My Notes on Blockchain, Cryptocurrencies and Smart Contracts.

~ by **Yashraj 'whynesspower' Shukla** 15th Oct 2021

NOTE: The following notes are a personal property and are distributed for individual educational purposes. I am not liable for any misuse of the knowledge provided by me.

'For best practice, kindly also read out all the mentioned articles and additional readings'

Lets connect !:

https://www.linkedin.com/in/whynesspower
https://www.linktr.ee/whynesspower

BLOCKCHAIN

Blockchain is a continuous growing list of records, called blocks which are linked and secured using cryptography.
Every block has previous hash, current hash and some data.
Genesis Block means the very first block, it has no previous hash.
Read *"How to time stamp a digital document"*
https://tools.superdatascience.com/blockchain/hash/

SHA256

256 bits size
64 characters long
Hexadecimal hash, alphanumeric
Made by NSA

https://tools.superdatascience.com/blockchain/hash

Hash Algorithms

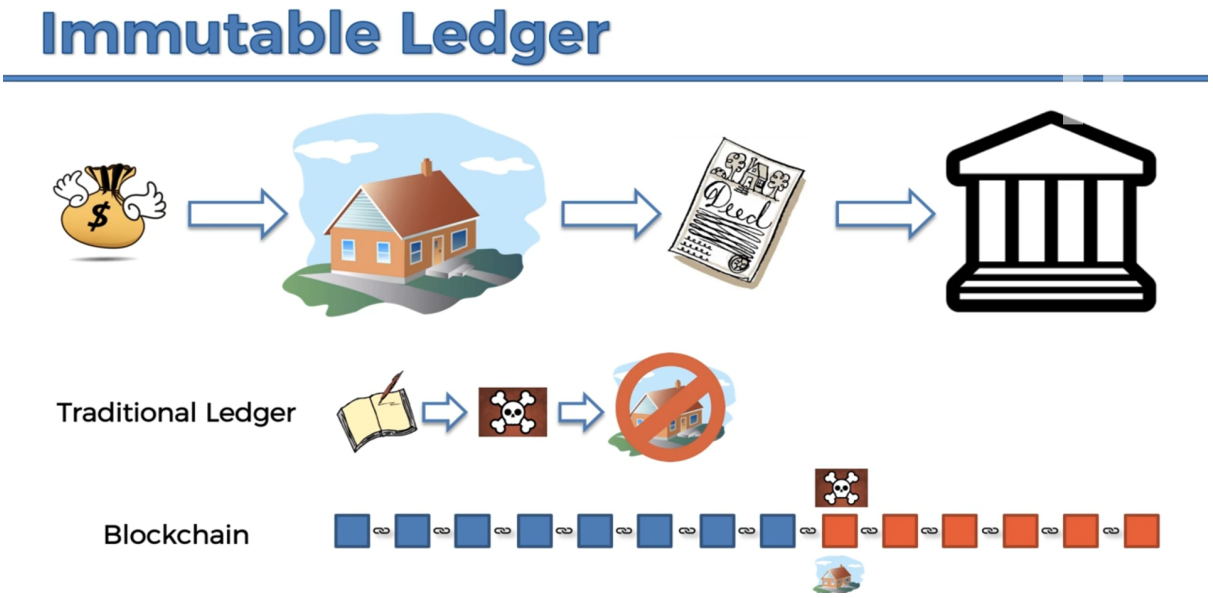
Sha256 is the best hashing algorithm out there as of now.
Top 5 requirements of a hash algorithm

1. One Way
2. Deterministic
3. Fast Computation
4. Avalanche Effect
5. Must withstand collision

Read "On the secure hash algorithm family (chapter 1 of cryptography in context)"

Immutable Ledger-

Blockchain acts like an immutable ledger. It has power to replace traditional physical ledgers at government offices and can digitise the whole propress of government recording keeping securely.

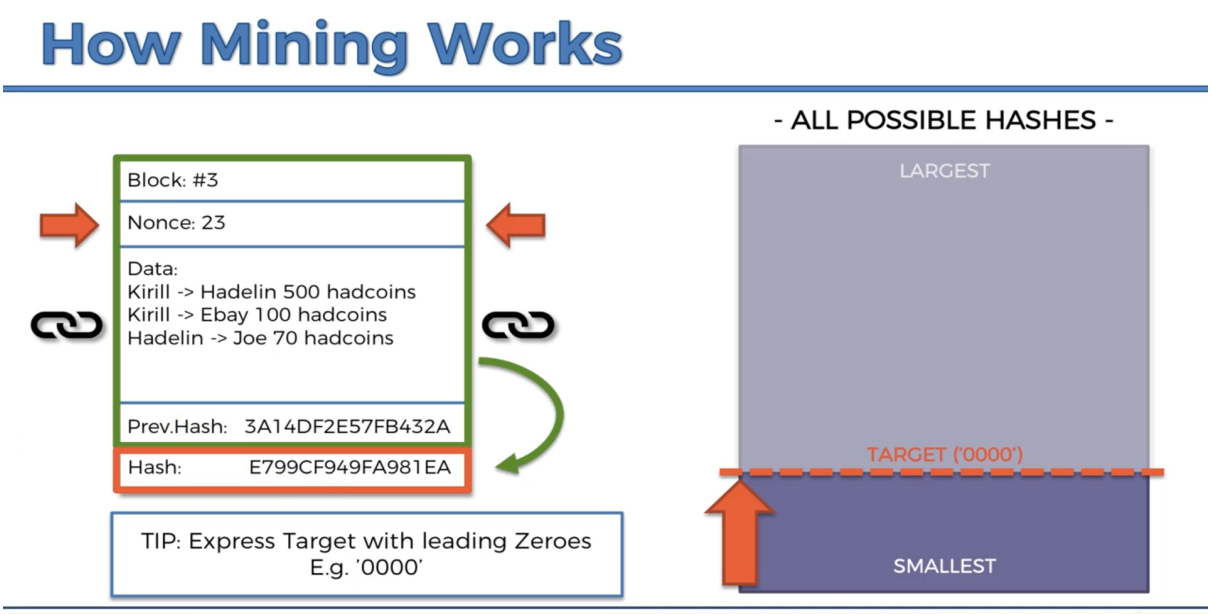


Distributed P2P networks

Provides one additional layer of security to the blockchain. As the same ledger or the blockchain is copied to a lot of computers at once, if one copy of the chain in somebody's computer is tempered, or hacked, instantly the blockchain copy which is running in majority computers will be copied to this computer too. The only way to hack a blockchain is to temper the blockchain of more than 50% of the computers at once.

Read *"the meaning of decentralization"* by vitalik buterin

Mining

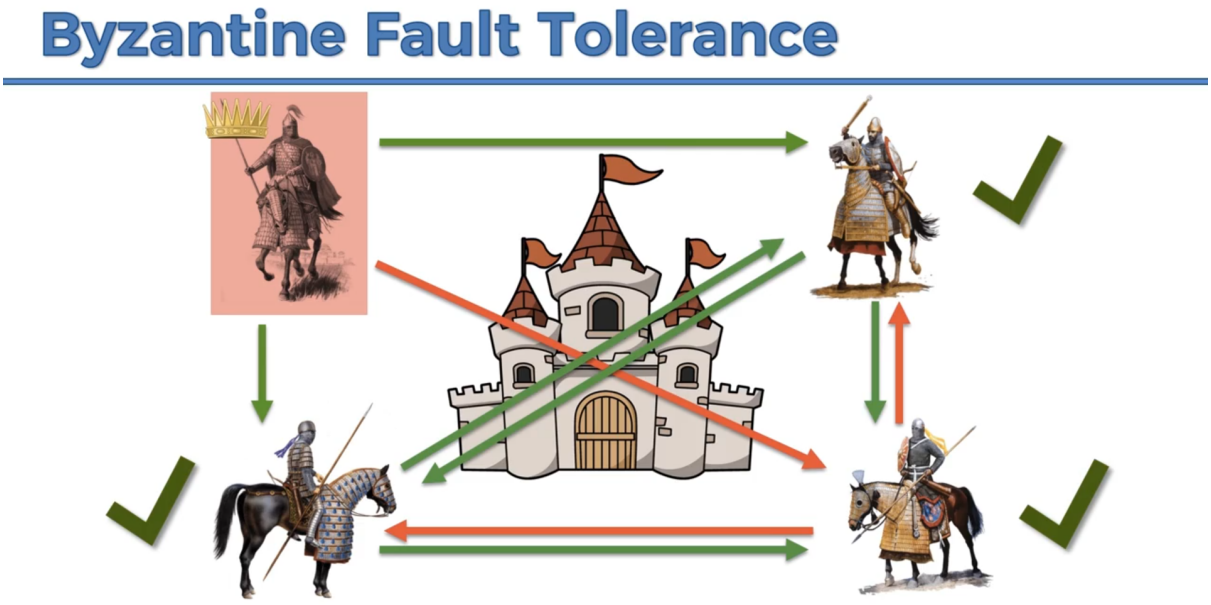


Nonce exist so that you can change the hash numbr of a block without chaning data or anything else.

Byzantine fault tolerance

Byzantine Fault Tolerance is a mechanism that enables a decentralized, trustless network to function even in the presence of malfunctioning or malicious nodes. No more than 33% should be traitors, for this algo to work Byzantine Fault Tolerance (BFT) makes it possible for a network to continue functioning as long as two-thirds of the network remains compliant.

.



Read *"the byzantine generals problem"*

Read *“understanding blockchain fundamentals part 1 BFT”*

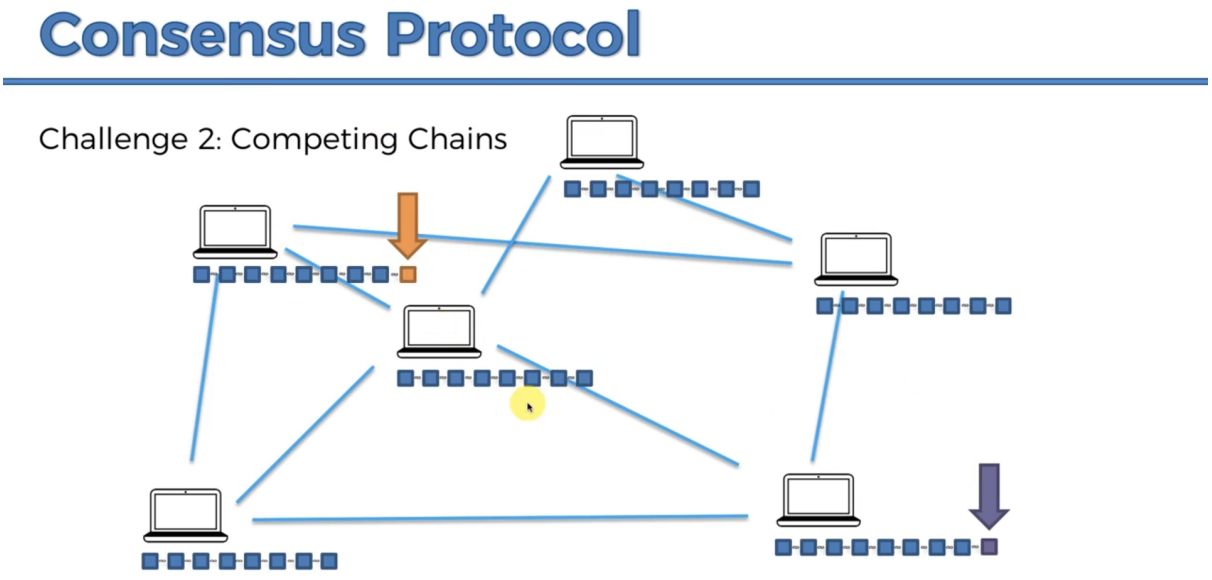
Consensus Protocol

Miner get money to successfully mine a block and also for playing fair.
Before a block is added a series of checks are done, to check if the block is legal or not.
There is a whole list of checks which have about 25+ items.

Consensus Protocol handles two tasks like -

1. Attackers adding malicious block
2. Competing chains which by chance have mined one different block then the other one.

A miner can’t add a fake block into the blockchain as all the other peers verify the block being inserted through a series of 100+ checks.
Cryptographic puzzel is hard to solve but easy to verify
Read “Re: Bitcoin p2p e-cash paper” by satashi nakamoto



For example say there are by mistake two different competing blocks added, orange and purple. Now these two blocks are propagated to different computers. And the computer which computes the next coming block first, the blockchain of that computer becomes the next official block chain, either with the orange or the purple block.
Some consensus protocols are Proof of work, proof of stake.

Read: Bitcoin P2P e-cash paper - Satoshi Nakamoto
Read: Amy Castor - A short guide to bitcoin consensus protocol

==========

CryptoCurrency Inituation

1. Protocols: is the set of rules which guides how participates over a network communicate with each other eg TCP, HTTPS
2. Every protocol has a coin attached to it. Bitcoin protocol has bitcoin as its coin and so on.
   Read: Bitcoin - A p2p electronic cash system by satoshi nakamoto

Bitcoin Monetary Policy:
Has two parts: 1. The Halving and 2. Block Frequency

The Halving:-

Bitcoin is a deflation type of currency. With time passing, one bitcoin will be able to buy more stuff.

The Halving

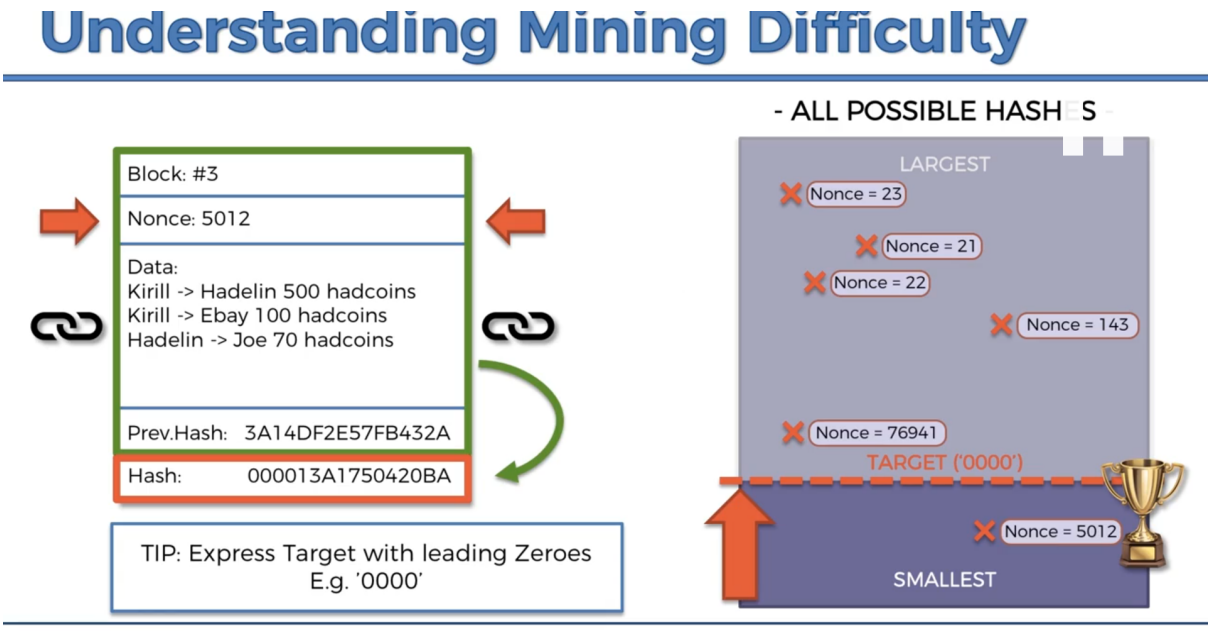
~2020: 6.25

~2024: 3.125

Date reached	Block	Reward Era	BTC/block
2009-01-03	0	1	50.00
2010-04-22	52500	1	50.00
2011-01-28	105000	1	50.00
2011-12-14	157500	1	50.00
2012-11-28	210000	2	25.00
2013-10-09	262500	2	25.00
2014-08-11	315000	2	25.00
2015-07-29	367500	2	25.00
2016-07-09	420000	3	12.50
2017-06-23	472500	3	12.50

Read: This Time is Different Part 2: What Bitcoin Really Is.

Mining Difficulty-



Probability to mine a valid block.

Current target = 00000000000000000 5d97dc0000000000000000000000000000000000000

18 zeros

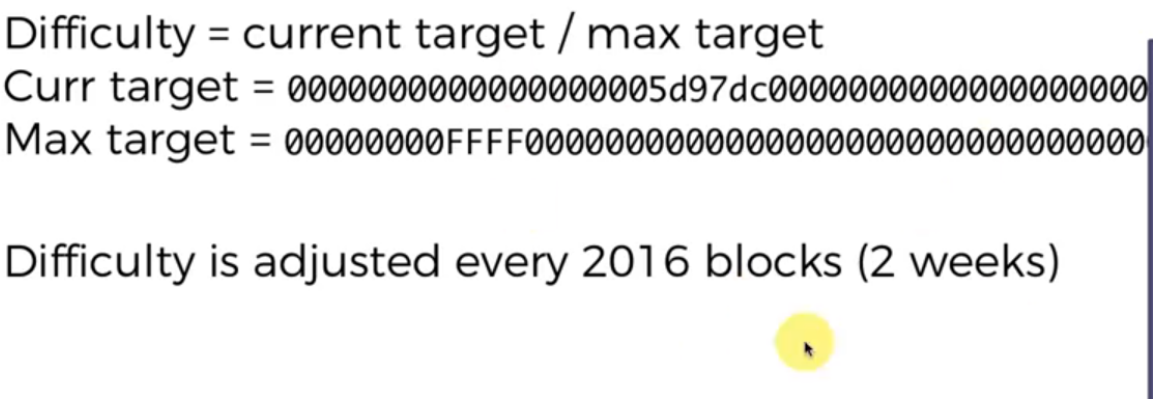
Let's do some estimations:

Probability:
Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$
Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Difficulty to mine a block

Difficulty to mine a block is adjusted every 2 weeks so that only one block gets mined every 10 minutes.



Mining Pools
There are public mining pools and big companies/organizations in which individual retail miners like us participate and hashing power is combined. All the profit which your organiations generates will be divided in proportion to your hashing power.

China has the biggest mining pools companies. Countries excess energy which was before going to waste is now used in mining pools .

Read: Bitcoin mining and energy consumption by Leo Weese

- How mempools work
- Orphaned blocks
- 51% attack

Blockchain Transactions:

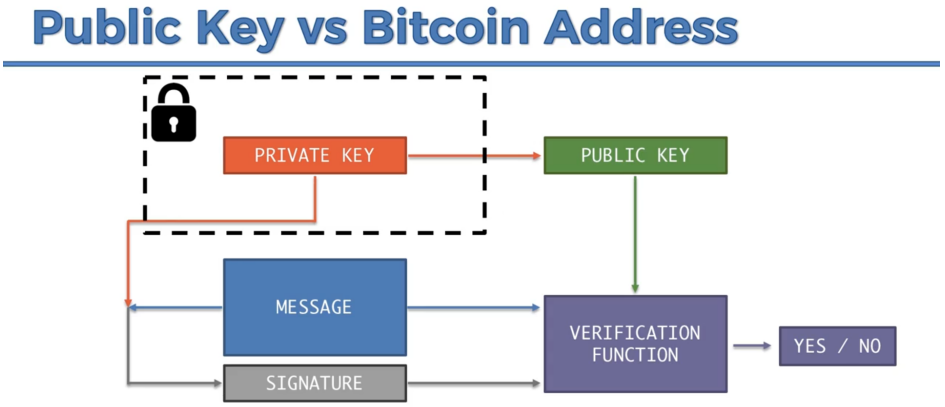
- UTXOs
- Where do transaction fee come from
- Wallets and UTXOs

25th Dec 2021 -

- Signature, Private and Public Keys.

1. Strong miners who can go through the range of nonce in less than a second(i.e before the timestamp changes) can change the configuration of the block, select some other transactions ID, and go over the nonce again.
2. You might have to accelerate your transaction if no miner is picking it, using third party service.
3. You can’t use ASIC when mining Ethereum as they are memory dependent and hence to calculate Eth-Hash is limited to your memory access speed.
4. You can’t compare the harshing power between two different cryptos as every crypto has varying level of mining difficulty
5. Always wait for 5 blocks to be mined after your block for your transaction to be considered successful. So that your block doesn’t get orphaned.

6. The 51% attack
7. Deriving the current target from decimal to hexadecimal
8. You calculate the balance of your wallet by summing up all the UTXOs of your account, unspent transactions output
9. Public keys are like you bank acc numbers, private keys are like password of your bank account number
10. **Segregated Witness** or SegWit, is the process by which the block size limit on a blockchain is increased by removing signature data from transactions that are included in each block. ScriptSeg is removed from the block



- You can use your bitcoin address instead of your public key to receive BTC
- Elliptic functions are used to verify if a particular signature is indeed coming from a certain private key or not.
    - Private key + message(transaction info) = signature
    - Signature + public key + message = verify if signature was indeed generated by certain private key.
- For transactions share your btc address, which is generated after you sha256 encrypt your public key, which is generated when you elliptically encrypt your private key
- Heirarchael Deterministic wallets(HD wallets) have master private key to generate a whole set of private keys. These have mnemonic to remember your master privatekey.

==========Smart-Contracts==========
26.12.2021

- Read: [What is Ethereum? | The Ultimate Beginners' Guide - CoinCentral]
- Smart Contracts

    - When you can create code or scripts over a existing blockchain of a cryptocurrency, you can create smart contracts over it.
    - Bitcoin script, solidity are such languages, Bitcoin script is turing incomplete because you can't code loops in it. Vitalilk buterin advocated for bitcoind script to include "loops" so that many projects can be created over bitcoin blockchain
- DApps: apps which have a frontend and backend as smart contracts over blockchain, smart contracts acts as a API to connect with blockchain in these apps.
- Ethereum Virtual Machine: Prevents virus hidden in smart contracts to spread, and privacy protection, your smart contract can't access anything outside EVM.
- Gas fee means that every computation that you do on blockchain is going to cost you gas. Due to this you can't write inefficient code in blockchain. Which keeps web3.0 fast and efficient. Read: Calculating Costs in Ethereum Contracts | Hacker Noon
- Gas is used instead of Ether as a currency to run operations of blockchain because ether is very volatile.
- DAOs decentralized autonomous organisation: When you create a organization which has director, managers and employees are smart contracts of blockchain read:DAOs, DACs, DAs and More: An Incomplete Terminology Guide | Ethereum Foundation Blo

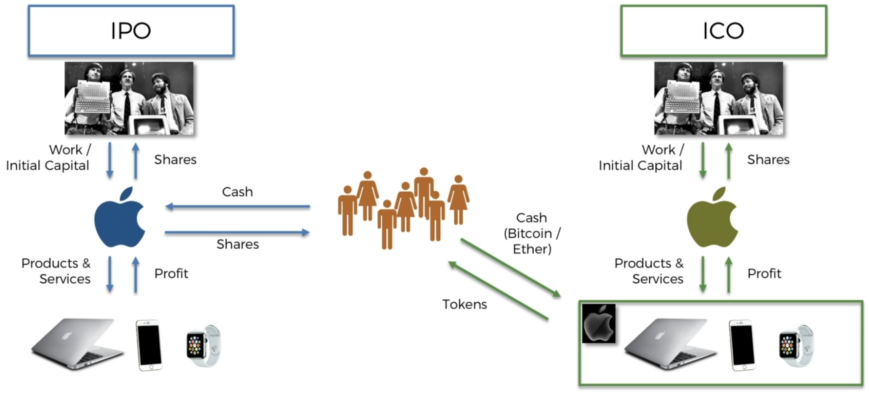
- DAO attack: DAO was itself an organization based on ethereum, which helped others to create other decentralized oraganizations on ethereum. It was croudfunded $150M. Hackers attacked the DAO found a flaw in the smart contract and got $50M dollars. Ether Thief Remains Mystery Year After $55 Million Digital Heist (bloomberg.com)
- Soft Fork: changes happen in the blockchain but those changes don't result in a separate chain. Hard Fork: changes happene and these also result a whole separate chain from the old chain.

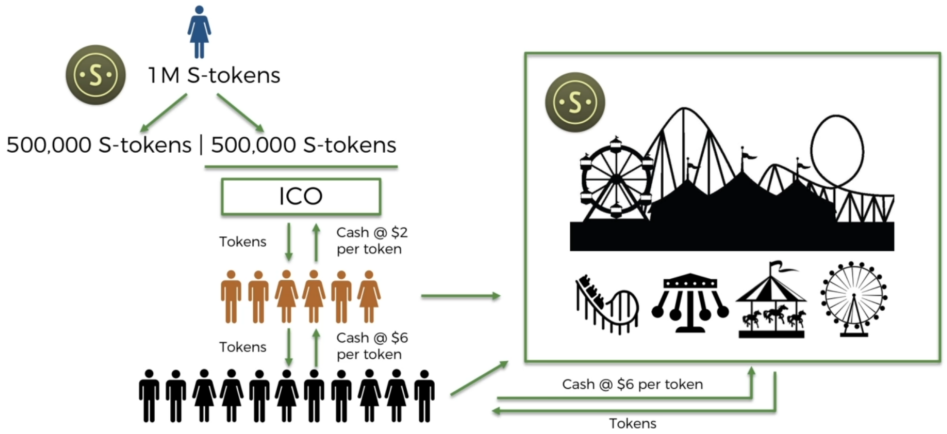
2016
On Ethereum
Investor-directed venture capital fund
Stateless
May 2016 Crowdfunded ~$150,000,000
June 2016 Hacked for ~$50,000,000
Dilemma: *"Code Is Law?"*
Hard fork
Ethereum split into ETH and ETC
Hacker walked away with ~$67,000,000 in ETC
Problem in DAO code not Ethereum

- If you own 1 bitcoin before hard fork, after the hard fork you willl still have 1 bitcoin plus 1 bitcoincash and 1 bitcoin gold.
-
- Hard forks are not backward compatible

Hard Forks = Loosen Rules

Soft Forks = Tighten Rules

-
-
- 

- ICO is another way for a company to raise money, a company creates a product and for those product it creates tokens and says that all the company's product will be sold only via these tokens, people can invest in these tokens when they get launched first, ICO, or they can also trade these tokens
- 

- For finding which Tokens are real purpose tokens and which ones are just pump and dump scheme, real white papers of the startups, you need tokens and coins when you create a micro economy of your own business.
- Web 3.0 means when the backend of the website will be hosted on a blockchain instead of a central server. Tho a particular users data exist on the blockchain, only the person with private key can access it.
-

Articles

How Bitcoin Mining Works - CoinDesk
Ethereum's Memory Hardness Explained — VIJAY PRADEEP
An in-depth guide into how the mempool works | by Marion Deneuville | Kaiko
Choosing ASICs for Sia. We recently announced that we would be… | by David Vorick | Sia and Skynet Blog

Understanding Segwit Block Size. After I wrote my last article, I was… | by Jimmy Song | Medium
Deterministic Wallets, Their Advantages and their Understated Flaws - Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides

What is Ethereum? | The Ultimate Beginners' Guide - CoinCentral
Blockchain: the solution for supply chain transparency | Provenance
Smart Contracts for Dummies (freecodecamp.org)
Nice DApp: Trending posts — Steemit
Calculating Costs in Ethereum Contracts | Hacker Noon
Ether Thief Remains Mystery Year After $55 Million Digital Heist (bloomberg.com)
Complete Guide on Bitcoin and Blockchain Forks — Steemit
WTF is an ICO? – TechCrunch
ICO Case Studies
What the heck is an ICO? | Hacker Noon
How Crypto Tokens Will Enable the Disruption of Businesses like Uber and Airbnb – Finn's Cave (finnscave.com)
Web3.0 Why the Web 3.0 Matters and you should know about it | by Essentia 1 | Medium