Bitcoin and Web3

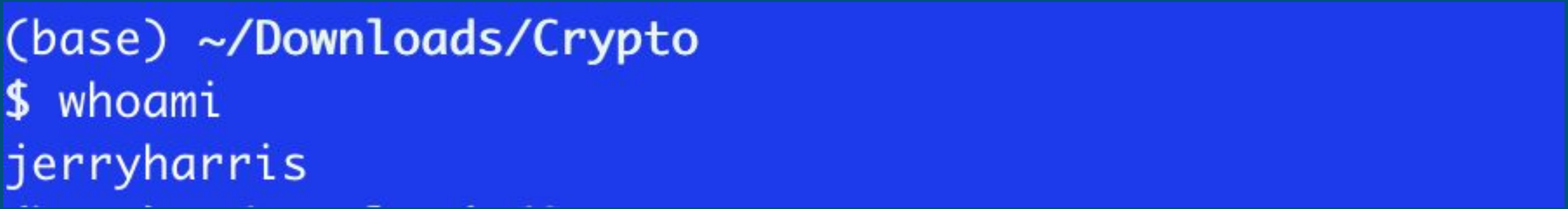
Behind the Curtain:
The Tech, Promise, and Hype

Jerry Harris
June 2022

Crypto Agenda

- whoami and whyami Doing This
- The Crypto Promises - anonymity, decentralization, censorship resistance
- The Tech - Blockchain, Coins & Tokens, Wallets, Bitcoin, Ethereum
- Web3 - Smart Contracts, NFTs, DAOs, DeFi
- The Scams and Thefts
- Summary
- Conclusions

whoami and whyami



```
(base) ~/Downloads/Crypto
$ whoami
jerryharris
```

Apropos Background

tl;dr - deep product development exp with web, HA, Big Data, financial transactions, time-series, and platform v protocol

Where & What	What	Apropos Lessons
AOL - Coder & manager	Browser, AOL Instant Messenger	Server architecture to support 5 million concurrent messaging users Dot-com bubble creation and bust
Nokia - Dir of Prod Dev	Mobile browser and web app ecosystem using HTML, CSS, and Javascript	Building a dev platform on standard protocols
Choicestream - VP Eng	Big Data Ad Tech - NoSql databases like HBase, Kafka, Cassandra	Making trade-offs to achieve high volume of transactions with clustered databases
EnerNOC - Sr Dir Eng	Leading 80 people to re-build an IoT platform with large # of devices	Ingesting high velocity time-series data streams in a messy real world
Airfox - VP Eng	Fintech Banking App for unbanked poor people in Brazil	Reliability and quality requirements of financial transactions are unreal. **A "$0 balance" bug (just a bug) can cause real harm in a person's life.**

whyami focusing on crypto?

- Summer ‘21 - started diving deep since crypto is the Next Big Thing™
- Focused on the community-building aspects of DAOs
- Started forming my own DAO
- My dot-com hype instincts were awakened the more I learned
- Became very curious about database characteristics of Blockchain
- This presentation captures my journey to answer these 2 questions:

What would survive a crypto crash?

Is Blockchain the next evolution of databases?

The Crypto Promises

Why Cryptocurrency?

Anonymous => better than Privacy b/c government can’t snoop
Snowden revelations

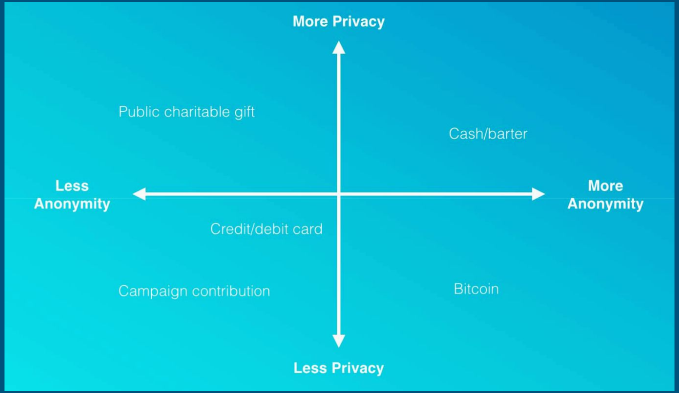
Decentralized => better than Centralized control by Govt, Big Tech, Big Finance
2008 financial crash

Censorship Resistance => outside regulatory and Big Tech’s reach

Create generational wealth! To the Moon!

Anonymity is better than Privacy

Definition: A transaction is “anonymous” if no one knows who you are.
Definition: A transaction is “private” if what you purchased, and for what amount, are unknown



The promise is that while your Blockchain transactions are not private,
no one will be able to map your identity to any set of transactions (more later)

Decentralized is better than Centralized

First, we need to update terminology.

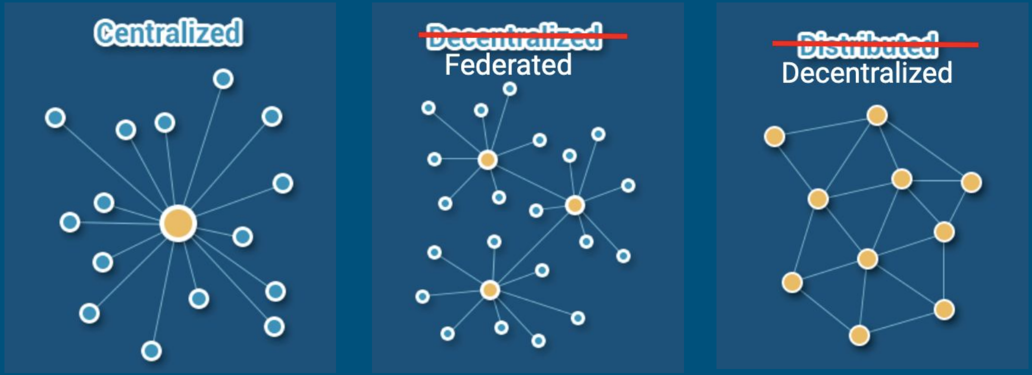
This is the classic diagram comparing network topologies first published in the 1960’s.

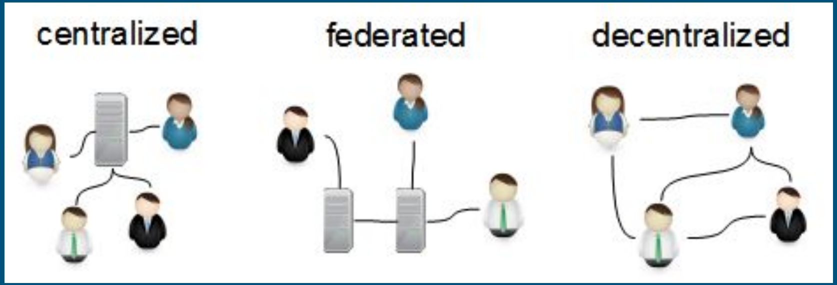
These terms have changed :

Centralized => Centralized

Distributed => Decentralized

Decentralized => Federated

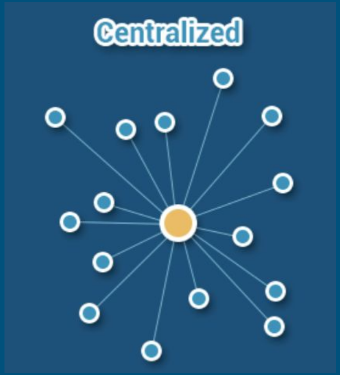


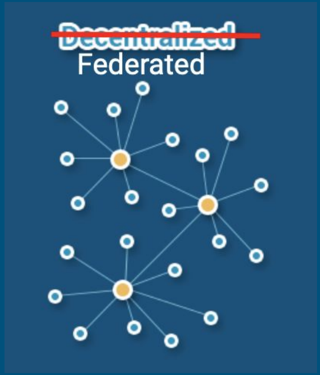


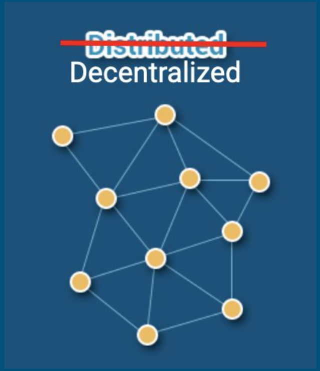
Decentralized is better than Centralized

The promise is decentralized is always better than centralized and federated

- Crypt and web3 are decentralized and good
- Web2 is centralized and bad







This is over-simplified

Any given system is a mix of all these, eg

- Bitcoin Blockchain is decentralized, but dApps are increasingly Federated
- Ethereum Blockchain with Sharding is Federated

Censorship Resistance > Gov't Regulation

The strong cryptographically-enforced immutability of a public blockchain means no one can ever change or delete a transaction or data on the chain.

Financial transactions can be done without any regulatory body involved*

Example used is when authoritarian regimes appropriate land and other material possessions of displaced persons.

The Blockchain would be proof of ownership.

Any conflict or disagreement would need to be judged in court

Any country can pass Laws banning any Blockchain "proof of ownership"

*As long as you don't want to convert the crypto coins or tokens into Fiat currency in a country with strong AML/KYC laws

Create Generational Wealth

Especially after the 2008 financial crash, many see the current financial world as corrupted by power and wealth, with little chance for the poor to build wealth in a fair system

Crypto is outside the normal controls of markets and government

The “little guys” can ban together to stick it to those in charge

The GameStop and AMC meme stocks and crypto are means to this end

The Basic Tech

0:15

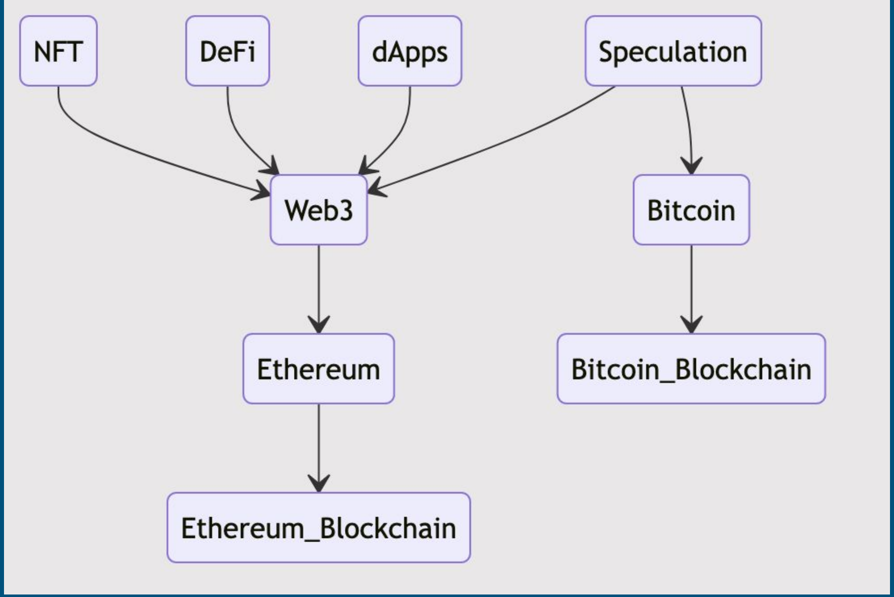
The Stack

Every good software has a tech stack

This orients the rest of our discussion

We will work bottom-up

Buckle up…we’re going on a ride!

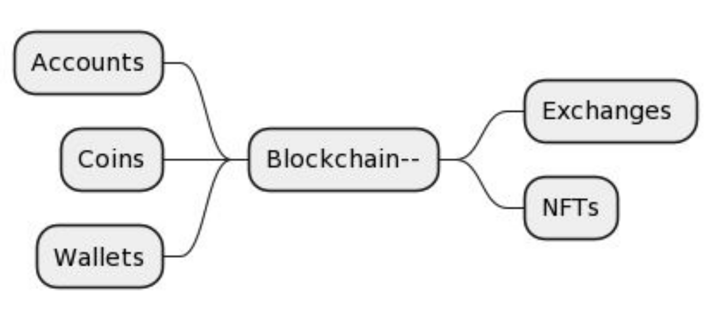


Blockchain

(high level)

Blockchain is a public, secure, append-only ledger of cryptocurrency transactions between users' accounts. The receipt can also be stored on the blockchain along with the transaction. Strong cryptography keeps it unchanged. A "distributed ledger".

Dependants



Use Cases - Mostly for Cryptocurrency

- Users can create new accounts for free
- Transactions are easy to initiate for variable fee
- All transactions are public
- Smart contracts add cool new functionality
- Node operators get paid in native coins (mining)

Other Possible Use Cases:

- Supply chain ownership records
- Car maintenance records
- Ledger for property deeds
- Voting! (what could go wrong? :-)

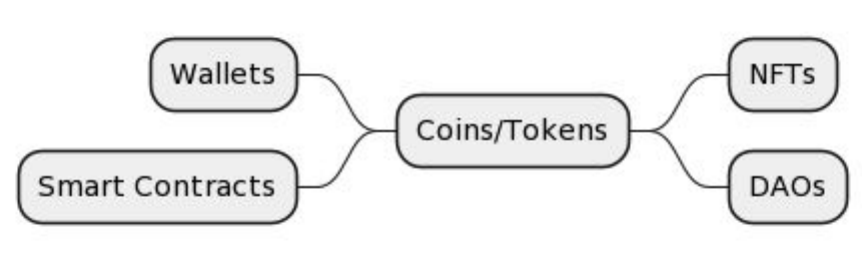
Risks

- Transactions are irreversible
- Coins can be sent to any wallet without permission
- Coins can be sent to inaccessible wallets
  - Study shows ~20% of all bitcoins on the blockchain are inaccessible
- Lost or forgotten passwords cannot be "reset"
- Transaction fees go up with more volume
- A hacked wallet gives access to all its accounts
- Transaction can't executed offline

Coins/Tokens

Coins and tokens are similar digital artefacts stored and transferred on a blockchain. Coins are native to their Blockchain and provide underlying system of monetary value. A token's "value" is defined by external protocols or contracts.

Dependants


Wallets
Smart Contracts
Coins/Tokens
NFTs
DAOs

Use Cases

- Currency like Bitcoin, Eth, Dogecoin, Litecoin, stablecoins
- Central bank digital currency (CBDC)
- Coins are fungible - one acts like any other
- Tokens can be non-fungible - unique and stands alone
- Exchangeable for Fiat Money (eg, USD)
- Scarce commodity conveys perceived value
- Mining and transaction fees use the Blockchain's native coin

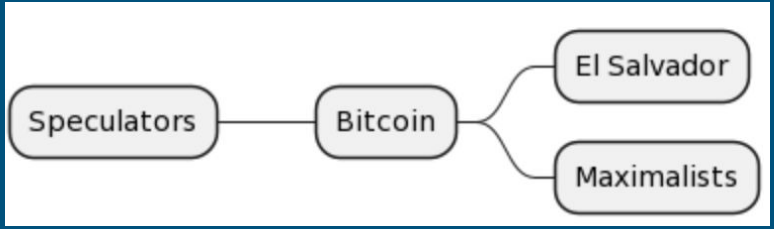
Risks:

- Fiat value leads to speculation & volatility
- Boom/bust cycles are common
- "Pizza guy" - any real-world transaction can lead to massive loss or gain because of a coin's explosive volatility
- Smart Contracts are code and vulnerable to bugs and security vulnerabilities

Bitcoin

The OG of cryptocurrencies. Bitcoin is the native coin for the Bitcoin Blockchain and defines the rules for the distributed ledger functionality of the Blockchain.

Dependants



Use Cases

- For storing “value”
- For speculative investing
- For purchases, although so far it’s limited to purchasing other digital assets like coins, tokens, and NFTs

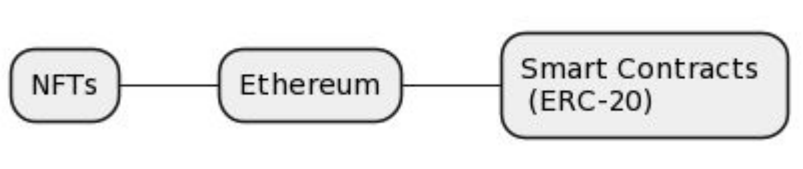
Risks:

- Volatility - which leads to massive appreciation or depreciation of either currency or digital good purchased
- Not resistant to inflation or other economic downward pressures
- Proof of Work consensus algorithm on the Bitcoin Blockchain requires high electricity consumption

Ethereum

A cryptocurrency with the additional functionality of defining smart contracts and for maintaining an immutable state machine on the blockchain. It's a different blockchain than Bitcoin's.

Dependants



NFTs

Ethereum

Smart Contracts (ERC-20)

Use Cases

- ETH-20 protocol on Ethereum define how to create and use Smart Contracts
- Provides the basis for all distributed Apps (dApps) functionality (access, receipts)
- The foundation of many De-Fi projects, NFTs, and DAOs with Smart Contracts
- Each transaction updates an existing state machine

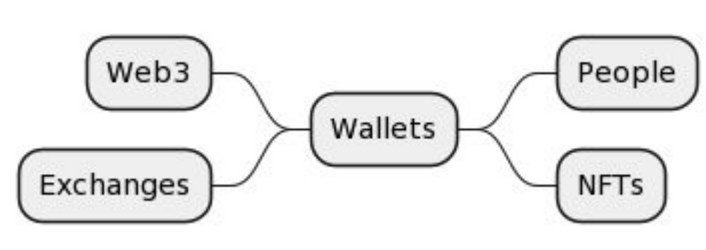
Risks:

- Speculative Volatility
- Not resistant to inflation or other economic downward pressures
- Proof of Work consensus algorithm on the Ethereum Blockchain requires high electricity consumption
- Switch to Proof of Stake is taking longer and the risk is it'll remain with Proof of Work
- The attempts to switch to Proof of Stake or off-chain processing are beyond the scope of this talk

Wallets

An application for creating and managing “accounts” on a blockchain. Accounts are identified by a cryptographic key pair. The Wallet manages the public and private key pairs for accessing the coins on a blockchain.

Dependants



Use Cases - “account” management

- Passwords are actually public/private key pairs
- A new keypair creates a Blockchain address
- Sharing addresses with other apps and users and websites for receiving coins/tokens
  - QR Codes should be used to prevent mistakes from typing in an address
- A wallet can be s/w or h/w
- Wallets calculate a person’s current balance across multiple addresses and blockchains

Risks:

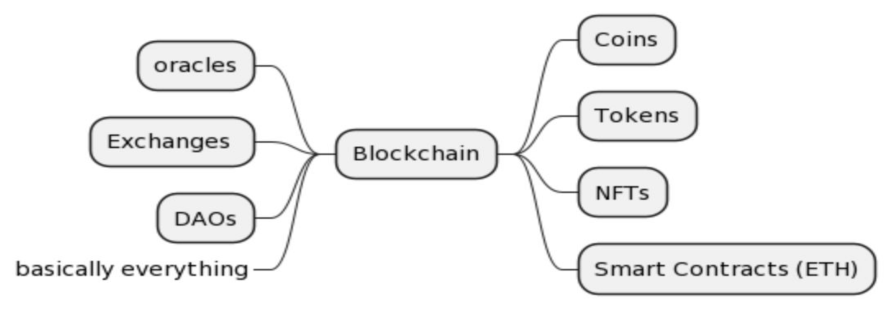
- Forgetting your wallet’s seed phrase means you lose everything
- Backups are crucial to avoid losing all digital assets
- New “accounts” may be lost if restoring a wallet from a backup w/o the new account
- Vulnerable to phishing attacks or malicious s/w
- Bugs or poor design can lead to lost money or lost transactions

Bitcoin Blockchain

(deeper)

Spoiler: There are no “accounts”, “users”, or “balances” on the bitcoin blockchain. Coins are stored at cryptographic addresses (2^160 possible) similar to an email address. An address’ balance needs to be computed and stored off-chain based on all transactions.

Dependants



Use Cases

- Each block contains multiple transactions
- Each transaction sends coins from multiple sources to multiple destinations
  - Destinations can be owned by multiple “people”
- Any coins not sent another person is “change” and needs an explicit address
  - The same address or a new one for greater anonymity
- Wallets hide many of these addresses from the users, but they exist

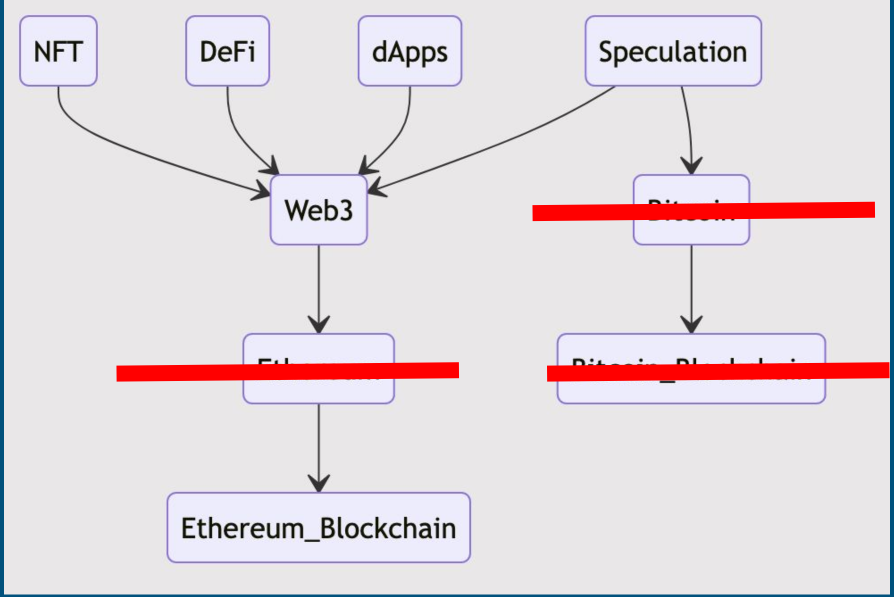
Risks

- Confusion about tracking change in a new address leads to wallets not being backed up properly
- Changing wallets needs to be handled carefully since not transferring all addresses can lead to lost money
- Anonymity is not absolute; no privacy by design

Calibration

Covered:

- Blockchain
- Coins/tokens
- Ethereum
- Bitcoin



Web3

Ethereum Blockchain
Decentralized Apps (dApps)

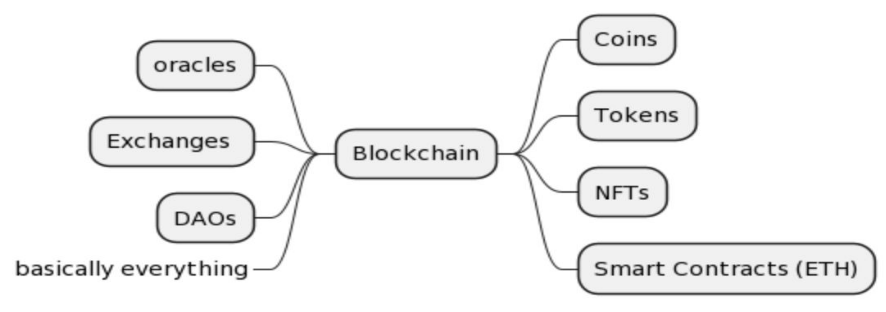
0:40

Ethereum Blockchain

(deeper)

Unlike with Bitcoin, the Ethereum Blockchain does store accounts and balances. The Eth Blockchain is a virtual compute environment with a state machine and a feature-rich scripting language.

Dependants



Use Cases

- Users will typically have one address through which all transactions take place
- Wallets will support the user creating and managing multiple accounts
- Transfers from one account to another is done on the Blockchain incurring fees

Risks

- Multiple accounts need to managed carefully to ensure the private keys aren't lost
- Changing wallets needs to be handled carefully since not transferring all addresses can lead to lost money
- Anonymity is not absolute; no privacy by design
- Once a 3rd-party can map your "identity" to your account, they can see all your past transactions
  - Think life insurance looking at past purchases
- It's still possible to glean personal identity from a Blockchain identity

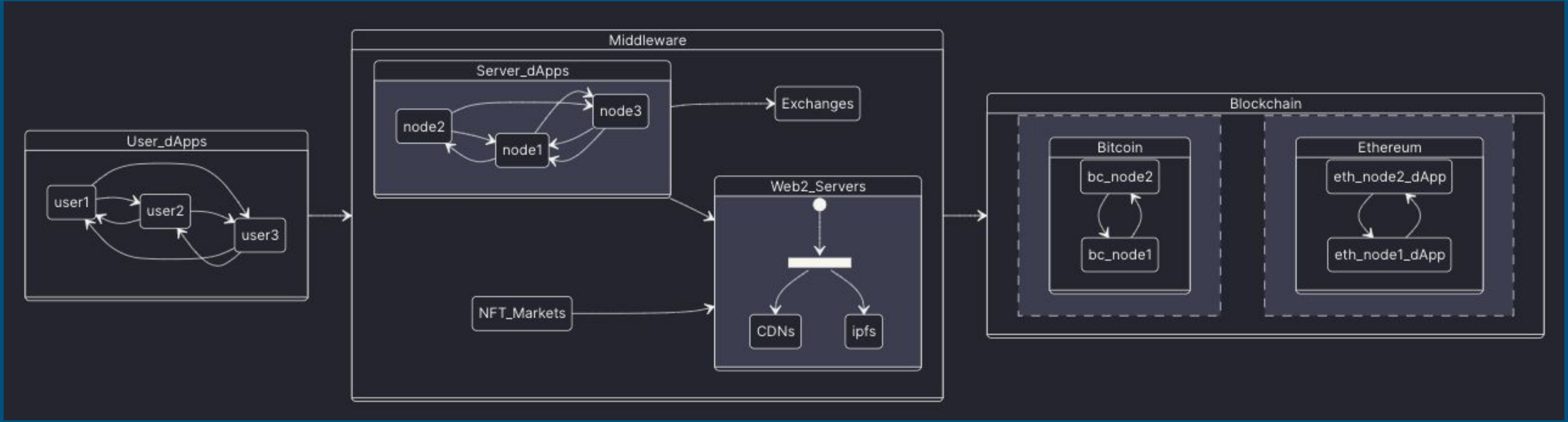
What are dApps?

They are apps that run on the Blockchain via Smart Contracts.

They are also apps that run at the user level like peer-to-peer (P2P) apps (eg, BitTorrent)

Smart Contracts are supported by a few Blockchains like Ethereum and Solana

Bitcoin has a scripting language, but it’s not very robust

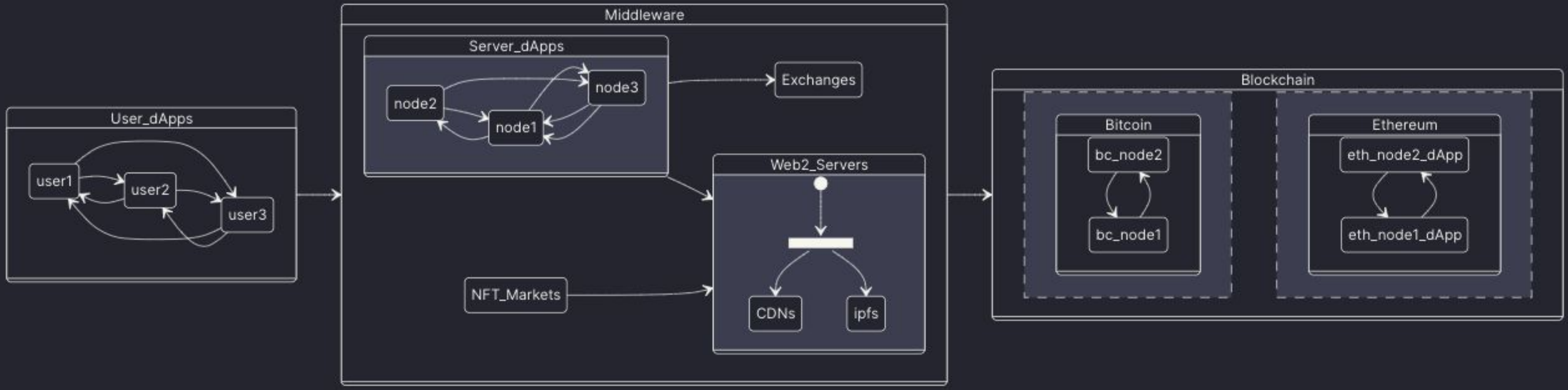


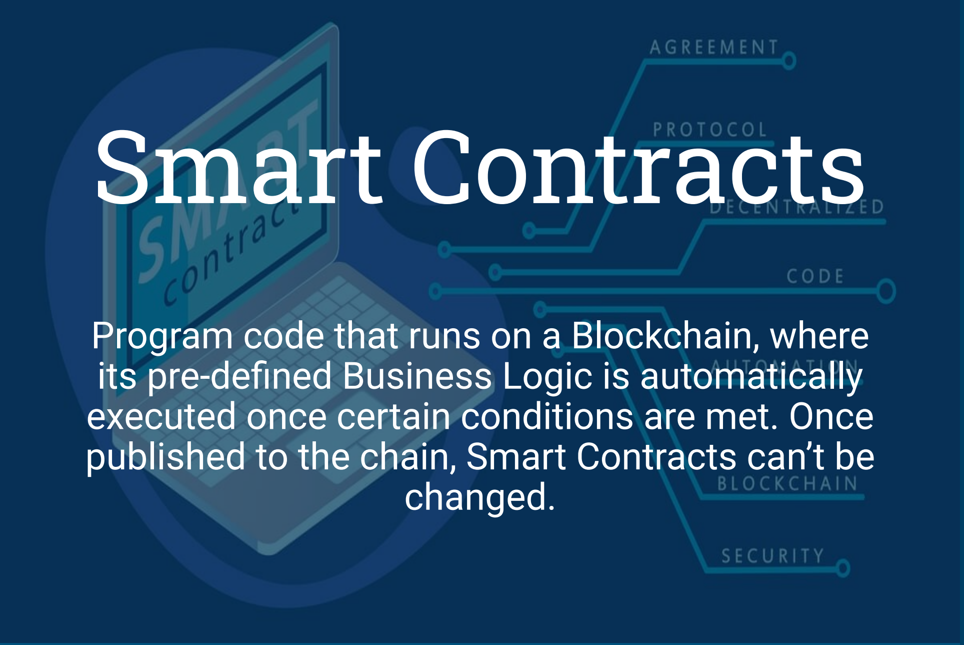
Decentralized re-visited

There is a tendency for many Web3 projects to proclaim they're decentralized because they are on a blockchain.

Web3 dApps must use and trust middleware APIs and platforms, making them more Federated than decentralized.

This is known as the platform v protocol dilemma

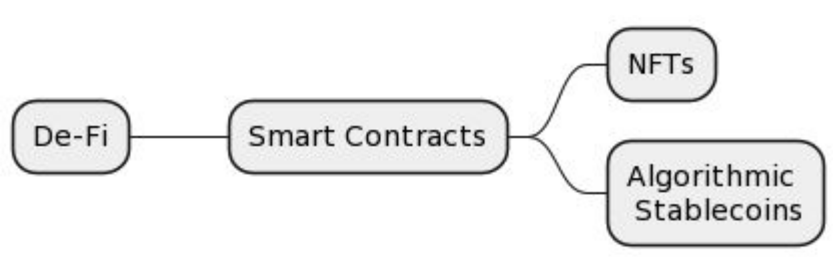




Smart Contracts

Program code that runs on a Blockchain, where its pre-defined Business Logic is automatically executed once certain conditions are met. Once published to the chain, Smart Contracts can’t be changed.

Dependants



Use Cases

- Trustless agreements between 2 parties - no need for 3rd-party intermediaries
- DeFi uses like lending, borrowing, swapping
- NFTs - unique digital assets
- Legally-recognized in several states as representing “enforceable” contracts

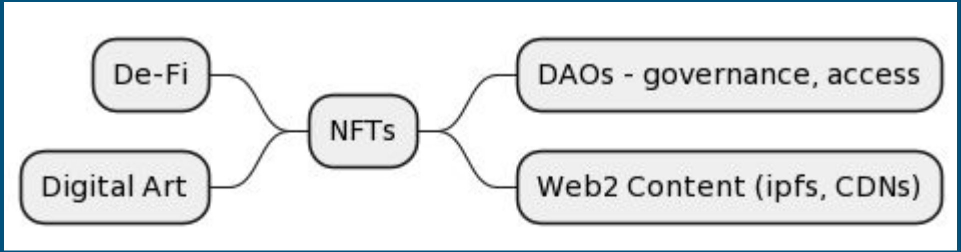
Risks:

- Smart Contracts on Bitcoin face difficulties: heterogeneous approach, use of poorly-documented features
- Enforceability has is not yet a proven legal concept
  - Tokens don’t require a signature or approval for acceptance into an address
  - Is it a contract w/o a signature?

NFTs

Non-Fungible Tokens are crypto-tokens bought and stored on a blockchain backed by a Smart Contract. NFTs represent unique, rare, and indivisible digital assets. Having a NFT in your wallet grants you special permissions based on the Smart Contract.

Dependants



De-Fi

Digital Art

NFTs

DAOs - governance, access

Web2 Content (ipfs, CDNs)

Use Cases

- In-game purchases
- Social media profile pics stored on Web2
- Access to exclusive online communities (usually Discord)
- Voting rights on DAOs and other communities
- Digital art

Risks:

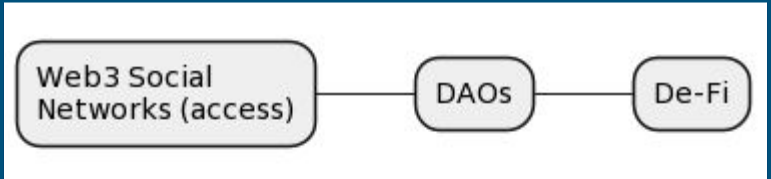
- Speculative market - Morgan Stanley is predicting an NFT crash
- High transaction fees put pressure on storing more data on Blockchain
- Content is not stored on-chain, but on web2 servers
- Content is public - nothing private can be stored on a public Blockchain
- Anybody can send you any NFT they'd like:
  - Picture of your house
  - NSFW images
  - Malicious NFT that executes malicious contract code when try to delete it

DAOs

Distributed Autonomous Organizations

A blockchain-based form of organization or company that is often governed by a native crypto token. Anyone who purchases and holds these tokens gains the ability to vote on important matters directly related to the DAO. They typically use smart contracts in place of traditional corporate structures to coordinate the efforts and resources of many towards common aims.

Dependants



Use Cases

- Crowdfunding the purchase of a copy of the Constitution
- Organize and make decisions about the direction of a DeFi project, NFT, or other digital community effort
- Uniswap - Cryptocurrency exchange

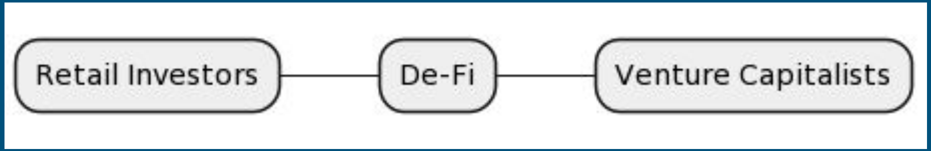
Risks:

- The DAO - DeFi VC project - hacked and robbed
- Digitization of country club networking

DeFi

Decentralized finance (DeFi) refers to blockchain applications that cut out middlemen from financial products and services like loans, savings, and swaps. All it takes is a smart person to create a protocol and write some smart contract code.

Dependants



Retail Investors

De-Fi

Venture Capitalists

Use Cases

- Loans w/o paperwork or thresholds
- Yield Farming with high yields (10%+)
- DAO structure - investors can vote on interest policy
- The credit risk models for Blockchain-based lending markets is similar to non-crypto markets

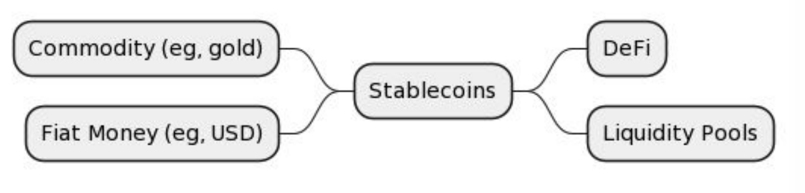
Risks:

- Flaws in code are common and Smart Contracts are open sourced
  - Credit risk on Blockchain moves from risk of borrower to risk of code of the system
- Trading frenzies on top of a rate-limited blockchain can lead to very high gas fees and lost trades
  - A lost trade can also mean you lose your coins with nothing in return
- The lending markets are immature and underlying weaknesses of Blockchain make mistakes immutable
- Scam Exchanges promise high rates of return and then impose high fees to remove your money or steal it altogether
- Yield farming projects need liquidity and need to draw in new investors to pay out existing investors

Stablecoin

Cryptocurrencies whose value is pegged, or tied, to that of another currency, commodity or financial instrument. Stablecoins aim to provide an alternative to the high volatility of the most popular cryptocurrencies including Bitcoin (BTC), which has made such investments less suitable for wide use in transactions.

Dependants



Commodity (eg, gold)

Fiat Money (eg, USD)

Stablecoins

DeFi

Liquidity Pools

Use Cases

- Used as collateral backing for DeFi liquidity pools
- Algorithmic stablecoins (eg, Terra) do not depend on “cash” reserves for stability
  - Use a dual coin/token system to stabilize the coin’s external peg (eg, Terra’s UST/Luna)
  - Algorithms burn/mint one or the other based buy/sell pressures on the coin/token

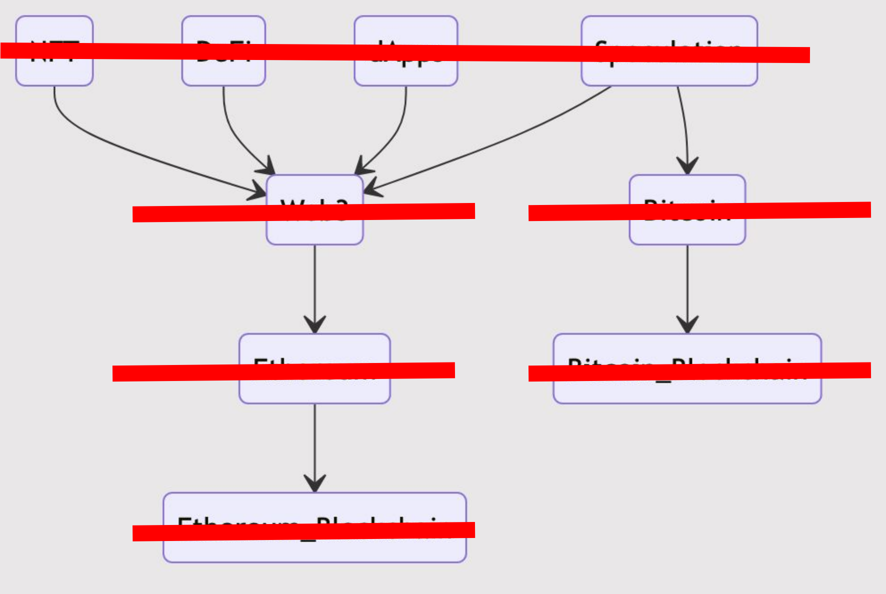
Risks:

- Vulnerable to attack with a large volume transaction that de-pegs the coin (eg, Terra/UST), which can lead to a death spiral of arbitrage and panic selling
- False sense of stability leads DeFi projects to place all their investments into the stablecoin (eg, Stablegains crash due to UST/Luna crash)
- Stablecoins are not fully audited (Circle’s USDC)
- Attestations don’t break down between liquid and illiquid reserves - adding risk the stablecoin can’t handle a “run on the bank”

Calibration

Covered:

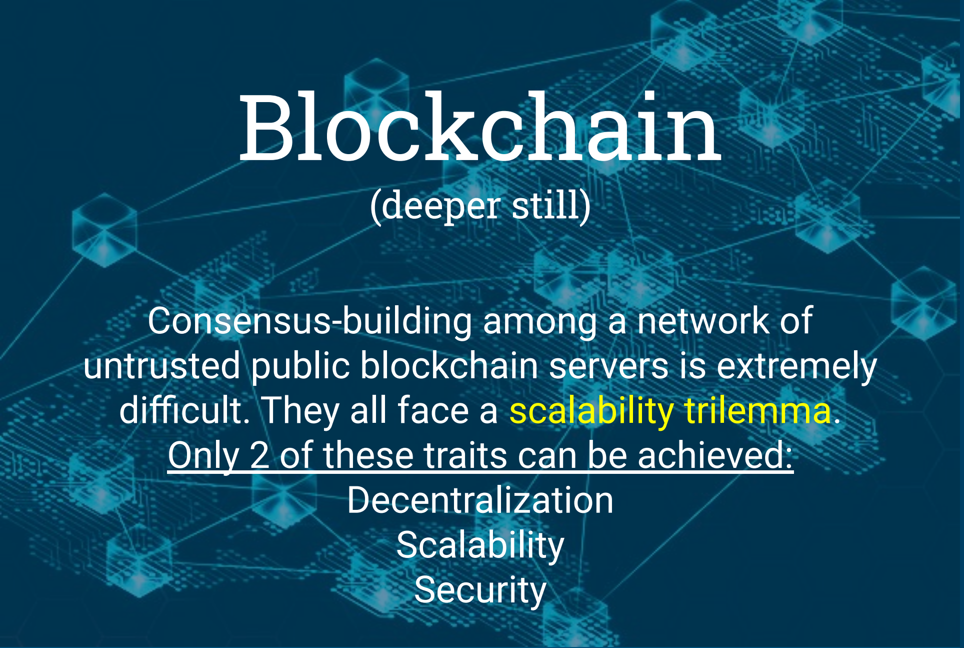
- Smart Contracts
- NFTs
- DeFi
- dApps



1:00

Even More Blockchain

0:40



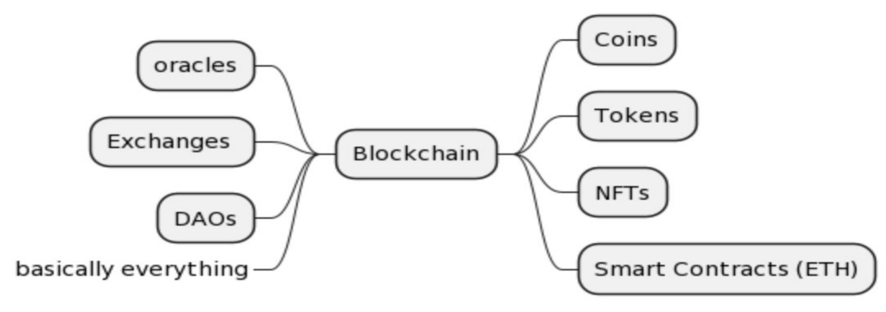
Blockchain

(deeper still)

Consensus-building among a network of untrusted public blockchain servers is extremely difficult. They all face a scalability trilemma. Only 2 of these traits can be achieved:

Decentralization
Scalability
Security

Dependants



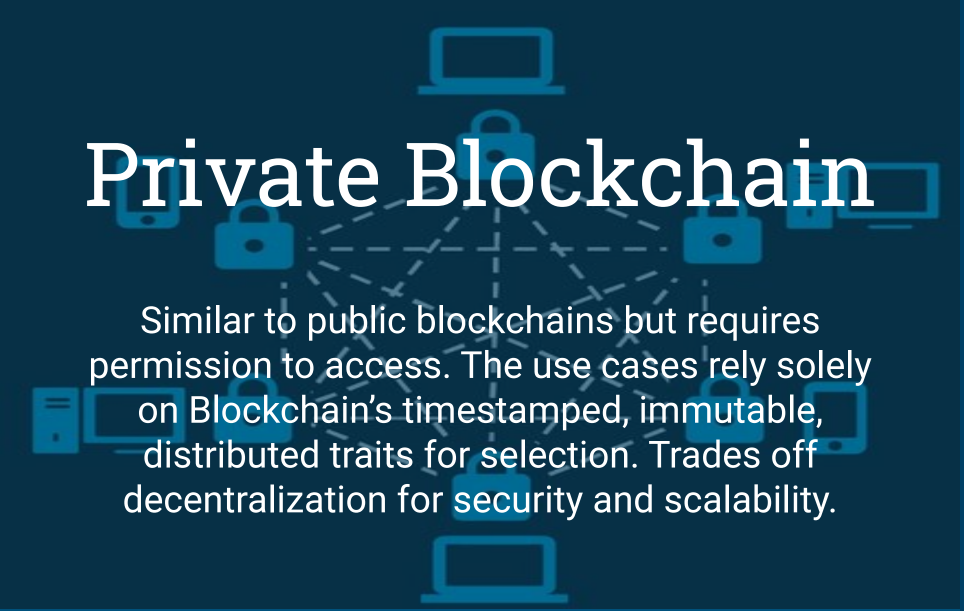
oracles
Exchanges
DAOs
basically everything
Blockchain
Coins
Tokens
NFTs
Smart Contracts (ETH)

Use Cases

- Proof of Work is deliberately compute-heavy and throttled (1 validated block every 10 mins) to achieve decentralization & security
- Proof of Stake is to add scalability, but at risk of decreased security
- Eth Blockchain Sharing adds Federation to address scalability and security, but loses decentralization
- Monetary incentives are built-in to incentivize unrelated parties to run the needed infrastructure
    - The server that gets to validate a new Block of data is granted some fractional coins (mining)
    - Transaction fees are shared

Risks

- Multiple blockchains expose more attack surfaces, fragmented functionality, and more bugs in dApps
- Monetary incentives for Blockchain node operators may not be sufficient as rules change and coin supply diminishes
- Web3 onchain changes are monetized, forcing them offchain, centralized, and unencrypted
    - Updating your profile pic
    - Transferring from one account to another
    - Saving social media status



Private Blockchain

Similar to public blockchains but requires permission to access. The use cases rely solely on Blockchain’s timestamped, immutable, distributed traits for selection. Trades off decentralization for security and scalability.

Dependants

Use Cases

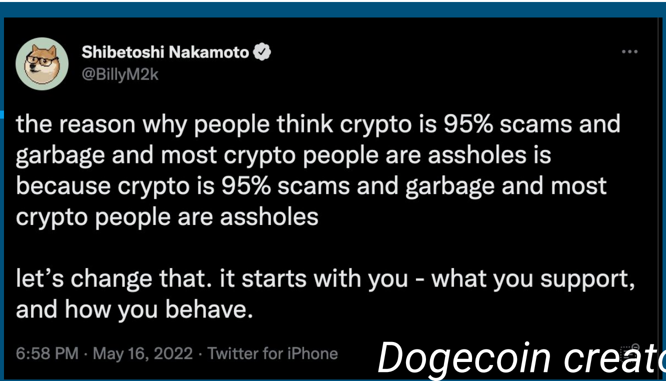
- Business workflows across corporate boundaries
- Provenance - records showing the history of each asset exist
- Improved discoverability

Risks

- Access must be managed by a central authority
- Blockchain data storage capacity is limited, requiring external servers which require proper permissions
- Managing access to Wallet needs to be tightly integrated with corporate Identity Access Management (IAM) systems (eg, Okta, SAML)
  - Employees should not be able to see private keys in order to retain them after they leave

Scams and Thefts

Scams & Thefts Rise >>> b/c the Targets are Rich



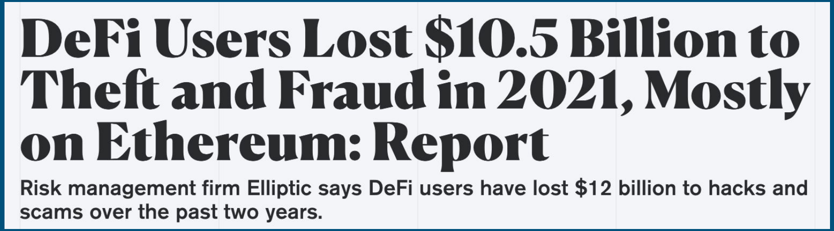
Shibetoshi Nakamoto
@BillyM2k

the reason why people think crypto is 95% scams and garbage and most crypto people are assholes is because crypto is 95% scams and garbage and most crypto people are assholes

let's change that. it starts with you - what you support, and how you behave.

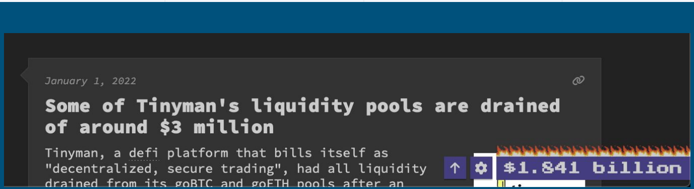
6:58 PM · May 16, 2022 · Twitter for iPhone

Dogecoin creator



DeFi Users Lost $10.5 Billion to Theft and Fraud in 2021, Mostly on Ethereum: Report

Risk management firm Elliptic says DeFi users have lost $12 billion to hacks and scams over the past two years.



January 1, 2022

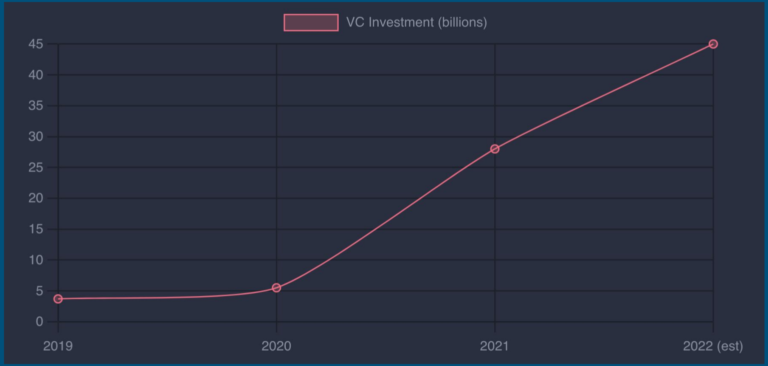
Some of Tinyman's liquidity pools are drained of around $3 million

Tinyman, a defi platform that bills itself as "decentralized, secure trading", had all liquidity drained from its goBTC and goETH pools after an

~$2B in scams/thefts YTD

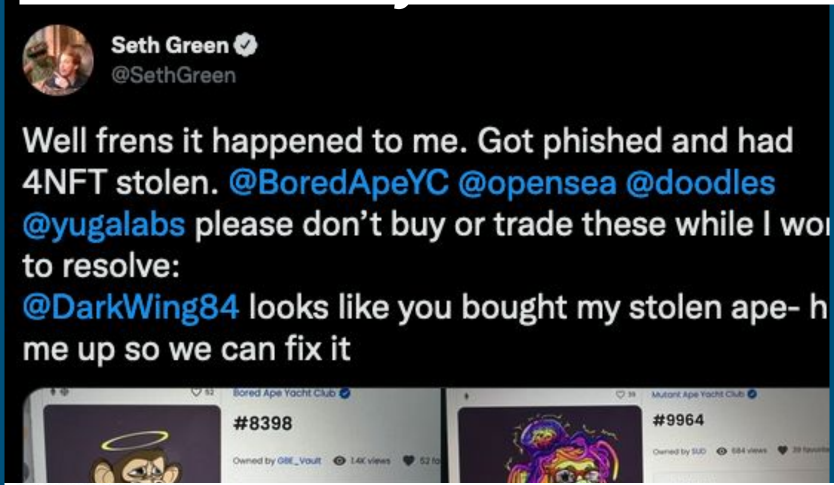
"I rob banks because that's where the money is"
Willie Sutton, bank robber

"$300B in TLV across all DeFi protocols…with 4 million unique addresses"
Medium.com, Mar 2022



VC Crypto Investments (billions)

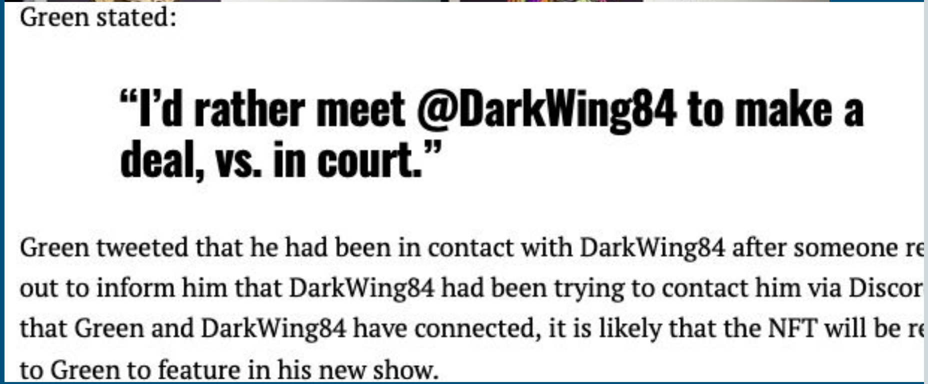
Case Study: Seth Green's Bored Apes Theft



Seth Green
@SethGreen

Well frens it happened to me. Got phished and had 4NFT stolen. @BoredApeYC @opensea @doodles @yugalabs please don't buy or trade these while I wor
to resolve:
@DarkWing84 looks like you bought my stolen ape- h
me up so we can fix it

Bored Ape Yacht Club
#8398
Owned by GBE_Vault 1.4K views 52 fa
Mutant Ape Yacht Club
#9964
Owned by SUD 684 views 39 favorite



Green stated:

> **"I'd rather meet @DarkWing84 to make a deal, vs. in court."**

Green tweeted that he had been in contact with DarkWing84 after someone re
out to inform him that DarkWing84 had been trying to contact him via Discor
that Green and DarkWing84 have connected, it is likely that the NFT will be re
to Green to feature in his new show.

Seth fell for a fake cloned site and lost 4 NFT's.

OpenSea stopped the sale of the NFTs.

Looks like Seth's publicity might bring his Apes home.

But…

What if you're not famous? Or spent $$$ on NFTs?

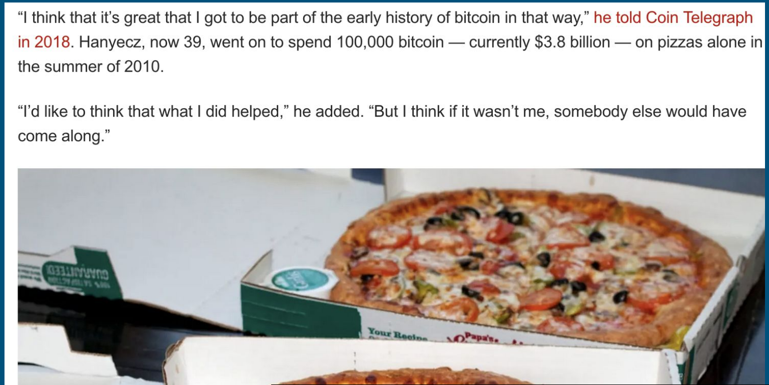
What court would hear this case? What if OpenSea decides not to intercede for you?

@DarkWing84 could sell NFTs directly without going through OpenSea

What if Seth was lying about being phished? Just had seller's remorse?

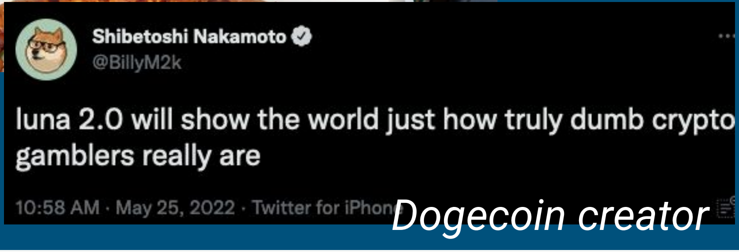
Bubbly

FTX Exchange is a leading centralized cryptocurrency exchange specializing in derivatives and leveraged products



“I think that it’s great that I got to be part of the early history of bitcoin in that way,” he told Coin Telegraph in 2018. Hanyecz, now 39, went on to spend 100,000 bitcoin — currently $3.8 billion — on pizzas alone in the summer of 2010.

“I’d like to think that what I did helped,” he added. “But I think if it wasn’t me, somebody else would have come along.”

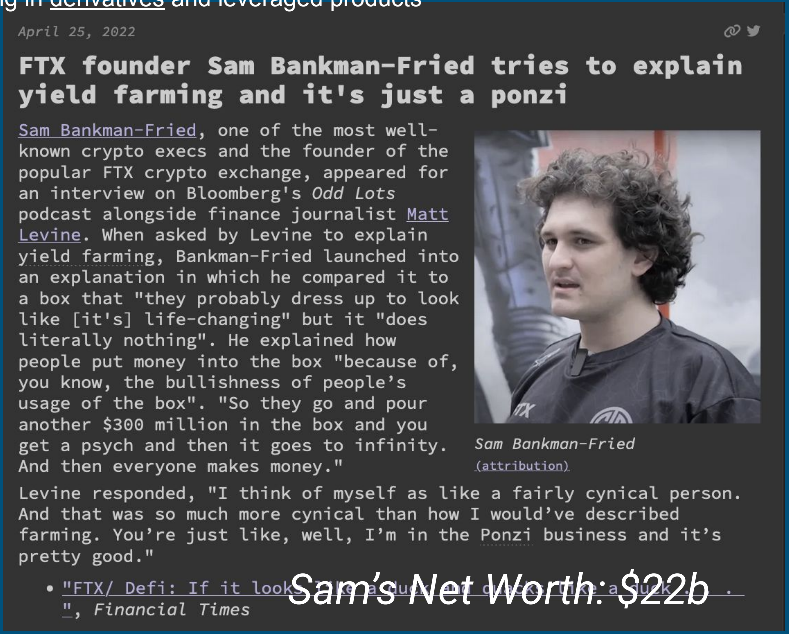


Shibetoshi Nakamoto
@BillyM2k

luna 2.0 will show the world just how truly dumb crypto gamblers really are

10:58 AM · May 25, 2022 · Twitter for iPhone

Dogecoin creator



April 25, 2022

FTX founder Sam Bankman-Fried tries to explain yield farming and it's just a ponzi

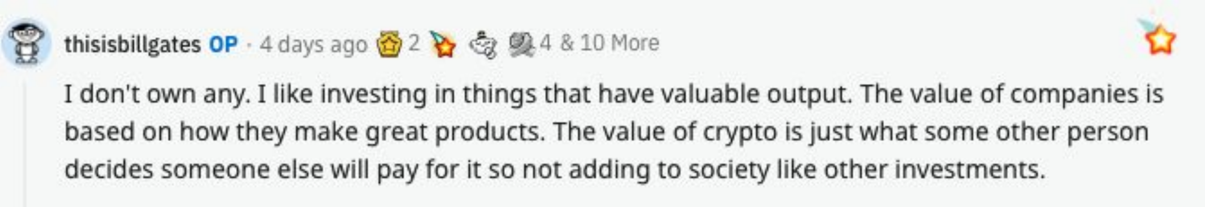
Sam Bankman-Fried, one of the most well-known crypto execs and the founder of the popular FTX crypto exchange, appeared for an interview on Bloomberg's *Odd Lots* podcast alongside finance journalist Matt Levine. When asked by Levine to explain yield farming, Bankman-Fried launched into an explanation in which he compared it to a box that "they probably dress up to look like [it's] life-changing" but it "does literally nothing". He explained how people put money into the box "because of, you know, the bullishness of people’s usage of the box". "So they go and pour another $300 million in the box and you get a psych and then it goes to infinity. And then everyone makes money."

Sam Bankman-Fried
(attribution)

Levine responded, "I think of myself as like a fairly cynical person. And that was so much more cynical than how I would’ve described farming. You’re just like, well, I’m in the Ponzi business and it’s pretty good."

- "FTX/ Defi: If it looks like a duck and quacks like a duck . . . ", *Financial Times*

Sam’s Net Worth: $22b

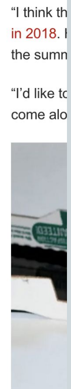


thisisbillgates OP · 4 days ago 2 4 & 10 More

I don't own any. I like investing in things that have valuable output. The value of companies is based on how they make great products. The value of crypto is just what some other person decides someone else will pay for it so not adding to society like other investments.

Pause on this...

FTX Exchange is a leading centralized cryptocurrency exchange specializing in derivatives and leveraged products



"I think th

in 2018. I

the sumn

"I'd like to

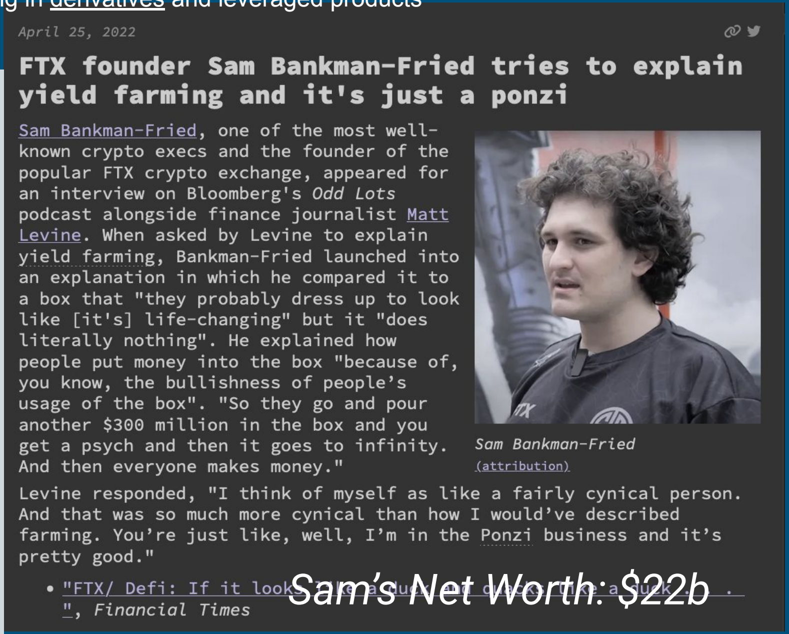
come alo

"People put money into the box because of, you know, the bullishness of people's usage of the box…It goes to infinity and then everyone makes money"

Sam Bankman-Fried on Yield Farming

"victims to believe that profits are coming from legitimate business activity, and they remain unaware that other investors are the source of funds"

Definition of a Ponzi Scheme



April 25, 2022

FTX founder Sam Bankman-Fried tries to explain yield farming and it's just a ponzi

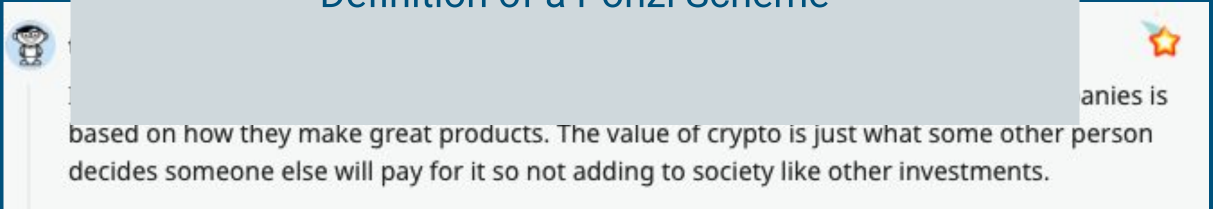
Sam Bankman-Fried, one of the most well-known crypto execs and the founder of the popular FTX crypto exchange, appeared for an interview on Bloomberg's *Odd Lots* podcast alongside finance journalist Matt Levine. When asked by Levine to explain yield farming, Bankman-Fried launched into an explanation in which he compared it to a box that "they probably dress up to look like [it's] life-changing" but it "does literally nothing". He explained how people put money into the box "because of, you know, the bullishness of people's usage of the box". "So they go and pour another $300 million in the box and you get a psych and then it goes to infinity. And then everyone makes money."

Sam Bankman-Fried
(attribution)

Levine responded, "I think of myself as a fairly cynical person. And that was so much more cynical than how I would've described farming. You're just like, well, I'm in the Ponzi business and it's pretty good."

- "FTX/ Defi: If it looks like a duck and quacks like a duck", *Financial Times*

Sam's Net Worth: $22b



anies is based on how they make great products. The value of crypto is just what some other person decides someone else will pay for it so not adding to society like other investments.

Summary & Conclusions

1:20

Summary

Applying Game Theory to the bottom layer (Blockchain) of the tech stack monetizes the entire ecosystem:

- Speculation and fast liquidity events lead to large investment
- Which leads to boom/bust cycles
- Re-directing investment from tech innovations that are needed to correct functional weaknesses and vulnerabilities
- Making the system unreliable for daily use
- Not to mention high gas fees when volume increases (a mini-auction for each transaction based on fees)

The Blockchain has to solve many competing gnarly problems, forcing trade-offs, some worse than others:

- Slow performance (10 mins for 1 block validation to allow for all nodes to sync up)
- Intense energy consumption (Proof of Work v Proof of Stake or Proof of History)
- Non-scalable (each node processes all transactions)
- Weak security (public v private Blockchains)
- Federated Blockchain (sharding to improve scalability)
- Privacy compromised (once someone knows your public key address, they can see all your transactions)

Web3 is built on these same assumptions

- No separation of tech and business and financial models
- No easy way to optimize (scale, innovate) the separate components without compromising the whole system
- Better tech isn't the solution to existing social networking problems

Conclusion

Crypto is a tightly-coupled, co-dependent financial and technical ecosystem reliant on code and online computationally-intensive servers to function.

It has captured billions of dollars in value that act as a honeypot to be gamed by scammers and thieves and whale investors to make quick profit off the continuing inflow of investment dollars.

Many see crypto as a way to make generational wealth outside of the broader financial system corrupted by the the rich and powerful, not realizing the crypto world has become corrupted by the same parties.

The technical underpinnings of the system are tightly-coupled which makes it difficult to upgrade or improve without causing vulnerabilities and weaknesses in the entire system.

Blockchain is not a static or homogenous technology, but a shifting trade-off of compromises to satisfy different sets of technical challenges.

Blockchain's immutability and tight integration with currency makes any flaw more highly critical than other similar tech.

More better tech is repeating the same mistakes made by social networking companies.

Background

Isn't this just overblown?
It's just like the dot-com bubble burst… right?

“Crypto currency industry is several different layers of industry, each moving in different directions and pulled by different forces. The bulk of market participants are people who've joined in the last 2 years, market-makers and venture capitalists who are driving the bulk of market dollars. VCs want things that they can grow fast and get liquidity from. Retail wants projects that they can make a quick buck on. Meanwhile the bulk of development work and research and thought that goes into the core crypto currency systems are by people who have been around for years. The bitcoin developers still care about solving challenging questions around decentralization, censorship resistance, privacy, and resiliency. But they do not command the massive amount of money and armies of people to make a significant impact.”

If we’re in a crypto bubble, will Blockchain survive?

Naturally there are other ways in which blockchains and regular databases can be compared. We could talk about codebase maturity, developer attractiveness, ecosystem breadth and more. But none of these issues are **_inherent_** to the technology itself. So when it comes to a long-term decision on using a blockchain, the question to ask is this:

- What’s more important for my use case?

- Disintermediation and robustness? -> Blockchain

- Or confidentiality and performance? -> Centralized DB

When examined in this simple light, many of the use cases currently under discussion **do not make sense**. The biggest problem tends to be confidentiality. The participants in a fiercely competitive marketplace will naturally prefer the privacy of a centralized database, rather than reveal their activities to each other. This is especially true if a trusted central party already exists and can provide the neutral territory in which that database can reside. Even though there may be some cost associated with this central provider, this is more than justified by the value of the privacy retained. The only motivation for a shift to blockchains would be aggressive new regulation

Are NFTs legally-recognized? >> Unclear

- States have passed laws to recognize crypto Smart Contracts as enforceable contracts
- Does the NFT grant IP or Copyright rights to the receiver? Typically not.
- Tokens w/ smart contracts can be sent to anybody’s blockchain address without approval or signature
  - Can the recipient be held accountable in a court of law?
- The Smart Contract is code
  - Can the originator of the code be held accountable in a court of law?
- The originator can be an individual or DAO
  - Is a DAO a legally-recognized entity that can be held accountable in a court of law?

Are crypto transactions really anonymous?

- To buy/sell cryptocurrency, you need to verify your identity with an online wallet or exchange according to KYC (know your customer) regulations
- To truly transact anonymously, you would need to acquire bitcoin in a private transaction or do mining
  - The dark web could be used for the private transaction
- Chain analysis can, at times, identify the owners of wallets on the blockchain
  - To avoid detection, use multiple “wallets” with each transaction
  - Route your coins through a tumbler that handles this kind of “washing” automatically
- Your identity is not as anonymous as people claim

Is web3 really decentralized? >> Yes and no

- This requires a deeper discussion into protocol v platform evolutions
- Bottom line is yes and no
- Platforms will evolve and are mostly Federated layers
- Some NFTs can only be viewed on 1 centralized platform
- Most digital content can’t be stored on the Blockchain
    - They are stored on traditional web2 content servers and ipfs

Will Blockchain survive?

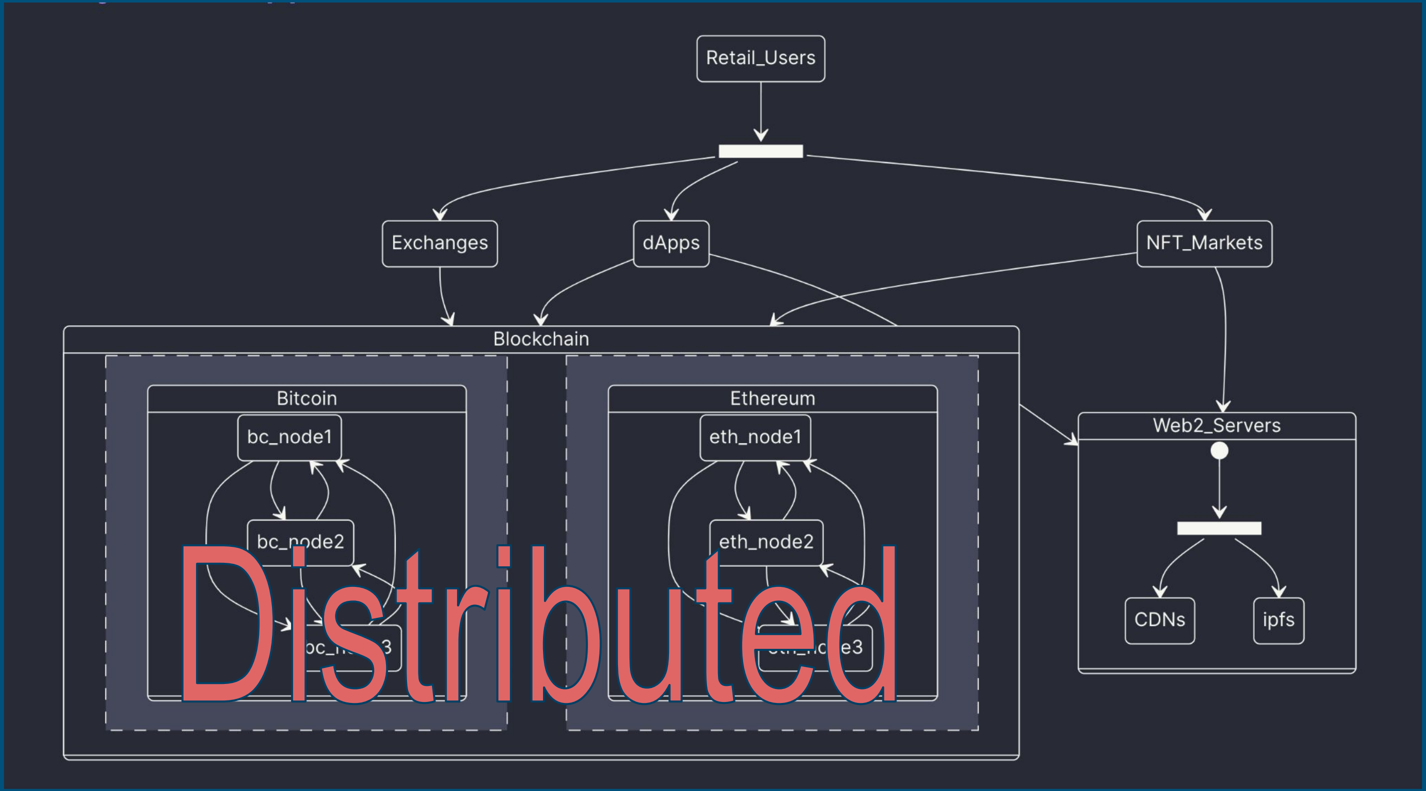
Many news sources, pundits, crypto exports say glibly “Oh, the bubble will burst, but the Blockchain will survive”

But, which Blockchain? Which set of scalability trade-offs will prove most useful going forward?

Is Blockchain tech inherently superior to existing SQL and NoSql databases?

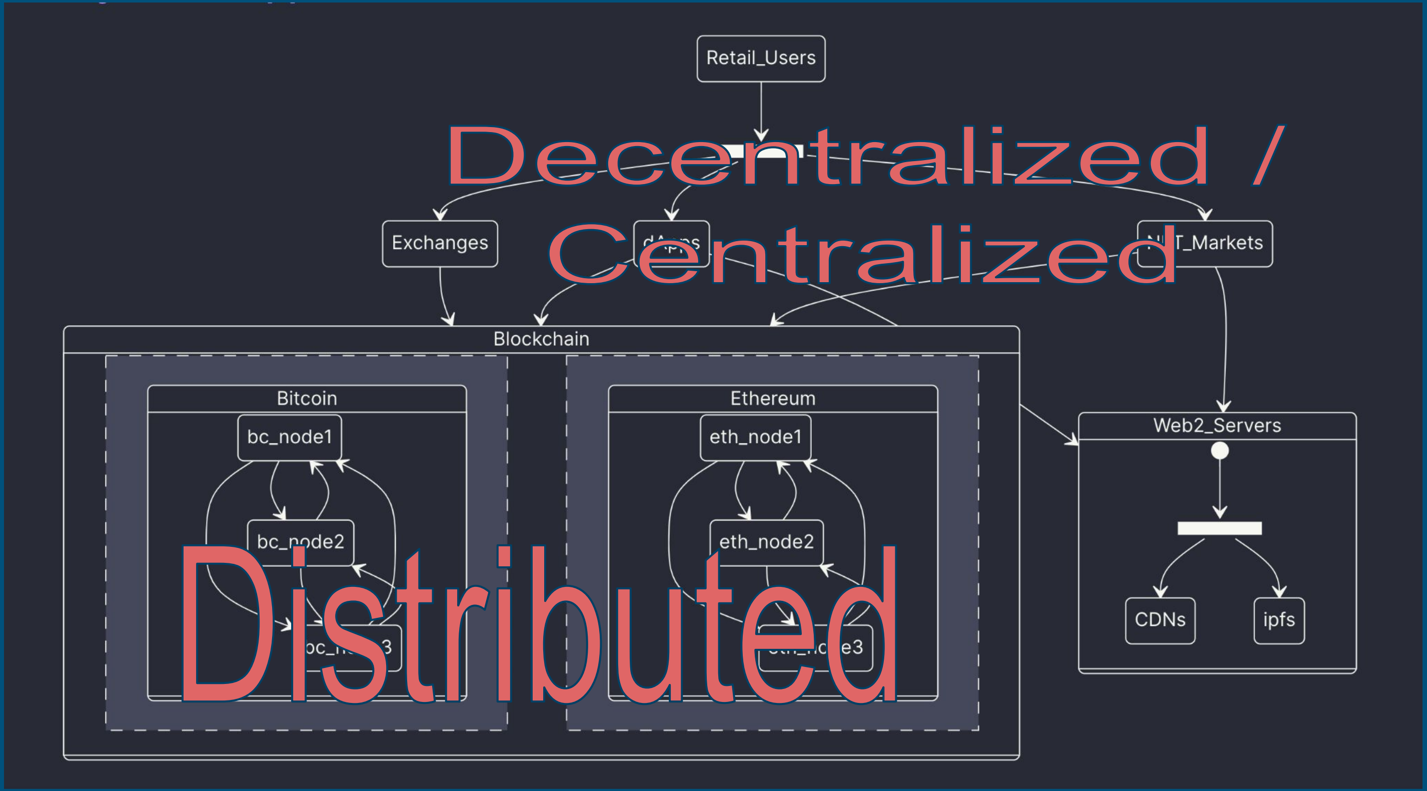
Aren’t these just technical problems that can be resolved?

Decentralized is better than Centralized



Distributed

Decentralized is better than Centralized



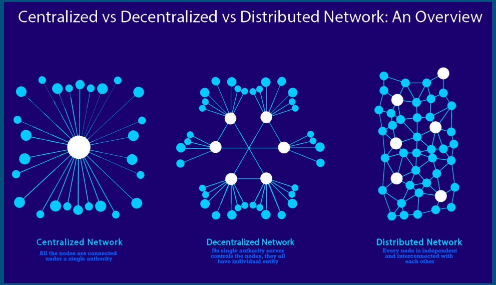
Decentralized / Centralized

Distributed

Decentralized is better than Centralized

Web2 Examples:

Example	Communication	Data Model	Login Paths
Social Media	Decentralized (APIs)	Centralized	Centralized
E-mail	Decentralized	Decentralized	Centralized
Productivity Tools	Decentralized (APIs)	Centralized/ Decentralized	Decentralized (SSO)


Centralized vs Decentralized vs Distributed Network: An Overview
Centralized Network
All the nodes are connected under a single authority
Decentralized Network
No single authority server controls the nodes, they all have individual entity
Distributed Network
Every node is independent and interconnected with each other

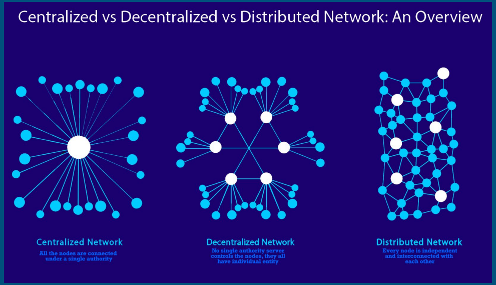
Decentralized is better than Centralized

Crypto/Web3 Examples:

Example	Communication	Data Model	Login Paths
Blockchain	Distributed	Distributed	Decentralized
Exchanges	Decentralized	Decentralized	Centralized
NFTs	Centralized/ Decentralized	Centralized/ Decentralized	Centralized

Only the Blockchain layer is truly distributed.

Not all data is stored on-chain, but also on web2 servers


Centralized vs Decentralized vs Distributed Network: An Overview
Centralized Network
All the nodes are connected under a single authority
Decentralized Network
No single authority server controls the nodes, they all have individual entity
Distributed Network
Every node is independent and interconnected with each other