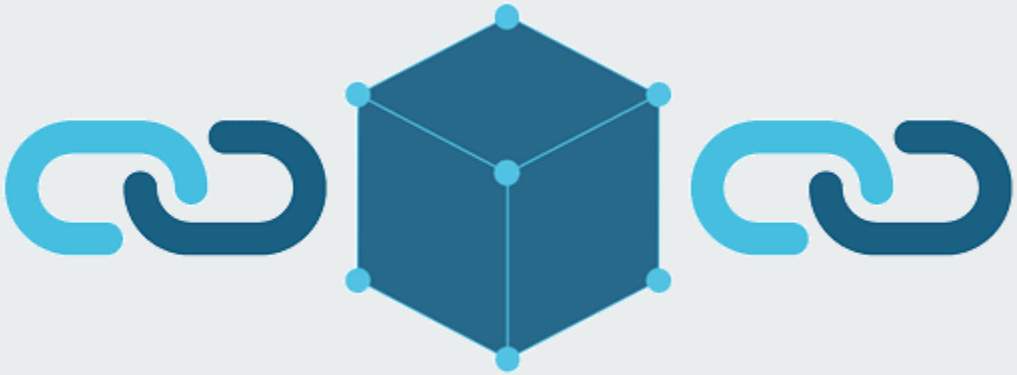
Blockchain, Crypto and NFT

KAVEH BAKHTIYARI



TOC

Overview

Blockchain Ledger

Consensus

Consensus Algorithms

Proof-of-Work

Bitcoin vs. Gold

Smart Contract

Ethereum Gas

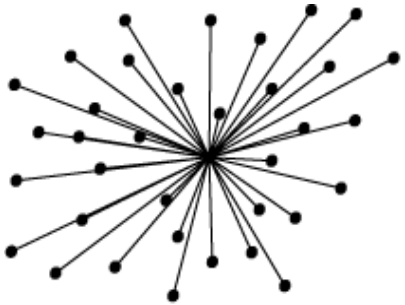
Smart Contract Limitations

Oracles

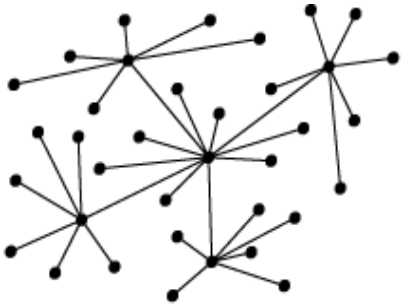
NFT

Bitcoin vs. Ethereum

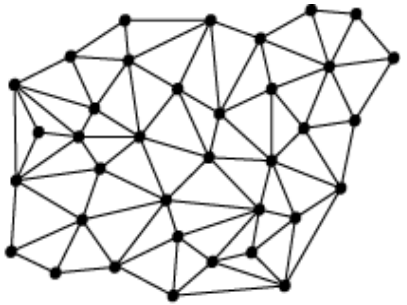
Overview



centralised



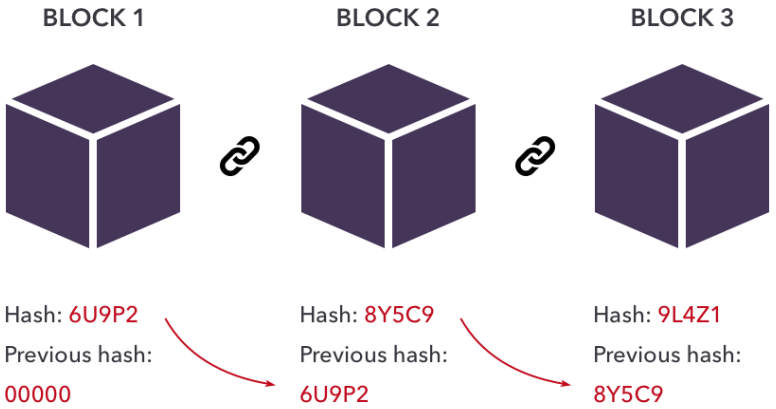
decentralised



distributed

Blockchain

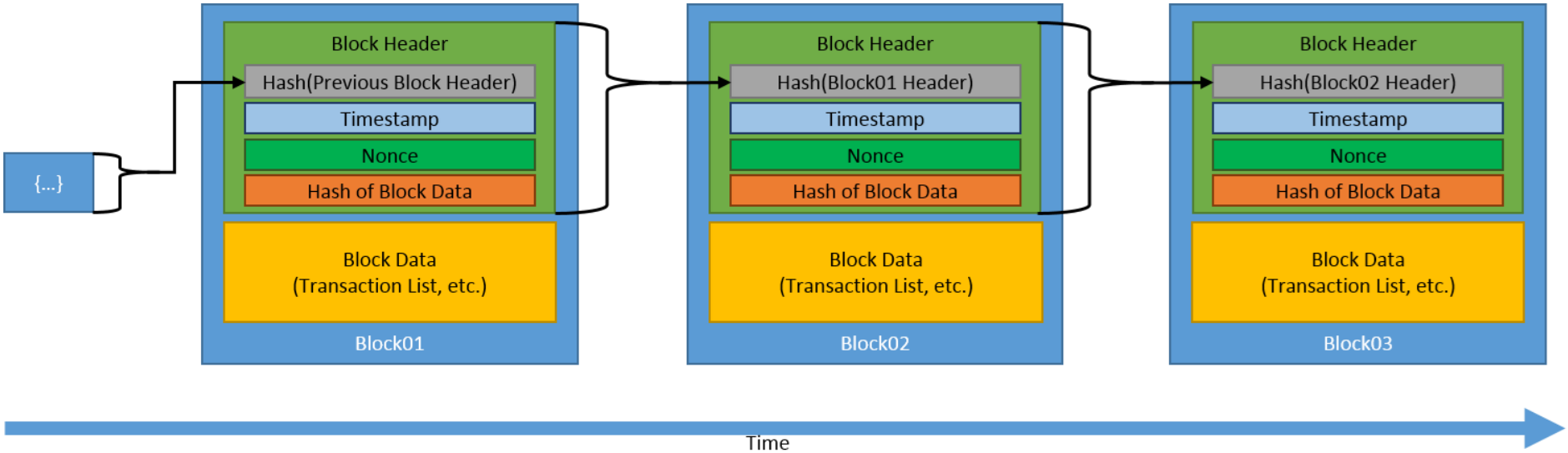
A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). By design, a blockchain is resistant to modification of its data.



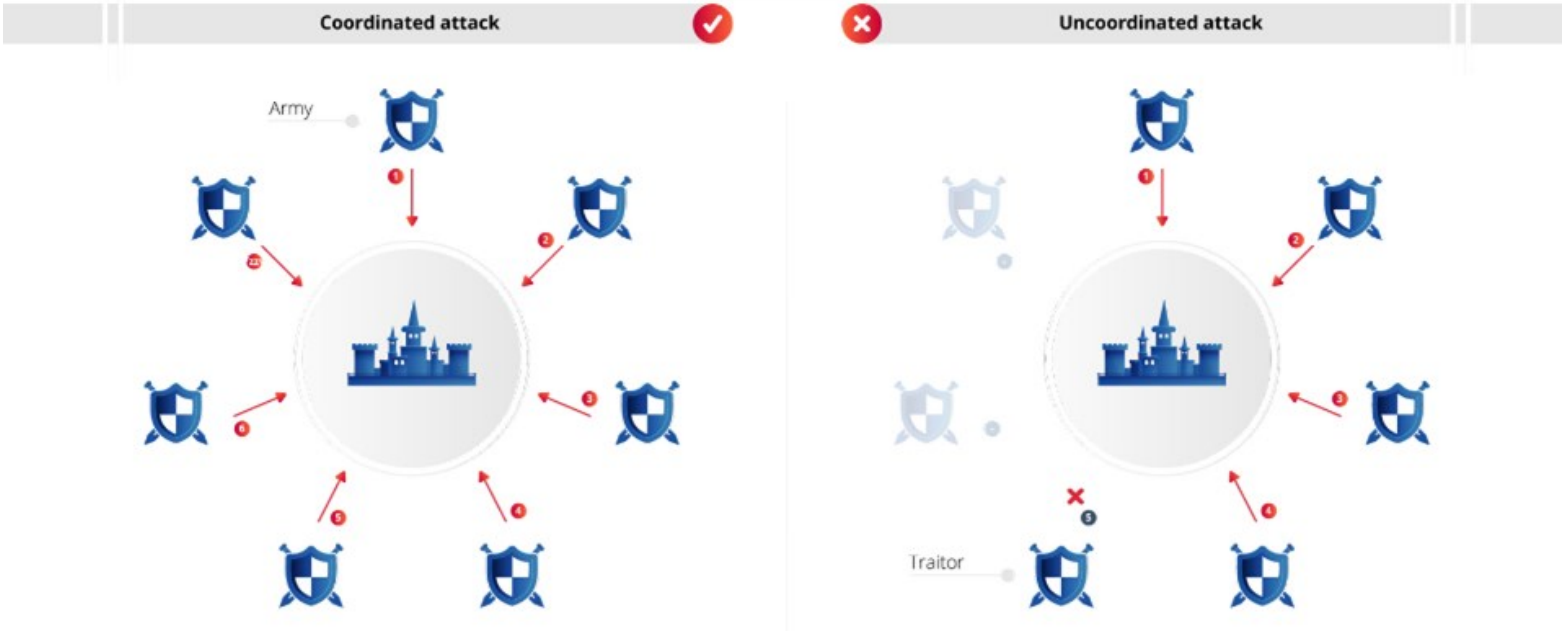
The blockchain was invented by a person (or group of people) using the name **Satoshi Nakamoto** in **2008** to serve as the public transaction ledger of the cryptocurrency bitcoin.

Source: https://en.wikipedia.org/wiki/Blockchain

Blockchain Ledger

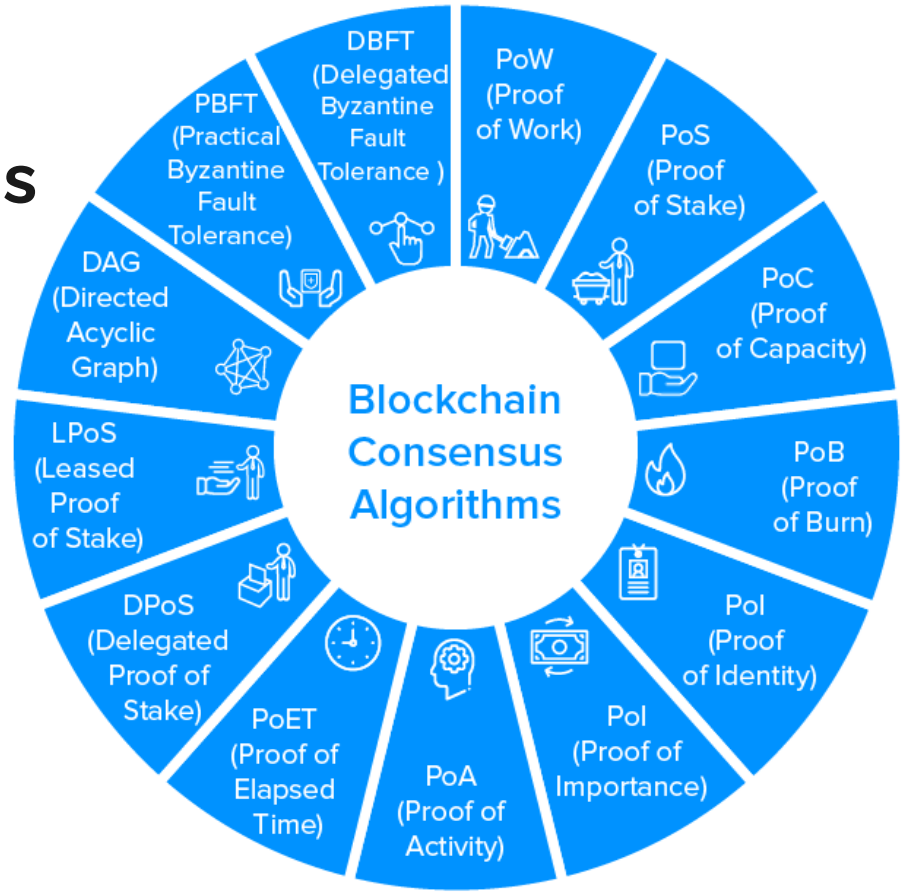


Consensus: Byzentine Fault Tolerance

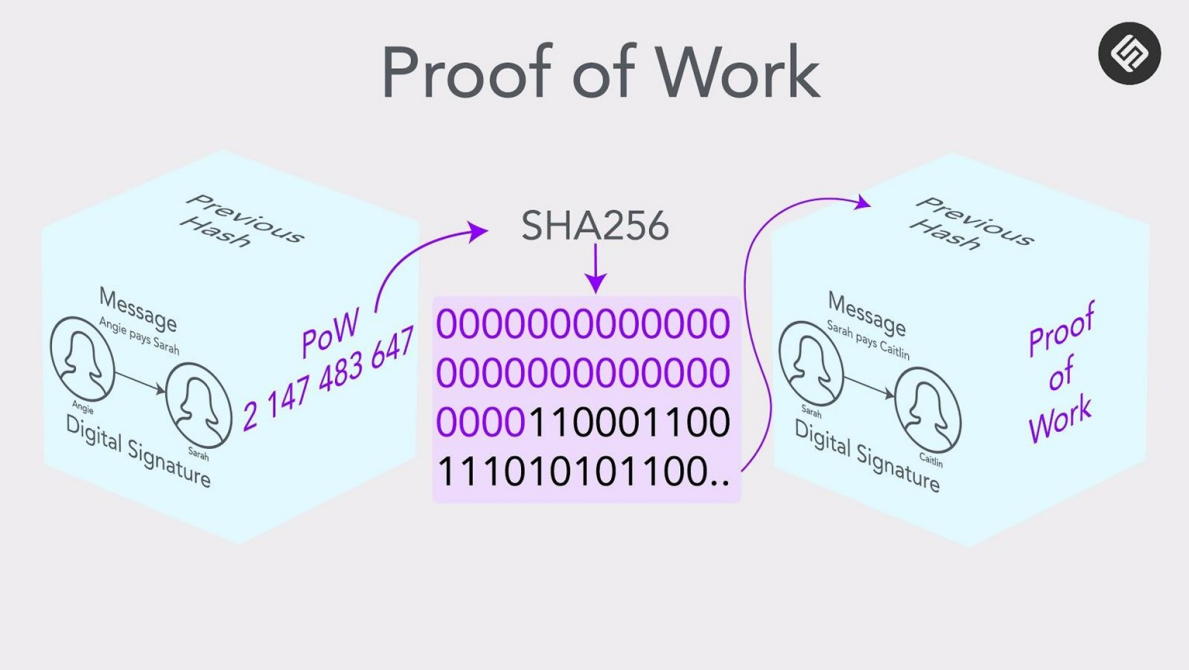


Consensus Algorithms

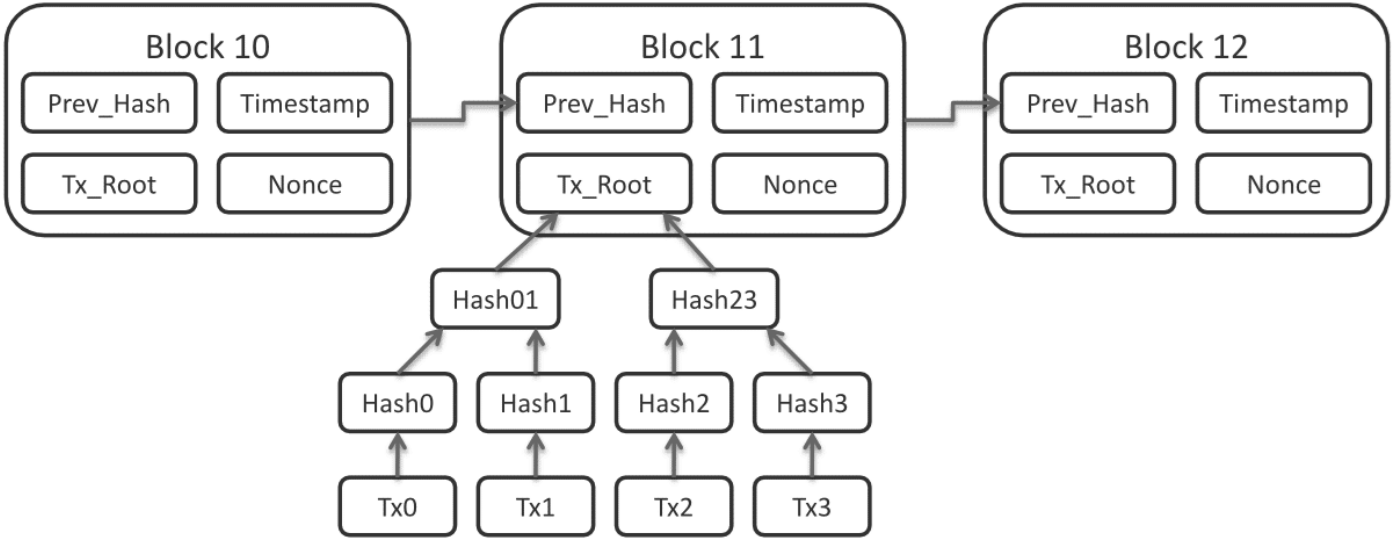
- **Bitcoin**: Proof-of-Work
- **Ethereum**: Proof-of-Work
- **Ethereum 2.0**: Proof-of-Stake



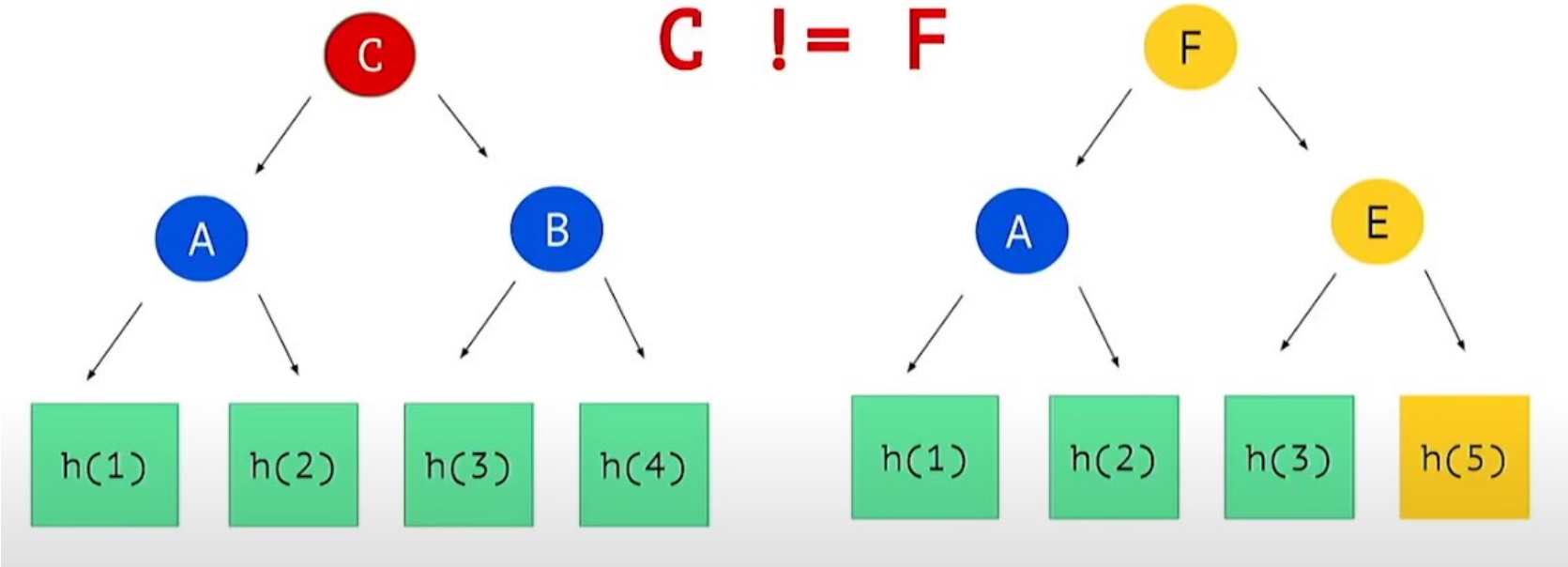
Bitcoin: Proof-of-Work



Bitcoin: Proof-of-Work

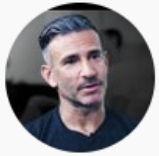


Merkle Tree



Bitcoin Mining & Reward

- Participants in the game of creating blocks are called Miners.
- Miners reward themselves a number of coins (e.g. Bitcoin) for solving the puzzle, which those coins are mined (newly minted) coins.
- The reward at the beginning of Bitcoin was **50 coins per mined block**, and over time it decreased.
- Number of rewarded coins is being halved **every 210,000 blocks** which is approximately equivalent to **every 4 years**.
- The last time it was halved was in **May 2020** and it is currently at **6.25 coins** per mined (created) block.



Josh Wolfe @wolfejosh · Aug 16, 2018

Q: How do I explain Bitcoin to my grandpa?
A:

> 
> **kraft dinar** @Theophite · Aug 16, 2018
>
> Replying to @am_anatiala
>
> imagine if keeping your car idling 24/7 produced solved Sudokus you could trade for heroin

60 2K 5.4K

Source: https://twitter.com/wolfejosh/status/1030292330513924097

Energy Consumption

In 2018, Ethereum mining consumes a quarter to half the energy of what Bitcoin mining does, however that still corresponds roughly **as much electricity as Iceland consumed**.

Source: Luxury fashion brands poised to join the NFT party: https://www.voguebusiness.com/technology/luxury-fashion-brands-poised-to-join-the-nft-party
Image Source: https://expertvagabond.com/iceland-facts/

Bitcoin vs. Gold

Bitcoin

21M

Maximum number of possible Bitcoins to mine - 89% mined, around 2 million left to be mined until around 2040.

Gold

200,000 Tons

Estimated resource of Gold on earth. Based on some estimations around 80% has been mined.

Mining per day

900 BTC vs. 8T

As we mine, it is getting more difficult and more expensive to mine new BTC/Gold.

Ethereum

Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether (ETH) is the native cryptocurrency of the platform. It is the second-largest cryptocurrency by market capitalization, after Bitcoin. Ethereum is the most actively used blockchain.

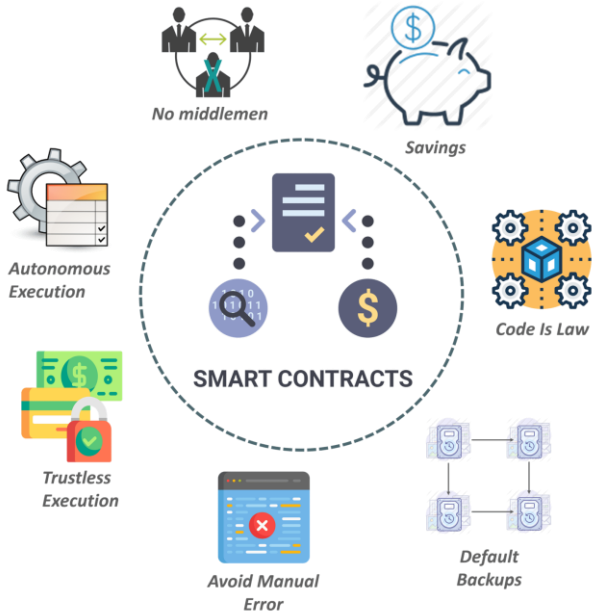
Ethereum was proposed in **2013** by programmer **Vitalik Buterin**. The Ethereum Virtual Machine (EVM) can execute scripts and run decentralized applications. Ethereum is used for decentralized finance, the creation and exchange of NFTs, and has been utilized for many initial coin offerings.

Source: https://en.wikipedia.org/wiki/Ethereum

Smart Contract (Dapp)

A smart contract is a self-executing contract with the terms of the agreement. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. Smart contracts render transactions traceable, transparent, and irreversible.

Nick Szabo, an American computer scientist who invented a virtual currency called "Bit Gold" in 1998, defined smart contracts as computerized transaction protocols that execute terms of a contract.



Source: https://www.investopedia.com/terms/s/smart-contracts.asp

Smart Contract: Gas

Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network.

Gas is paid in Ethereum's native currency, ether (ETH). Gas prices are denoted in **Gwei**, which itself is a denomination of ETH – each **Gwei** is equal to 0.000000001 ETH (10^{-9} ETH).

The speed of transaction will be defined by the amount in ETH whom the user is willing to pay for each gas. More info on [ethgasstation.info]

Source: https://www.coindesk.com/ethereum-gas-limit-eth-price-soars

Smart Contract Limitations

- No floating number (10/3 = 3.3333....)
- No random number
- No access to the outside world
  - Weather condition
- No date / time
  - Only block number (estimation)
- Limited number of variables
- Block size limit
- and very expensive

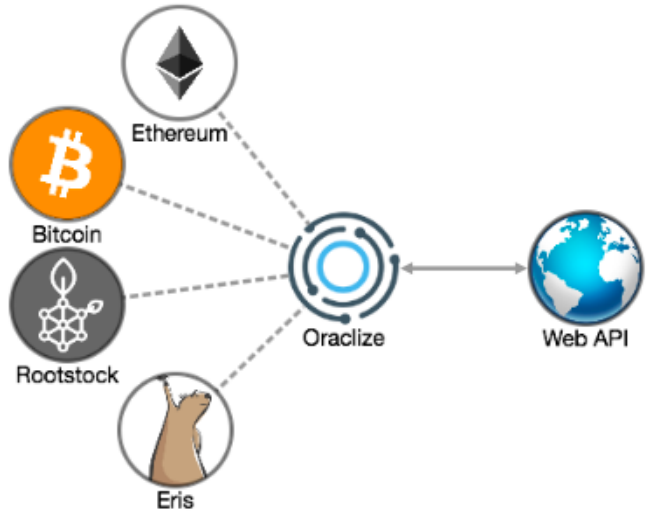
Sample Smart Contract: Random generator

```
pragma solidity >=0.4.22 <0.7.0;
contract Math {

          // Generate a random number between 0 and 100
          function random() public view returns (uint8) {
          return uint8(uint256(keccak256(abi.encodePacked(block.timestamp,
block.difficulty))) % 100);
     }
}
```

Source: https://github.com/kavehbc/Cloudchain/blob/master/Ethereum/BLOR/math.sol
Ethereum Smart Contract - Solidity IDE: https://remix.ethereum.org/

Smart Contract: Oracles



Oracles are data feeds that connect Ethereum to off-chain, real-world information, so you can query data in your smart contracts. For example, prediction market dapps use oracles to settle payments based on events. A prediction market may ask you to bet your ETH on the next president of the United States. They'll use an oracle to confirm the outcome and pay out to the winners.

Source: https://ethereum.org/en/developers/docs/oracles

NFT (Non-Fungible Token)

=

NFT (Non-Fungible Token)

A non-fungible token (NFT) is a unit of data stored on a digital ledger (blockchain), that certifies a digital asset to be unique and therefore not interchangeable.

NFTs can be used to represent items such as photos, videos, audio, and other types of digital files.

https://www.larvalabs.com/cryptopunks/details/3100
Sold on 11 March 2021 for 4.2K ETH ~ 7.58M USD ~ 9.40M CAD

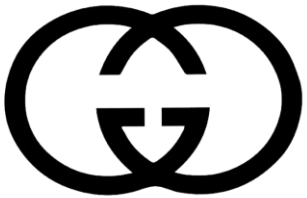
Source: https://en.wikipedia.org/wiki/Non-fungible_token

NFT: Luxury Market

"Right now, fashion being sold via NFT is fashion as art, and not necessarily fashion as a utility," says Cathy Hackl, CEO of the Futures Intelligence Group

"We're eventually going to get to the point where there's more utility, but we're not there yet."

GUCCI



Source: https://www.voguebusiness.com/technology/luxury-fashion-brands-poised-to-join-the-nft-party
Nike Sneakers US Patent:
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=1&f=G&l=50&d=PTXT&p=1&S1=non-fungable&OS=non-fungable&RS=non-fungable

Bitcoin

Mining: Proof-of-Work
Mining Algorithm: SHA-256
Network: Public
Cryptocurrency: Bitcoin
Altcoins: None
Coin limit: 21 Millions
Smallest Unit: 1 Satoshi (0.00000001 BTC)
DApp: None
NFT: Not natively supported except (coloured Satoshis)

Ethereum

Mining: Proof-of-Work (Ethereum 2.0: Proof-of-Stake)
Mining Algorithm: EtHash
Network: Public and Private
Cryptocurrency: Ether (ETH)
Altcoins: Tether, USDC, PAX, etc.
Coin limit: No limit - 18 millions per year
Smallest Unit: Wei (1 ETH = 1e18 wei)
DApp: Smart Contract
NFT: Supported

Investment: Bitcoin vs. Ethereum

Below, there is an snapshot of each cryptocurrency price. Also, the 1-year change of each currency is mentioned.

Bitcoin (BTC)

76,350 CAD

+250%

Ether (ETH)

5,400 CAD

+797%

Snapshot on 16 November 2021 at 10:30 AM EDT in Canadian Dollar.

Can cryptocurrency be used like a fiat currency?

- **Storage:** All nodes keep a copy of ledger, and its growing size is an issue
- **Scalability:** There is relatively a huge transaction delay compared to the other payment networks such as Visa or MasterCard networks
  - Bitcoin processes 7 transactions per second
  - Visa can handle 65,000 transactions per seconds
- **Volatility:** There is a huge volatility in the value of cryptocurrencies
- **Cost:** Very expensive on-chain transactions

Some interesting facts:

- If one satoshi is 1 cent (0.01$), **one BTC would be 1M$**.

- A few **large holders commonly referred to as whales** continue to own most Bitcoin. About **2% of the anonymous ownership accounts control 95% of the digital asset**, according to researcher Flipside Crypto.

- According to the BlockWorks Group analyst, Jake Levison, you only need **0.28 BTC to be in the top 1% richest of the world**.

Source: https://www.bloomberg.com/news/articles/2020-11-18/bitcoin-whales-ownership-concentration-is-rising-during-rally

Interesting Video to Watch

https://www.youtube.com/watch?v=UBZ6Bd0LDjs


Q&A