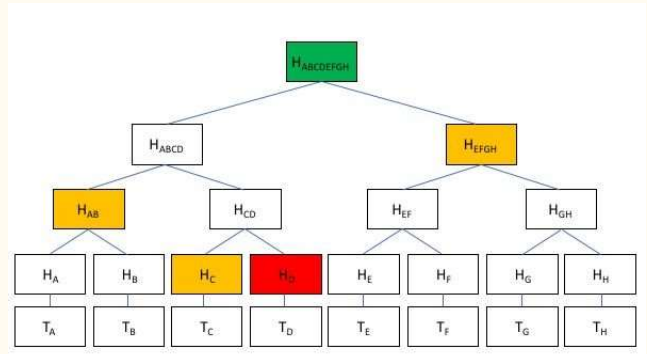
Blockchain: a complete picture

Transactions Hashed in a Merkle Tree

Transactions in Merkle Tree
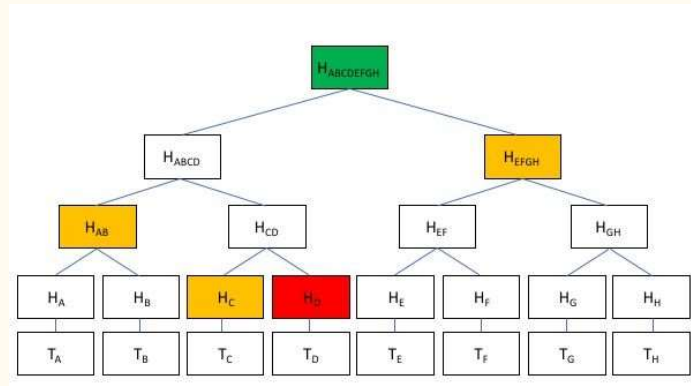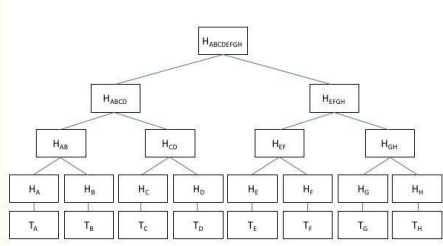
Merkle Tree is to combine all transactions into one hash.

What' in a Block?

- Block 0: transactions + Timestamp
- Block 1: hash of Block 0 + transactions + Timestamp
- Block 2: hash of Block 1 + transactions + Timestamp
- Block 3: hash of Block 2 + transactions + Timestamp
- ...

Timestamp adds an extra layer of verification. Timestamp must be increasing together with the block number. In Blockchain, hash is performed on data, the previous hash and a timestamp.

Blockchain Definition

- It is a **continuously growing list of records**, called blocks, which are **linked** and **secured using cryptography hash**. ("Block")
- Each block typically contains **a cryptographic hash of the previous block**, a timestamp and transaction data. ("Chain") "append-only"
- By design, a blockchain is **inherently resistant** to modification of the data.

Bitcoin's Blockchain

https://blockchain.info

#497959 is the latest block of now.
hash:
0000000000000000013f779c1c823ba7845c89c81ebdad4d278303279f10eb8

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.*

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

Block #0

Summary			Hashes	
Number Of Transactions	1		Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Output Total	50 BTC		Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Estimated Transaction Volume	0 BTC		Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Transaction Fees	0 BTC		Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
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			

Blockchain: Review

- One block has two parts: body and header.
- Header contains the hash of the previous block, the timestamp and the index.
- Body is a merkle tree, Merkle tree is a grouped hash of data. Binary tree is combine two-record per hash.
- Blockchain is blocks linked by Hashes.

Blockchain: Review

The blockchain was designed so transactions are immutable. To traceback from one block to its root, there could be only one way back.

Yet, it is possible to rewrite history by throwing away certain blocks and restarting the chain from past block, it's called "Fork".

Part 2: Consensus

Consensus Algorithm

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

"Consensus algorithm", which is social-economics-science-engineering.

Blockchain Live!

- Blockchain lives in a distributed peer-to-peer (p2p) network of users. "client" software.
- The nodes on network will gossip with each other about what it knows about the blockchain, "who/when/what".
- It's a big network that each other is talking to each other about what's happening.

Consensus Algorithm

The blockchain network needs to achieve following goals.

- Crucially, participants agree on the dynamic content of the data i.e. nodes have a mechanism to resolve conflict ("**Safety**")
- Not any one entity controls the content of the data ("**distributed authority**").
- The data can move forward, ("**Liveness**")

Consensus algorithm is about to achieve these.

Nakatomo Consensus

The inventor of Bitcoin, Nakatomo Satoshi proposed the following process:

- To create a new block with new transactions, Alice needs to first **solve a hard problem**. Once she works it out, she will be **rewarded**. She **broadcast** the answer to the network.
- Bob/Charlie/Danny would **validate** the block that Alice **has really solved the problem** and the block is correctly constructed so there is no wrong records, like "double spending". Only valid block would be accepted and passed.
- "Bob/Charlie/Danny/Eva/Frank/..." will start working solving the problem for the next block. Who's the lucky one this time? Go back to step 1 above.

Game with Hash: hard problem

It needs to guess a number that adds to the current hash to produce a new hash with certain number of leading zeros.

hash("ABC" + XXXX) => 000000....... XXXX is the nonce.

1/16 * 1/16 * 1/16 => smaller the probability, the harder the problem.

Because cryptographic hash has no easy guess between input and output. Node has to start from 1, try, 2, try, 3, try, till it reaches a number that satisfies the condition.

PoW: Proof of Work

Satoshi's PoW systems appears to kill four birds with one stone:

- Coin production = reward for solving the problem.
- Broadcast transaction and make it acceptable
- Grow the blockchain correctly: record new transaction. Chain selection, longest
- Who produces blocks, and When blocks are produced
  - "Setting difficulty level" and "low-probability" (one kind of hardness)

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 = $3.7999142e\text{-}66$ chance of winning the hash puzzle—meaning a Bernoulli trial.

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.

One design that solves many
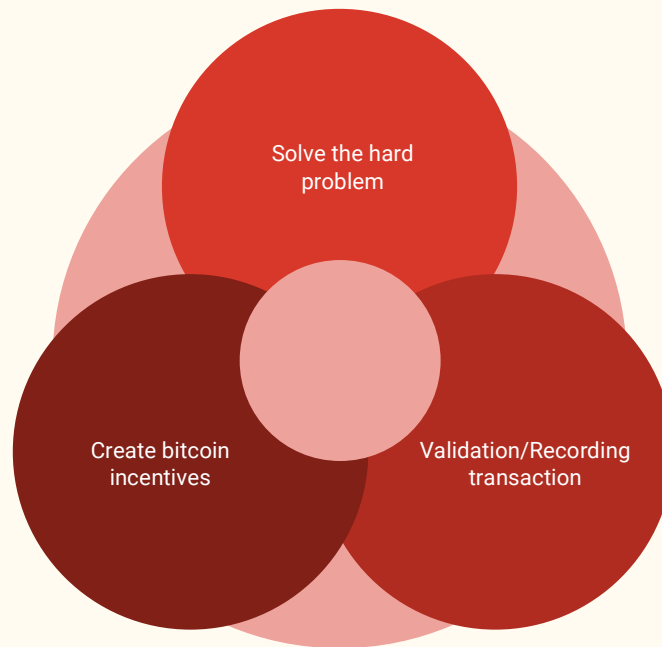
Bitcoin - the great social experiment

- 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.

Add new block to Blockchain

- For blockchain, old data can't be modified but only new data can be added. It's about who can add new legitimate (correct answer and correct construction) block and make others to accept it.
- To add new block, we need to work out the nonce. hash("ABC" + XXXX). Nonce: XXXX
- Satoshi called it **Proof of Work**. The result of PoW (nonce) is the simple number. It can be easily verified by other nodes.
- Low-probability game: every nonce has a 440 billion / 2^256 = 3.7999142e-66 chance of winning.
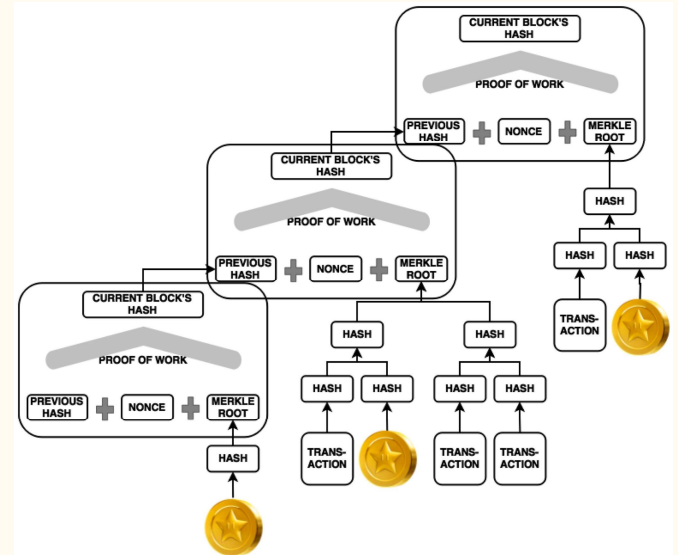
Consensus dynamics

Once a node knows that he is lagging behind the current latest block, he will stop his current effort of solving, download the latest and switch to work on it instead. He hopes to work it out and incentivized. If the node keeps on working his problem and doesn't give up, it's quite sure that he will be always be lagging behind the network and his blocks are not to be accepted by the network. => need more computing. If

Consensus dynamics/2

There could be two solutions worked out almost concurrently. what if? ...let's keep it going until there is one winner of the higher height.

For bitcoin, there was instances that two versions of chain co-existed for about 24 hours but finally one chain won out.

51% Attack and Byzantine Generals' Problem

Related problem, For bitcoin, there is some one controls 51% of the network's computing power (or close to it), someone can create chaos to the network. Alice has the power to rewrite the history and forge the records. This has not happened.

A more academic problem is the Byzantine Generals' Problem is about how to tolerate "traitors" among all generals. Mathematically, more than two-thirds of nodes need to be faithful (Lamport 1982). This requires higher level of loyalty from the participants.

Nakatomo Consensus in Detail

- There is only one way to solve the problem: brute-force.
- Difficulty is adjusted according to the computational power of all participants. To keep only one solution every 10 minutes.
- Who will get the solution? It depends on how much computational power you have and luck.
- There is incentives to **reward** the solution.
- Longer chain is always preferred to resolve conflicts.

http://fermatslibrary.com/s/bitcoin

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.

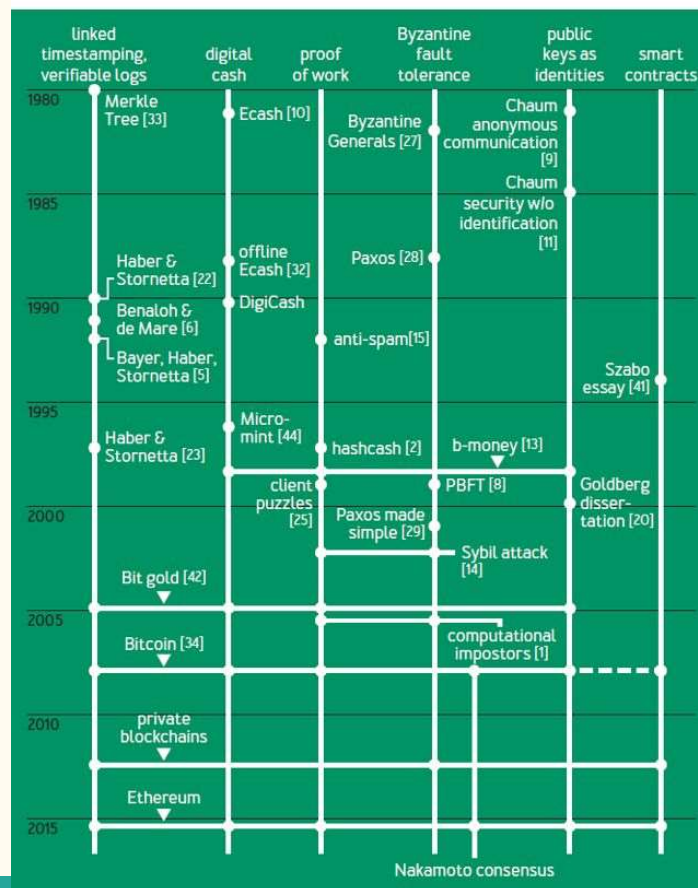# Bitcoin as a descendant of technologies in the last 30 years.

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

Mining

- Therefore, solving the problem has been specialized into "mining". Miners are equipped high-performance computing power and low-cost electricity.
- Mining gear has progressed from CPU, to GPU, to special circuit, ASIC.
- Hashrate is 30PH/s= 30 x 10^{15}. Energy per year is over 63 TWh, between Chile (17mil pop.) and Austria (8.7mil pop.).
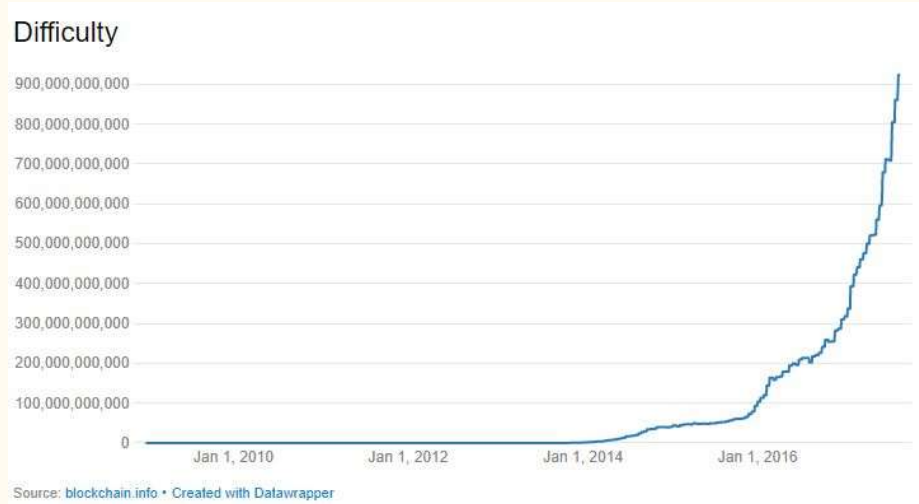
Mining gear

- TSMC's big client is mining chip design company
- Increasing use of special hardware.
- Energy consumption
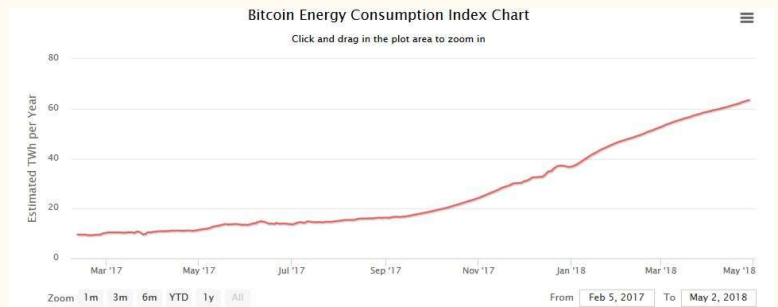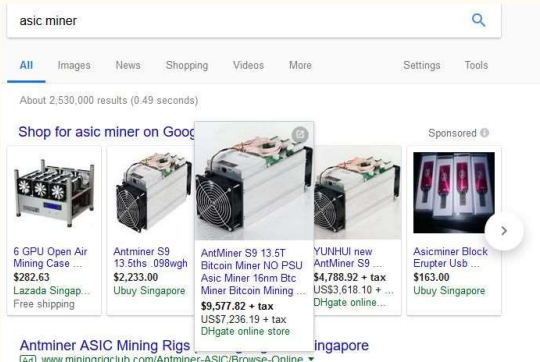
Participants in Cryptocurrencies

- Developer: Application.
- Miners (one with huge computing power): Value and Application.
- Trader: Price.

Mining Difficulty

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.

The infrastructure of Cryptocurrency

There are five parts in the infrastructure:

- Public record - blockchain-based
- Decentralized consensus algorithm
- Economic incentives
- Distributed p2p network
- Transaction authentication and programming

We have covered many aspects of first four aspects. We will continue with the transactional side of the blockchain and more topics. So long, next time!

Just NOT an investment guide

Lecture 12: Transaction and Smart Contract

MFE FE8828 Cryptocurrency Technologies /2

2018/11/26

Yang Ye

Course Overview

Lecture 11: Blockchain and Consensus

Lecture 12: Transaction and Smart Contract

Lecture 12 Transaction and Smart Contract

- Part 1: Transaction
    - Public-key encryption
    - Transaction booking method
    - Transaction flow
- Part 2: Smart Contract
- Part 3: Future (or, in fact, now) technology

Part 1: Transaction

Transaction

- In your normal routine,
    - Take out your wallet from pocket or bag
    - Take out cash
    - Pay
    - Online banking/mobile payment is similar mechanism.
- You own your "wallet" (virtual or real). If anyone gets access to your wallet, they get access to your cash.

Transaction on Bitcoin network

- Your wallet is public as record stored the blockchain.
- Placing the wallet on the table.
- Everyone can see it but only authorized person can access it.

Transactions	Your Balance
You received 100 from Alice.	100 = 100 + 0
You paid 50 to Bob.	50 = 100 - 50

Crypto's Transaction Design

Blockchain needs to take in instructions from outside , verify, validate and execute the transaction.

- Verify: it's authentic from the owner
- Validate: it's valid as a transaction: no over-spending beyond owned.

Crypto Transaction Process

Like a cheque-system but runs with encryption

1. Draft the cheque

2. Sign on the check

3. Post the cheque

4. Network (Bank) receives the cheque, verifies the signature and balance, verifies the payee and does the transfer.

Building Blocks for Transaction

Cryptocurrency builds a network protocol to take on transaction process. The necessary building blocks to enable this are

1. The public key-based cryptography, which provides address, signature and verification process.
2. Transaction booking method.

Public-Key Cryptography

- Public-key encryption: to ensure a message comes from a user by.
- Asymmetric cryptography: public key and private key are a pair. But it's one-direction (asymmetry), private key can verify a paired public key but public key can't deduce what its paired private key is.

Public and Private Key in action

Public key can encrypt. Private key can validate and decrypt. If validation fails, decryption also fails.
Alice use Bob's public key to encrypt. Only Bob can decrypt with Bob's private key.
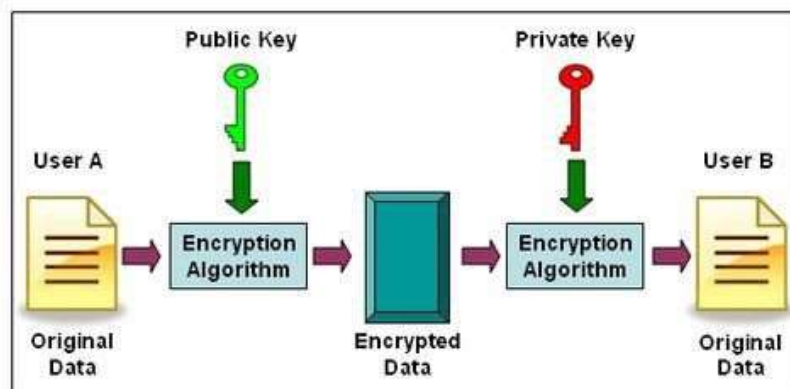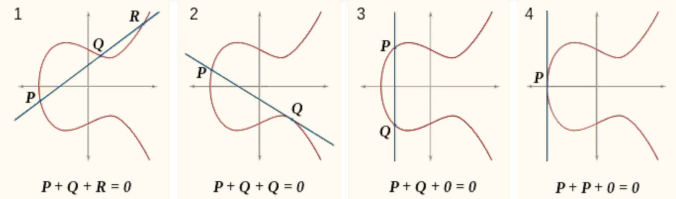
Some cryptographic 2

- 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

How to use biginteger to build a public key/private key pair:

$$p * q = R, R \text{ is a very big integer}$$

Big integer factoring is a "hard problem".

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.

Public-Key Infrastructure

- A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Why we need PKI?

Our previous example introduced Charlie, the listener. I said that we assume Charlie only intercepted the hashes not the message. In fact, Charlie can intercept any message. Hash (only does validation) is not sufficient. We need encryption of the data.

Charlie

Bring me the rabbit!

Alice

0fbf2612

Bob
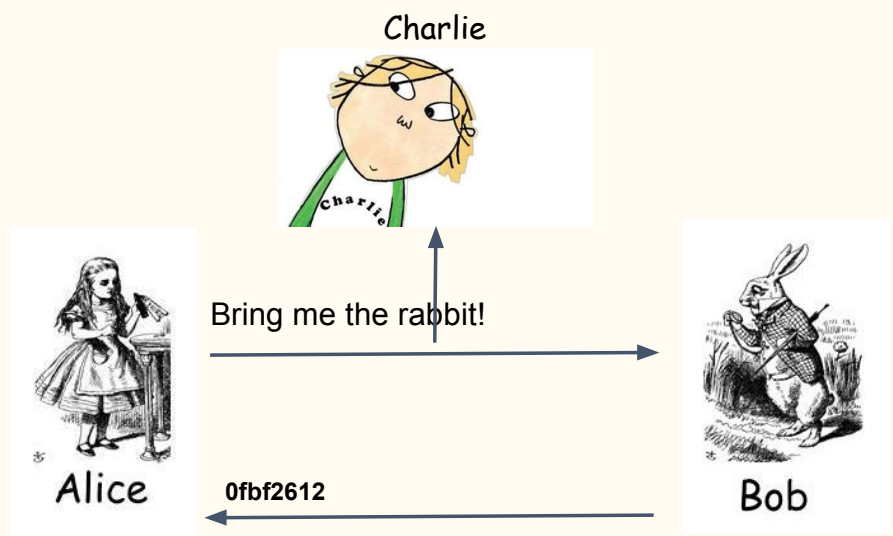
Before communication, Alice and Bob needs to discuss how to encrypt the conversation. Then they begin the encrypted communication. PKI defines a formal way of encrypted communication.

Transaction booking

In bitcoin, a transaction is a list of inputs and outputs, with each input pointing to the output of an earlier bitcoin transaction.

Each output specifies the conditions that need to be satisfied in order to spend the coins in that output. The simplest transactions just require a digital signature—cryptographic proof that a transaction has been approved by the owner of a particular private key.

Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin
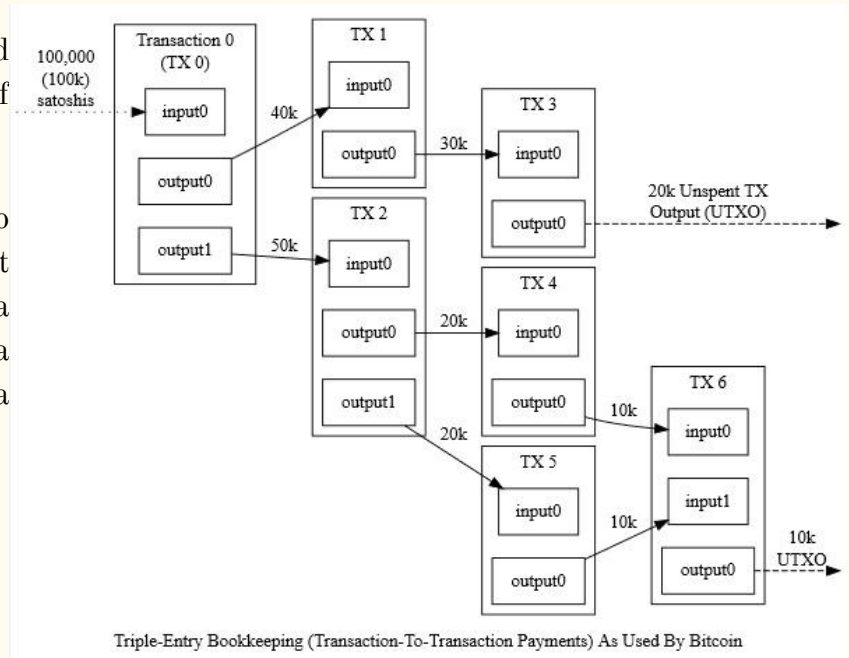
Receiving before spending

- Alice wants to send Bob 3 coins.
- Bob provides the pubkey hash (just the hash, as) to Alice.
  - Note: The hash shortens and obfuscates the public key. Satoshi preferred "additional security measure", like the use of double SHA-256.
- She creates a transaction, recording Bob's pubkey.

Alice broadcasts the transaction and it is added to the blockchain. The network categorizes it as an Unspent Transaction Output (UTXO), and Bob's wallet software displays it as a spendable balance.

In summary, a transaction creates at least an Input and Output.

Spending it

In order for Bob to spend it, he creates a new transaction which provide three items. Two items are "Double-verification" of identity. One for receiving.

- **His full (unhashed) public key**, so the pubkey script can check that it hashes to the same value as the pubkey hash provided by Alice. ("Check Bob's IC")
- **An secp256k1 signature** that combine certain transaction data with Bob's private key. This lets the pubkey script to use public key to verify that Bob owns the private key. ("Let Bob sign")
- **An new wallet with an input** points back to Alice's transaction's output. ("Transfer")

Bob broadcasts the transaction to Bitcoin miners through the peer-to-peer network. Each peer and miner independently validates the transaction before broadcasting it

Bitcoin transaction summary

- Each transaction has at least one input and one output.
- One wallet can only be used once.
  - Say I have 10 BTC in my wallet "IronWolf" and I want to give "Baracuda" 2. Then I need to create new wallet "IronWolf2". The transaction will say "Take the 10 BTC from IronWolf, give 2 to Baracuda and give 8 to IronWolf2".
- Because each output of a particular transaction can only be spent once, the outputs of all transactions included in the blockchain can be categorized as either Unspent Transaction Outputs (UTXOs) or spent transaction outputs. For a payment to be valid, it must only use UTXOs as inputs

Transaction summary

- The transaction process of Bitcoin is a product of very careful thoughts of security and process.
- This is a particular model of transaction. Other cryptocurrency system may opt for other kinds of process.
- Transaction is a key mechanism for blockchain. Its function ensures a secure and speedy transaction.

Part 2: Sma Contract
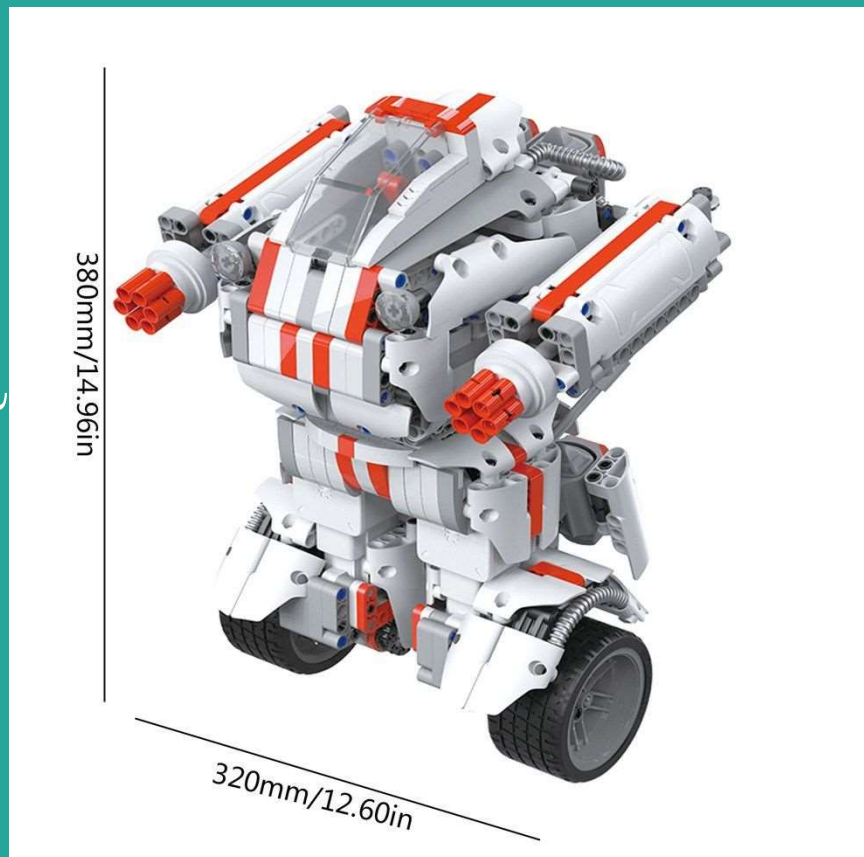
Smart Contract

- Everyone would like to have a robot assistant to follow our orders and do our tasks.
- Smart contract is a robo-assistant to facilitate, verify and enforce the real contract
- Smart contracts were first proposed by Nick Szabo, who coined the term, in 1994.

Smart contract Advantage

- Smart contract is to provide more security that is superior to traditional contract and reduced transaction cost.
- Smart contract removes middle-man as notary and executer. "No agent, No lawyer and No policeman"

Smart contract with Blockchain

- Blockchain stores asset/cryptocurrencies. Because economics is one big component in contract. Various cryptocurrencies have some implementations for smart contracts.
  - Bitcoin has had, from the very beginning in 2009, a pretty extensive smart contract language called Script.
  - Ethereum calls it "a decentralized platform that runs smart contracts."

How Cryptocurrency will do smart contract

- "Smart contract code": Code that is stored, verified and executed on a blockchain.
  - The most widely discussed opportunity of this type is machine-to-machine commerce. For instance, a washer that buys its own detergent or a car that can pay to recharge itself.
- The growing ecosystem of smart devices - will eventually need a way to engage in basic commercial interactions with one another.

How Cryptocurrency will do smart contract

- "Smart legal contracts": as a complement, or substitute, for legal contracts. Let's name these
  - These smart legal contracts would most likely be a combination of smart contract code and more traditional legal language.
- This takes more than technology. It needs to move entire asset/legal doctrine online.
- Maybe AI and Blockchain would lead us a bit closer to this.

What could be soon?

- "Smart contract code"
  - Financial instruments are just one type of contract that could benefit from blockchain code. As the technology matures, other assets - e.g. real estate, or intellectual property - may be stored and traded over blockchain systems.
- Central bank may play a big role here while closed-loop community, e.g. game, virtual world, would get the first implementation.

Part 3: Future (or, in fact, now)

Development theme

- Speed of Function
  - Distributed or centralized
    - Authority
    - Data
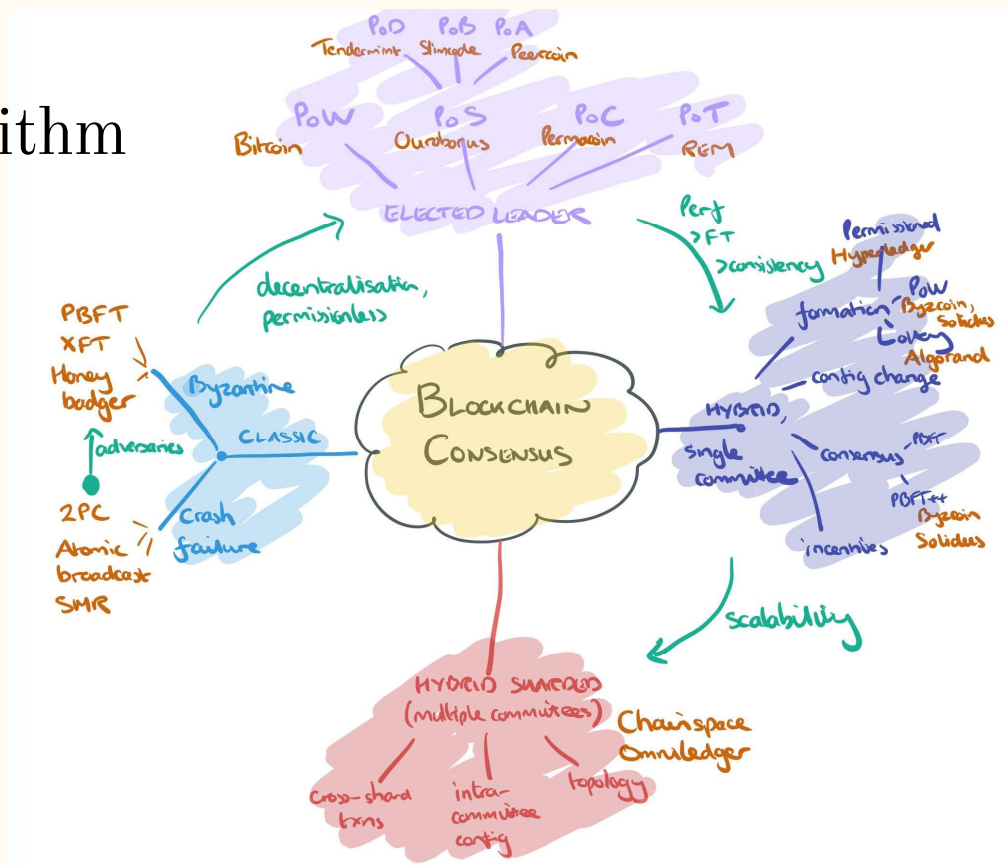- Security

Consensus Algorithm

PoW: Bitcoin. Computing power!

PoS: Proof-of-Stake: Ethereum.
More holding tokens.

PoA: Permissioned blockchain.
Appointed nodes (central model)

...

https://blog.acolyer.org/2018/0
2/12/sok-consensus-in-the-age-o
f-blockchains/

Sharding

Non-sharding blockchain would make update of data global so all nodes know what's happening
Sharding is to have divide nodes into shard and each shard has its own transaction history so node
only need know a fraction of the "world".
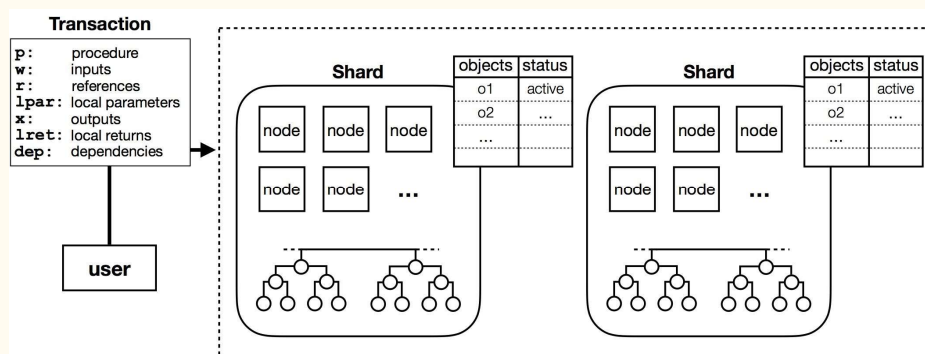
Security

- Ownership
- Smart contract Security
  - Wrong code
  - Hacker attacking buggy code
- Consensus:
  - Byzantine General problem
  - Fake transaction
  - Decentralized and centralized

Ownership

"Ownership simply means knowing a private key which is able to make a signature that redeems certain outputs — an individual owns as many bitcoins as they can redeem."

Lost private key = lost wealth

Man Who Threw Away a Fortune in Bitcoin Now Looking to Dig Up a Landfill

Bryan Menegus
12/04/17 6:28pm · Filed to: DIRTCOIN ⌄

338.3K 144 4

LOUISE MATSAKIS SECURITY 05.28.18 07:00 AM

HOW WIRED LOST $100,000 IN BITCOIN

Bug in Smart contract code

- In 2016 when a hacker stole $50 million from the so-called Decentralized Autonomous Organization, which was based on the Ethereum blockchain. Through a "hard-fork" (rewriting blockchain), recovered most.
- And in November around $150 million suddenly became inaccessible to users of the wallet service Parity, which is also rooted in Ethereum.

Summary

- Bitcoin as Blockchain 1.0 has many designs to make it decentralized, except the mining part.
- Other latecomers are are still experimenting features. There is no set of features can be officially called "2.0".
- The future lies in moderating between "Decentralized" and "Centralized", "Security" and "Functional"