

# Blockchain to NFTs

Understanding the technology that enables trustless marketplaces

5 May 2022

Presented by Tyler Pinckard at BIME PRO - Bogota Colombia

# Overview

- Speaker Bio
- Marketplaces and the birth of currency
- Banking system
- Cryptocurrency
- Blockchain
- Bitcoin / ETH
- L1 / L2s
- NFTs!



# Tyler Pinckard Bio



<http://tylerpinckard.com/>

<https://www.linkedin.com/in/tylerpinckard/>

# Marketplaces

- In the beginning, there was direct barter exchange for goods
  - You guard the village and I'll grow enough food for both our families
    - Goods for Services
  - I'm good at growing Onions, you're good at growing potatoes-
    - Lets trade so that we can some of each!
- High transactional cost, low fungibility



# Fungibility

What does fungibility mean?

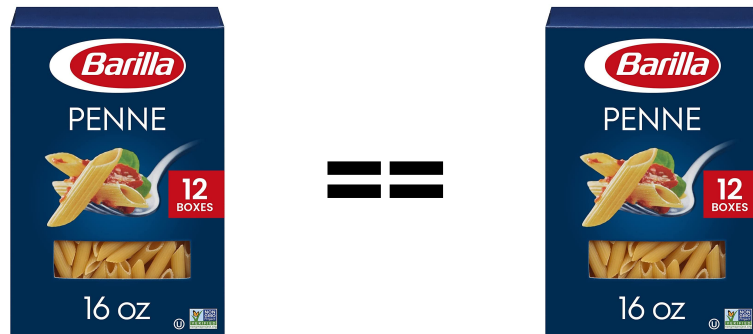
- 1 unit == 1 unit

Examples that are fungible:

- Dollars (if we ignore the serial numbers)
- A box of pasta
- Common shares of a company

Examples of non-fungible:

- Real estate (location, location, location)
- Rare trading cards
- IRL works of art (e.g. mona lisa, insert your favorite)

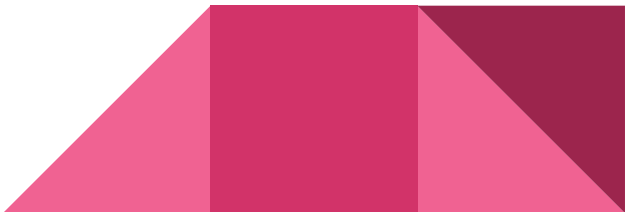


# Currency

- Carrying around a bunch of physical goods to exchange for other products is not efficient
- Currency introduced as medium of exchange
  - The invention of money predates written history
  - First recorded use by the Mesopotamians ~5000 years ago
- Great! Now I can carry fungible coins to exchange for goods that I want
- Currency greatly increases the SPEED at which business can be conducted



# Fractional Reserves

- Exchange currency for precious metals
    - US Gold standard
  - Banks create money through the use of fractional reserves
    - Not enough physical gold to allow creation of new currency
  - Fiat currency introduced
    - government-issued currency that is not backed by a commodity (such as gold)
  - How is that currency created?
  - How is currency introduced into the economy?
- 

# Enter cryptocurrency

- BITCOIN!
  - Described by Satoshi Nakamoto white paper in 2008 - Network launched in 2009
  - Currency introduced on hard-coded, fixed schedule, as a reward to network participants that “do the work” of mining for new blocks
  - Bitcoin is a Permissionless P2P system
    - Anyone can join, participate in the network, wallets start with zero balance





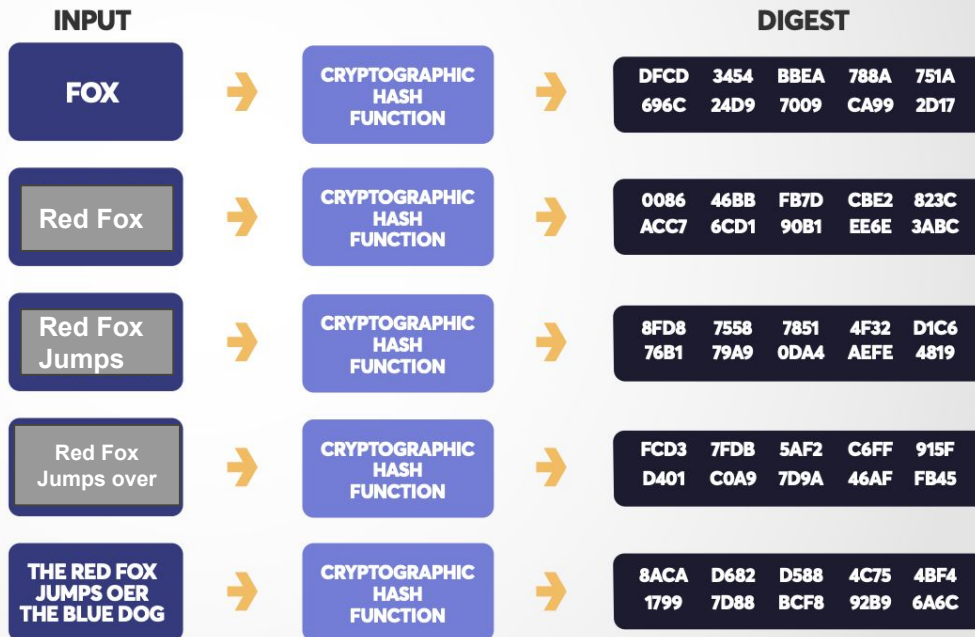
BUT HOW DOES THAT WORK?!



# QUICK INTO TO CRYPTOGRAPHY

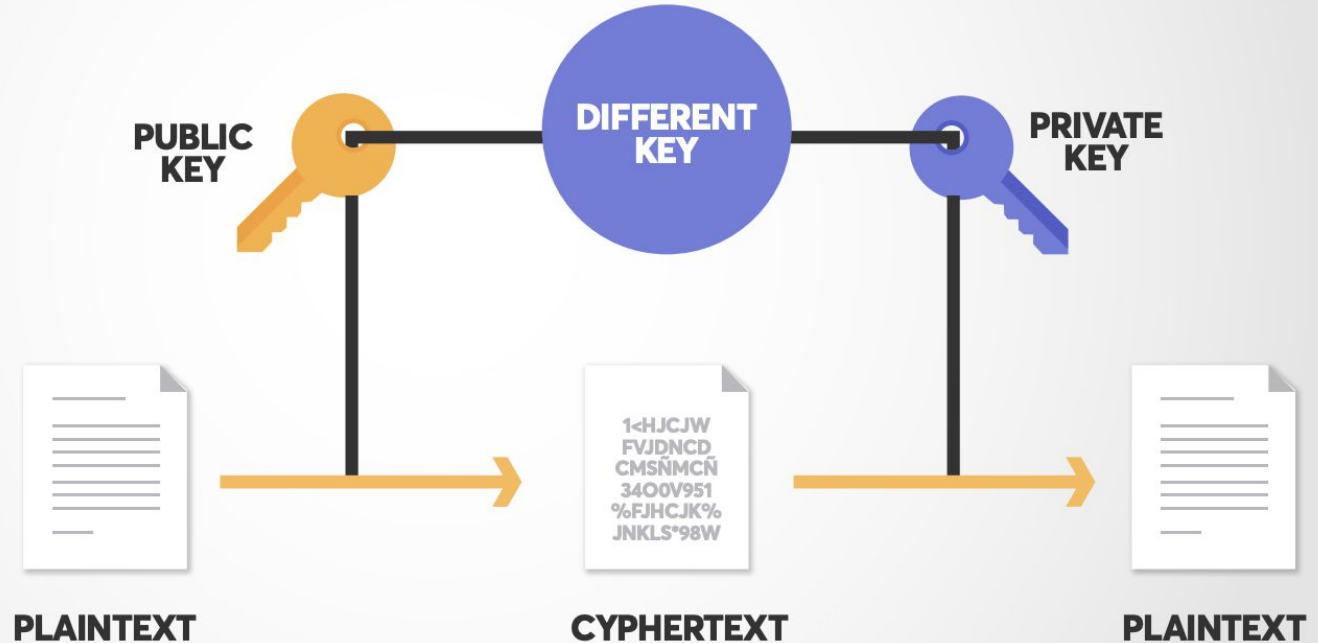
Hash:

- One-way function maps arbitrary input to fixed length output.
- Very hard to reverse (ie- given the output, figure out the input).



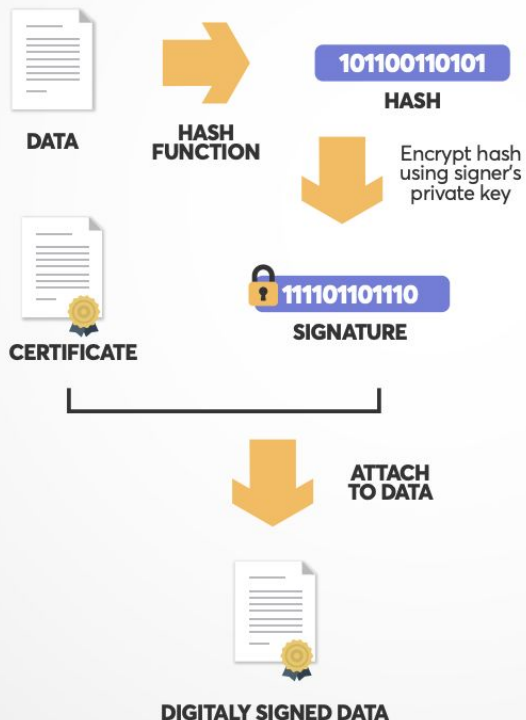
# QUICK INTO TO CRYPTOGRAPHY

**ASYMMETRIC  
CRYPTOGRAPHY:**  
Different keys used to  
encrypt and decrypt



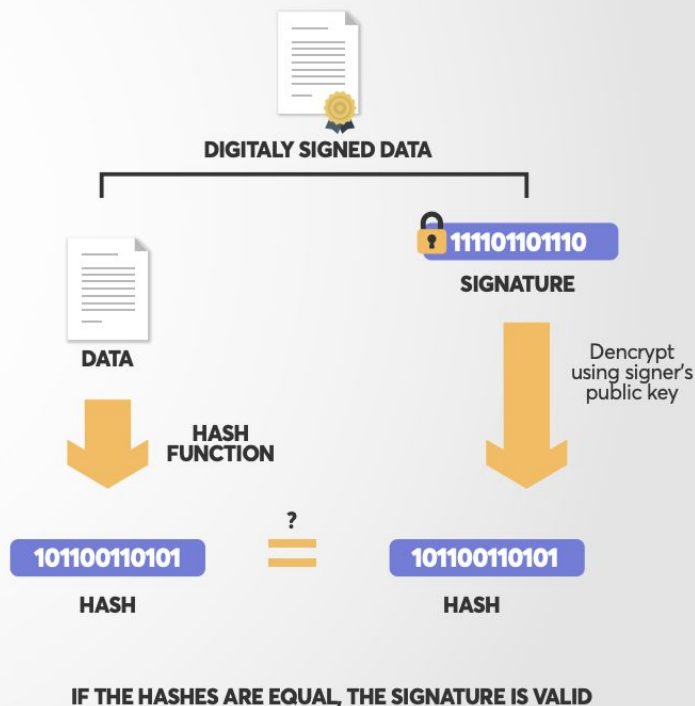
# QUICK INTO TO CRYPTOGRAPHY

## SIGNING

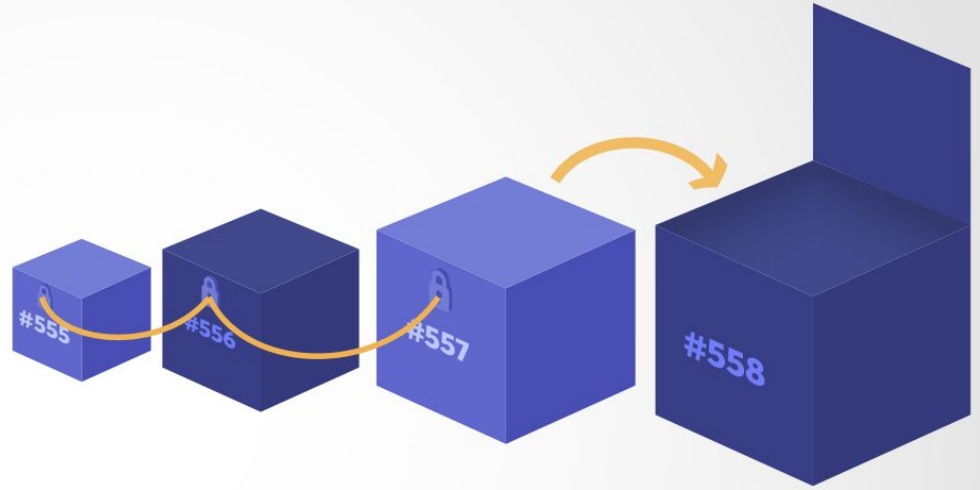


CRYPTOGRAPHIC  
SIGNATURE:

## VERIFICATION



# WHAT IS A BLOCKCHAIN?



A blockchain is a way of storing information, such as transactions, as events on a timeline. So no matter how data is accessed, every action is recorded in a mathematical proof.

Distributed Ledger Technology, (aka - blockchains) record transactions immutably, and in order.

Enables users to trust the math instead of each other.


# Blockchain Characteristics

All information on blockchain accessible by everyone else at all times

Authentication required in order to participate

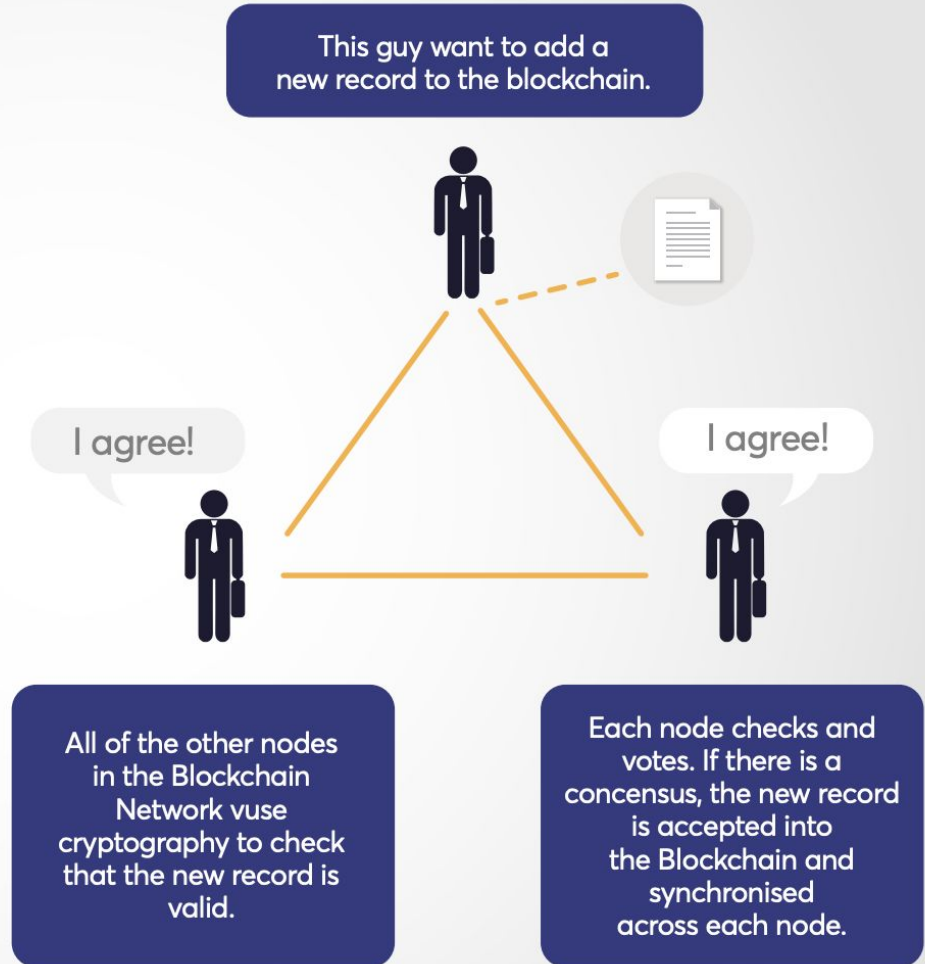
- Verify “who” you are (control private keys)

Blockchain elements:

- Replicated ledger
  - Cryptography
  - Consensus
  - Business Logic
- 

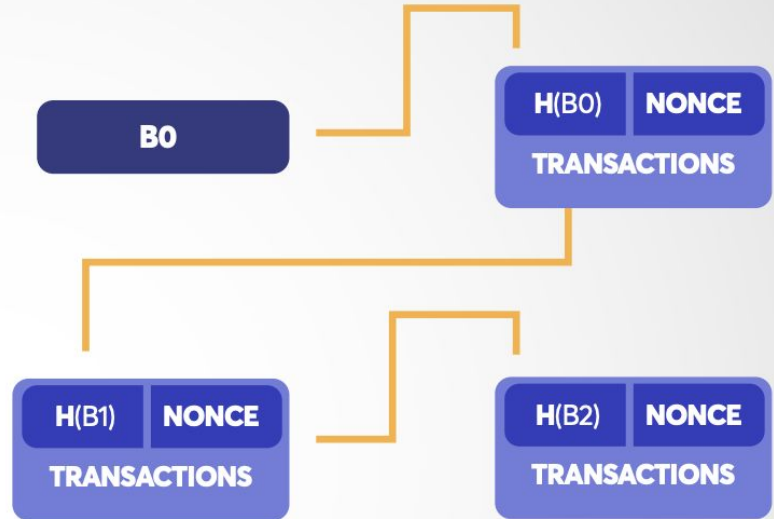
# CONSENSUS

- Consensus about what constitutes an accurate record can be achieved in several ways
- Not a new problem in distributed systems



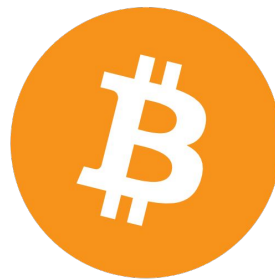
# PROOF OF WORK

- Users submit transactions to node(s)
- Node prepares blocks
  - List of valid transactions (tx)
  - All tx valid
- Race to find low hash value (the work)
  - Nodes try different nonce values until they find one that produces a hash that is of a sufficiently low value, starting with a series of zeros "00000000".
  - Block difficulty is adjusted by adjusting how low they need to guess in order to "win" the block
  - Impossible to guess; effectively randomizes block round leader.





# Bitcoin continued



- Nakamoto consensus mechanism
  - Guess the magic number - you win! (the block reward)
- Each block represents changes to the global bitcoin state, going back to the original genesis block
- Fun fact, bitcoins are not fungible
  - Every bitcoin can be traced back through EVERY transaction that the bitcoin has been part of since it was first created

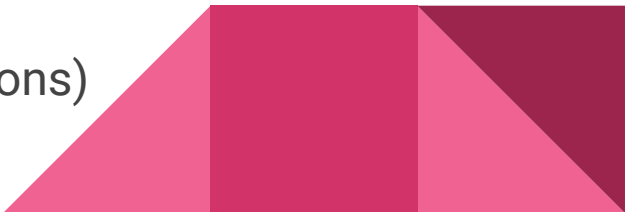
# Enter Ethereum

Introduced in 2015 - to add enhancements to the distributed consensus mechanism introduced by bitcoin:

Native Smart Contracts

Blocks include not only changes to state, but also a full copy of system state

Allows for on-chain functions

- Enter the smart contract
  - Cost \$\$ to run (to prevent DOS, tragedy of the commons)
- 

# From BTC to ETH

Conceptual analogy:

If bitcoin represents a distributed spreadsheet, think of etherium as an enhancement that adds functions to a spreadsheet- actions that occur automatically based on programmatic inputs.



# Ethereum tokens

Ethereum uses ERC (Ethereum request for comment) to bring improvements to the protocol

- Modeled after the same system used to introduce standards and improvements to the internet (RFCs)
- ERC-20 - fungible tokens
  - Discrete fungible tokens that ride on top of ethereum
  - Transfer and spends require ETH to power gas
  - Top tokens: <https://etherscan.io/tokens>



# Ethereum tokens

Back to NFTs: (ERC-721 - non-fungible tokens)

- <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>

ERC-1155 Multitoken standard - similar to ERC-721 with additional functionality to support

- supports multiple creators per contract, where only the creator is able to mint more copies
- pre-mint items for the “lootbox” rewards for smart contract participants



# What happens when the network get busy?

- Costs go up



# Contention on Ethereum

Making smart contracts on Ethereum can be expensive!

> Gas costs spiked over 5000 on 30 April due to NFT launch for smart apes



Estimated Cost of Transactions

Name	Label	Interaction	Gas Used	Rapid	Fast
ETH	Native	Transfer	21,000	\$430.55	\$389.50
USDT	ERC20	Transfer	46,109	\$945.35	\$855.20
USDC	ERC20	Transfer	48,481	\$993.98	\$899.20
DAI	ERC20	Transfer	34,718	\$711.81	\$643.93

<https://ethgasstation.info/>

# Alternate L1

- L1 - entirely separate blockchain
  - Dogecoin
  - Solana
  - Cardano
  - Monero
- And More, lots lots more!
  - (over 15,000 cryptocurrencies on cointracker/coingecko)

-



































# Layer 2 scaling solutions

- L2 - A bridge created between Layer 1 and Layer 2, and at periodic intervals, a summary of Layer 2 transactions is added to Layer 1 for a permanent record.
  - Sidechain - Polygon network
  - State Channels - Lightning Network for bitcoin
  - Rollups :
    - Optimistic rollups: assumes transactions are valid by default and only runs computation, via a fraud proof, in the event of a challenge.
    - Zero-knowledge rollups: runs computation off-chain and submits a validity proof to the chain.



#	Coin		Price	1h	24h	7d	24h Volume	Mkt Cap	Last 7 Days	
☆ 1		Bitcoin	BTC	\$37,738.23	-0.2%	-1.9%	-6.8%	\$23,781,650,750	\$718,961,235,781	
☆ 2		Ethereum	ETH	\$2,781.44	-0.4%	-1.8%	-7.5%	\$13,353,838,724	\$336,042,766,834	
☆ 3		Tether	USDT	\$1.00	-0.1%	-0.3%	0.0%	\$42,785,140,056	\$83,298,697,914	
☆ 4		BNB	BNB	\$382.64	-0.3%	-1.2%	-5.4%	\$1,242,668,680	\$64,425,002,373	
☆ 5		USD Coin	USDC	\$0.998337	-0.1%	-0.3%	-0.1%	\$4,453,075,672	\$48,929,486,567	
☆ 6		XRP	XRP	\$0.601744	-0.9%	-0.9%	-13.5%	\$2,567,944,996	\$29,065,206,838	
☆ 7		Solana	SOL	\$85.17	-0.6%	-2.0%	-15.9%	\$912,936,502	\$28,545,714,404	
☆ 8		Terra	LUNA	\$82.46	-0.6%	0.4%	-15.0%	\$1,428,035,071	\$28,429,308,944	
☆ 9		Cardano	ADA	\$0.768159	-0.7%	-1.1%	-14.6%	\$564,895,559	\$24,753,673,440	
☆ 10		TerraUSD	UST	\$1.00	0.2%	-0.1%	-0.0%	\$624,440,129	\$18,669,341,375	
☆ 11		Binance USD	BUSD	\$0.999048	-0.0%	-0.4%	-0.2%	\$3,630,009,030	\$17,889,684,401	
☆ 12		Dogecoin	DOGE	\$0.128389	-0.3%	-1.8%	-18.5%	\$494,822,739	\$17,068,737,840	
☆ 13		Polkadot	DOT	\$14.66	-0.1%	-1.1%	-19.1%	\$379,584,603	\$16,312,539,128	
☆ 14		Avalanche	AVAX	\$58.69	-1.1%	-2.7%	-19.4%	\$553,900,065	\$15,851,453,456	
☆ 15		Shiba Inu	SHIB	\$0.000020272018	-0.5%	-1.5%	-16.9%	\$414,862,595	\$11,175,310,137	

# NFT

*NFTs are tokens that we can use to represent ownership of unique items. They let us tokenise things like art, collectibles, even real estate. They can only have one official owner at a time and they're secured by the Ethereum blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence.*

- [ethereum.org](https://ethereum.org)



# Thesis

## ERC-20 :

- Loosen the grip of the venture capitalists
- Allows decentralized funding for companies

## ERC-751 :

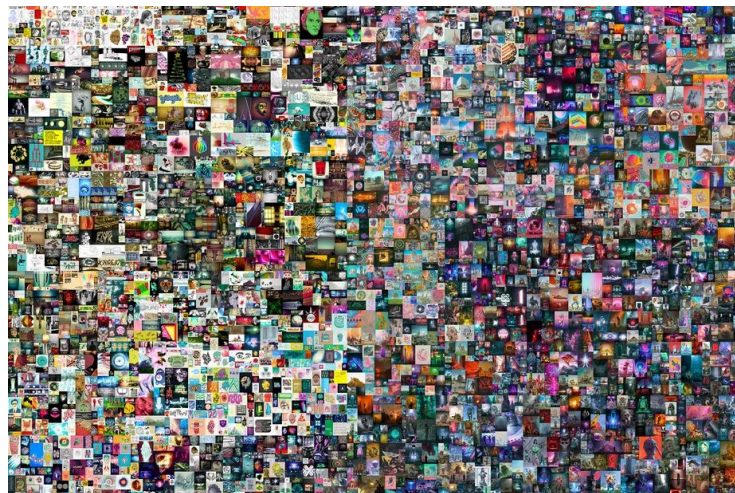
- Loosen the grip of media makers
- Allows decentralized funding for artists



# NFTs

## The Art

- Generative Sets
- 1 of 1s



# NFTs

## The technology

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/utils/Counters.sol";

contract EmotionalShapes is ERC721 {
    using Counters for Counters.Counter;
    Counters.Counter private _tokenIdCounter;

    constructor() ERC721("EmotionalShapes", "ESS") {}
    function _baseURI() internal pure override returns (string memory) {
        return "https://YOUR_API/api/erc721/";
    }

    function mint(address to) public returns (uint256) {
        require(_tokenIdCounter.current() < 3);
        _tokenIdCounter.increment();
        _safeMint(to, _tokenIdCounter.current());

        return _tokenIdCounter.current();
    }
}
```

<https://www.freecodecamp.org/news/how-to-make-an-nft/#initialize-the-project>

# NFTs

## The technology

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/utils/Counters.sol";

contract bime_pros is ERC721 {
    using Counters for Counters.Counter;
    Counters.Counter private _tokenIdCounter;

    constructor() ERC721("bime_pros", "ESS") {}
    function _baseURI() internal pure override returns (string memory) {
        return "https://YOUR_API/api/erc721/";
    }

    function mint(address to) public returns (uint256) {
        require(_tokenIdCounter.current() < 3);
        _tokenIdCounter.increment();
        _safeMint(to, _tokenIdCounter.current());

        return _tokenIdCounter.current();
    }
}
```

# What is minting an NFT?

By minting an NFT, you publish a unique token on a blockchain.

This token is an instance of your Smart Contract.

- Each token has a unique tokenURI
  - contains metadata of your asset in a JSON
  - conforms to NFT schema that holds the metadata is where you store information about your NFT,
    - Name
    - Image
    - Description
    - other attributes.





# Example NFT

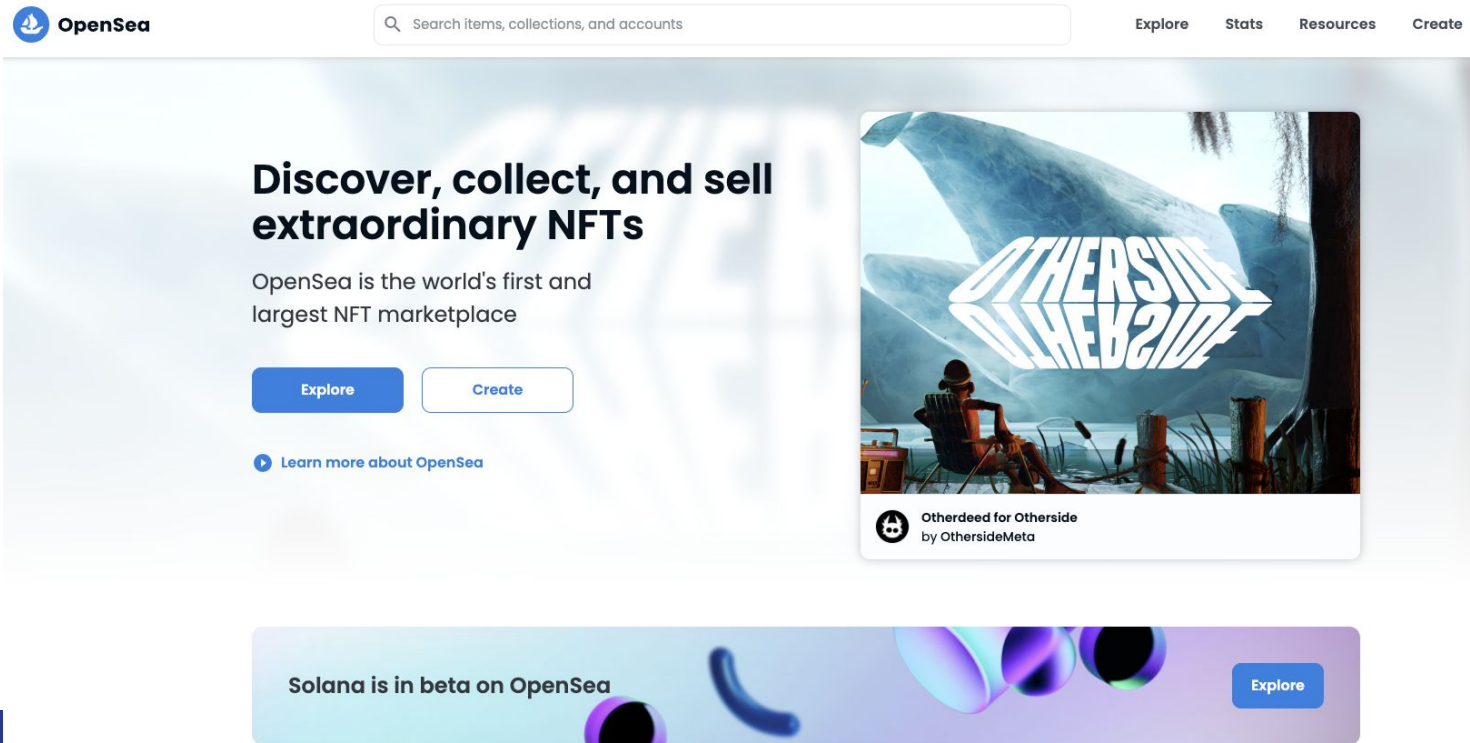
```
{
  "attributes": [
    {
      "trait_type": "Shape",
      "value": "Circle"
    },
    {
      "trait_type": "Mood",
      "value": "Sad"
    }
  ],
  "description": "A sad circle.",
  "image": "https://i.imgur.com/Qkw9N0A.jpeg",
  "name": "Sad Circle"
}
```

- NodeJS
- <https://www.freecodecamp.org/news/how-to-make-an-nft/#initialize-the-project>
- Alchemy
- <https://docs.alchemy.com/alchemy/tutorials/how-to-create-an-nft/how-to-mint-a-nft>



# You Do Not Need to be a Coder to launch NFTs

> Note, you DO NOT have to write smart contracts to launch NFTs. You can launch today on OpenSea, Rarible, looks Rare- however you will need a wallet created with funds to be able to mint (generate) your NFT



# Create New Item

\* Required fields

## Image, Video, Audio, or 3D Model \*

File types supported: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF. Max size: 100 MB



## Name \*

## External link

OpenSea will include a link to this URL on this item's detail page, so that users can click to learn more about it. You are welcome to link to your own webpage with more details.

## Description

The description will be included on the item's detail page underneath its image. [Markdown](#) syntax is supported.

## Collection

This is the collection where your item will appear. ⓘ

Select collection



### Properties

Textual traits that show up as rectangles



### Levels

Numerical traits that show as a progress bar



### Stats

Numerical traits that just show as numbers



### Unlockable Content

Include unlockable content that can only be revealed by the owner of the item.



### Explicit & Sensitive Content

Set this item as explicit and sensitive content ⓘ



## Supply

The number of items that can be minted. No gas cost to you! ⓘ

1

## Blockchain



Ethereum



# Improve your security posture

Practical things you can do to improve your security posture wrt

- Keep a few different wallets with different funds
- Invest in a hardware wallet, purchased directly from the vendor (beware supply chain attacks)
- Multisig any wallet you wouldn't want to lose
- Backup seed phrases/keys to metal



Q & A



# Resources

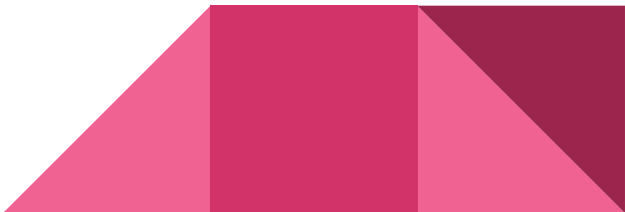
[https://www.wikiwand.com/en/History\\_of\\_money](https://www.wikiwand.com/en/History_of_money)

<https://etherscan.io/tokens>

<https://www.pcmag.com/encyclopedia/term/layer-2-blockchain>

<https://www.freecodecamp.org/news/how-to-make-an-nft/>

- No Code create an NFT:
  - [creativebloq.com/how-to/make-and-sell-an-nft](https://creativebloq.com/how-to/make-and-sell-an-nft)
- OpenSea ERC-1155 Starter contract
  - <https://github.com/ProjectOpenSea/opensea-erc1155>





# Backup Slides

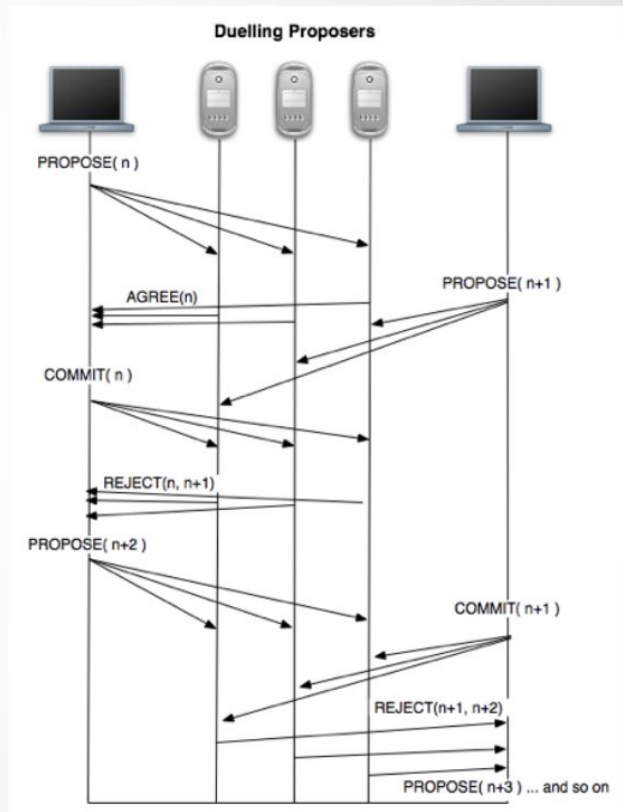


# CONSENSUS ALGORITHMS

- Defined by how each node reacts to one or more of the following items:
  - Response time (latency)
  - How many of them responded (aliveness)
  - What their opinion of 'truth' is (voting)
- Bitcoin - play by the rules and you may get to be king for a day!
- Permissioned systems typically report 10-1000x performance over permissionless, as they authenticate participants and can assume more trust during operation.

# CONSENSUS ALGORITHMS

- Byzantine Fault Tolerance well studied in computer science.
  - Paxos (and derivatives).
  - Raft, Cubby, etc.
- Very Different for Permissioned vs. Permissionless!
  - Permissioned systems.
    - Non adversarial participants.
    - Only known and vetted nodes are allowed to join.
    - Often proof of stake.
  - Permissionless
    - Anyone can spin up a node instance and contribute to the network.
    - ie- bitcoin w/ proof of work.



# BLOCKCHAIN CHARACTERISTICS

## REPLICATED LEDGER

- History of all transactions.
- Append-only with immutable past.
- Distributed and replicated

## CRYPTOGRAPHY

- Integrity of ledger
- Autenticity of transactions
- Privacy of transactions
- Identity of participantes

## CONSENSUS

- Decentralized protocol  
Shared control tolerating  
disruption
- Transactions validated

## BUSINESS LOGIC

- Logic embeddeb in the ledger
- Excecuted together with  
transactions
- From simple "coins" to  
self-enforcing "smart contracts"

# BLOCKCHAIN SYSTEM DESIGN CONCERNS

- Distributed system- multiple, disparate actors
  - Information takes time to propagate
  - Speed of Light - Network Latency
- Not everyone has the same set of "facts" at the same time  
Time is a relative, each participant has their own perspective.
- How to keep the network synchronized?
- How to prevent double spend?