# ← : WEB3 : →

Anything online will be stored as a token on a blockchain.

## CH1: WEB 3, WEB 3.0 & THE METAVERSE

→ 1991 - 2004 : Web 1.0 – Static : Read

→ 2004 - present : Web 2.0 – Read + Interact

→ Next : Web 3.0 → Multiple possible pathways

- Semantic web :– All data is Machine Readable parsed by ML Algos through API
- Spatial Web – Web interaction through env. (IOT)
- Metaverse – interaction through VR - alternate reality

underlying idea – data is owned & shared by users or Decentralized contrast to current framework where data is centralized & owned by companies

Web3 - Introduced by Ethereum cofounder in 2014 by Gavin Wood

Decentralized & tokenized system on blockchain tech.

- different from Web 3.0 - ask people before continuing
- became a umbrella term for all blockchain tech. (DeFi, cryptos, DAOs, NFTs, ..)
- shares a possible vision for the future of the web. Not there yet.

## → Metaverse

- cryptos provide solution to setup metaverse economy withour setting up a new virtual economy
- funding metaverse through Blockchain - by setting up DAOs and selling NFTs

META ∞ ← TUG OF WAR → WEB 3 ENTHUSIATS

## → Promise of Web3

- Root - transfering power from centralized authorities to the users
- place data on decentralized storage - creating global economy
- problem with centralization - moderation & regulation.
  → borrowed trust

Decentralized Ideology - Lassez-faire capitalism
+
Meritocracy

→ Two key characteristics

① Everything becomes a transaction stored on an immutable blockchain

② Everything on the blockchain has tradeable value

→ Creating a token consumes energy

→ Energy is paid in cryptocurrency

→ Earning crypto is done by verifying transactions & adding new blocks to the chain

## Web3 Goal

Re-engineer the entire web ecosystem to be built on blockchain tech - and make distributed blockchain as a single source of truth – social media, finance, property deeds, medical records etc.

Access to the blockchain and control over what goes next in the block is where the power will lie

## Decentralization

→ web app hosted on a central server - single source of truth but also single point of failure
- centralized services own and control what goes on the platform

→ decentralization - distributes data b/w the users.

- → **Federated** - multiple data sources are mapped to act as cohesive units. You chose your server. which interacts with other servers

  Web 3.0

  - Brittle – data lost on that server is lost everywhere.

- → **Absolute** –

Web3

Full copies of data are distributed to all participants

- fast but uses lot of computing power.
- no issues of data loss

→ Removes middleman.

## Web3 Acronyms

→ DeFi (Decentralized Finance) - financial transactions w/o bank on the blockchain - use smart contracts to offer P2P financial instruments

- goal: get rid of intermediaries (banks)

→ GameFi (Blockchain based games) - game awards that you can trade, invest & grow & borrow against.

- Rewards utilized within and outside the game
- Some people are playing games as full-time job

→ DeSci (Decentralised Science)

- science on blockchain (idea for now)
-

De___ - decentralized something
___Fi - blockchain based [industry|activity]

## dApp

→ current apps centralized -

APP PROVIDER ← data → USER

→ dApp is a decentralized app which provides user-friendly interface for the blockchain & decentralized storage

- comprised of smart contracts on the blockchain
- deterministic - same functions in every environment
- turing complete - perform any action it is set-up to perform given enough resources
- isolated - malfunction does not affect any other entity

→ <u>Benefits of dApp</u>

- persistency
- data security & integrity
- privacy & resistance of censorship

→ <u>Drawbacks</u>

- smart contracts difficult & expensive to update
- blockchain based drawbacks - scaling, network congestion, network access cost etc. come into play
- easy to use interfaces are difficult to build

→ solution to these issues all involve part / complete centralization

## Decentralized Storage

→ Web3 can't store most of the information on web - slow & prohibitively expensive

→ decentralized storage connected to blockchain - like P2P file sharing (BitTorrent)

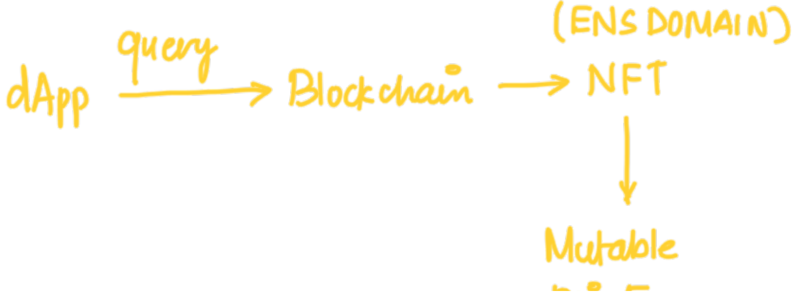
→ IPFS (Inter planetary file system)

- evolved from BitTorrent
- files stored as multiple objects of 256k with a hash + index of how to retrieve those files
- they are stored in the decentralized fashion.
- Problem: file updates → hash updates
- Requires a mutable pointer to always point to the latest file while also keeping previous files for historical permanence.

Adding domain names to the blockchain like - Ethereum Name system (ENS).

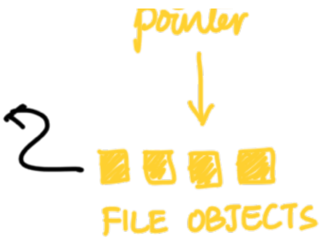
Blockchain domains are NFTs that point to pointers or addresses

Fetching files is completely rewritten

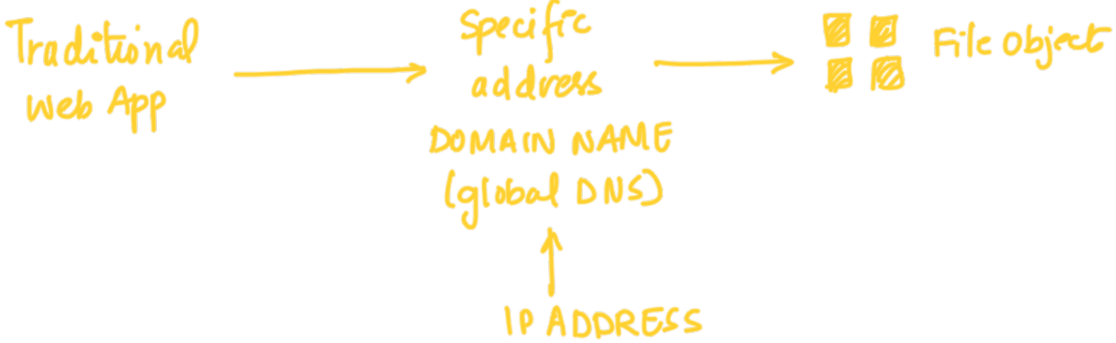


← updating on the blockchain if pointer needs updating

Files Reassembled by browser. Web3 browsers & existing browsers support IPFS.



this is different from current approach.



point at a physical location

## Challenges of Decentralized Storage

→ No incentive to store files from random person – Enter Filecoin a crypto earned by sharing space on decentralized storage – becomes a tradeable commodity to be used as investments

→ Equity – participation requires free storage and stable broadband internet
- digital divide means many can't afford. – decentralization to succeed we need to address global inequity

→ Data permanence -
- decentralization allows this but is bad for things like harmful/sensitive content

- GDPR, EU, CCPA - exclusive right to get data removed. very difficult to achieve

Decentralized storage is ethical, ideological, legal & political issue

## BLOCKCHAIN AND WEB3 BASICS

Blockchain - is an immutable ledger of information.

- is a chain of blocks containing transactions - that have ever taken place
- once the transaction is added to the block & block to the chain, the info becomes permanent
- maintains immutability by storing info about all previous blocks. If tampered, block changes, everyone can see tampering b/c the next block will not have info on the previous block.
  - using SHA-256 encryption

Block - think of it as sealed transparent box - inspect but cannot be changed.

Header - block metadata

Timestamp

Hash - of all trans in the block

Hash always in the

results in same output if input is exactly same

Hash for prev block

Nonce - arb. rand. # used to create the block
- miners guess this to create the block

Transaction counter - # of trans in the block

List of transactions

Additional metadata - depends on the blockchain

## Decentralized Blockchain

Transaction stored in ledgers. If ledger is a blockchain then it can be

### Trusted Blockchain

- trust in central authority (bank)
- transactions added only by people having permissions to the blockchain
- single blockchain

### Trustless Blockchain

- trust using consensus mech.
  - incentive for users to add valid trans. & penalize cheaters
- P2P transactions
- everyone has access

## Consensus Mechanism

Double Spend problem - spending money in multiple places by abusing the latency of the system. Also a fundamental problem with distributed ledgers

Consensus Mech. solves double spend problem

- → Proof of work : (POW):
- → Proof of stake : (POS) :

Incentive to participants to validate transactions. For a consensus 51% of the network say one transaction is valid, the validators on the winning side are rewarded with crypto while losing side lose computing resources. This is called Mining or Forging blocks.

## Crypto Mining & Forging

Whenever a block is added to the blockchain, a new block is open for a fixed period (10 min for BTC) or max block size limit is reached.

When its time to close the block, participants on the block start working on consensus - decisions on which transactions should go in the block - using POW or POS - miners or forgers create a block with specific version of events and pass it to the n/w for validation

If 51% of miners accept it as truth - block is added to the blockchain - this is rewarded with crypto

## Proof of Work

→ original consesus mechanism - validation method

→ used by BTC

→ adding block to blockchain by burning electricity

↳ miners guess number ⟶ compile hash → guess the right number

If guessed then paid in BTC ⟵

else

Burned a lot of electricity doing nothing

(Nonce - Number used once)

Network generates a complex target hash. which miners have to guess by throwing millions of guesses

complex sequence of symbols

right guess - closest guess - wins that contest

POW - is willingness to burn electricity to guess the right nonce to win the lottery.

# miners ↑ ⟹ complexity of target hash

meant to reduce competition.

# computers ↑ ⟹ likely of wining ↑ ⟹ enormous env. impact

So PoW is enormous intentional waste of energy.

So, POW is enormous intentional waste of energy

## Why POW is used ?

→ in part solves the immutability problem

## Proof of Stake

→ POW - expensive (cost of hardware + electricity) + env. impact.

→ In POS, people creating blocks are called validators.
creation of block is called forging. (instead of mining - POW)

→ Validators register with the blockchain
(stake crypto in escrow on the chain)

↓

When a new block is ready to be added, random validators are picked to validate the data block

↓

Non chosen validators attest the work

↓

consensus reached (validated + attested), block is closed.

↓

validators and attesters paid a fee.
validators also paid for compute time 4 n/w transaction as gas fees

↑

Losing the stake and access is what keeps the validators from adding invalid transactions

## Cryptocurrency

A digital currency generated on and traded on the blockchain - value of coin is determined by what people believe - this is no different from fiat currencies

→ not controlled by central bank - printing & manipulation avoided

→ global

→ used for speculation (Buy low, sell high)

→ beleived to be better investment than stock market

## Tokens or Coins

→ crypto exchanges for trading coins b/w blockchains

→ Crypto token – representation of an asset on the blockchain

- asset could be a coin or something else
- btc blockchain - all tokens are coins - b/c it is a crypto blockchain only
- eth blockchain – tokens can be ETH, alternative token currencies, smart contracts (DOWs), NFTs etc...

Coins - function as plain old money

- transactions
- fungible - all coins have same value / interchangable
- can be traded in fractions

Smart Contract - self activating logical programs embedded in the token itself on the blockchain

Tokens - can be traded directly within blockchain
- coin value of token can vary greatly depending on what it represents

All coins are tokens, Not all tokens are coins but all tokens are backed or paid for by coins

NFTs - Non fungible tokens

- cannot be copied, substituted or subdivided (Non-fungible)
- is a token - tradeable asset
- unique entity
- contains hyperlinks to assets, or smart contracts - performing action any time the NFT is activated or traded - b/c cost of storing data is extremely high

| | | | |
|---|---|---|---|
| 5MB image | ⟶ | $500,000 | gas fees |
| link to image | ⟶ | $70 | gas fees |

- does not mean ownership
    - holding the NFT of the art does not mean you own the art

→ Ticket fraud will be impossible - on blockchain

→ Membership and perks & special priviledges

→ Sell art → raise money

→ Investment asset

## Issues

→ privacy - eg: land title could be stolen

→ adding personal info is permanent & immutable

## Crypto Wallet - equivalent of digital bank card

→ Access to blockchain
- username & password
  (public key) (private key) - security enabled - impossible to guess even with brute force
  Address encrypted
- making a transaction requires passing both public and private keys
- assets does not live on crypto wallet
- tool to access & modify info on blockchain

## Several Versions

- Web-based ( ≡ bank a/c) ← centralized / 3rd party
  ← possible theft
- software based - on your device
  (more secure)
- 'cold wallets' - physical devices to store public & 'hard wallets' private keys

- unlike bank a/c, address is used as pseudonym, nobody knows who owns the address
  - not anonymous - but pseudonomous
    can be figured out by pattern of transactions

## Smart Contracts

- token / coin - passive
- smart contract ~~on~~ token - active agent
- self executing function to perform actions on blockchain
  - sharing profits anytime NFT is traded - smart contract
  - Revenue sharing, if X then Y,
  - no room for disputes & arbitration
  - immutable
  - broken & malicious contract can live and be serious
    - override with new smart contracts
    - maintainence is difficult

# DAOs

- Blockchain based org.
- series of tokens 4 NFTs with smart contracts - executes the function of an org. eliminating need for traditional org tools like board of directors, accountants
- look a lot like shareholder companies
  - DAO can issue votes and smart contracts to keep track of votes to decide the direction of org.

→ all roles are public

→ autonomous

→ DAO used for raising money, revenue sharing

→ in future may eliminate the need for lawyers and accountants

- can be complex (written 4 maintained by same expensive lawyers 4 a/ctants)
- financial liability will still require legal and accounting assistance
- human work | unwritten roles cannot be captured.
  - budgets limits

Organization will find it challenging to code human