Universal Computation on the Blockchain: Ethereum and Smart Contracts

Anthony Lee Zhang

March 28, 2024

Outline

- Brief History
- Structure of Ethereum
  - Smart contracts
  - Gas
  - User interface
  - Data
- Alt L1's, L2's
- The Market For Promises

Vitalik Buterin

- Born in Kolomna, Russia, 1994 (younger than me!), father a computer scientist
- Moved to Canada at 6
- Attended University of Waterloo, RA'd for cryptographer Ian Goldberg
- Wrote Ethereum whitepaper in 2014
- Got $100k Thiel fellowship in 2014, dropped out to work on Ethereum full-time

Vitalik Buterin

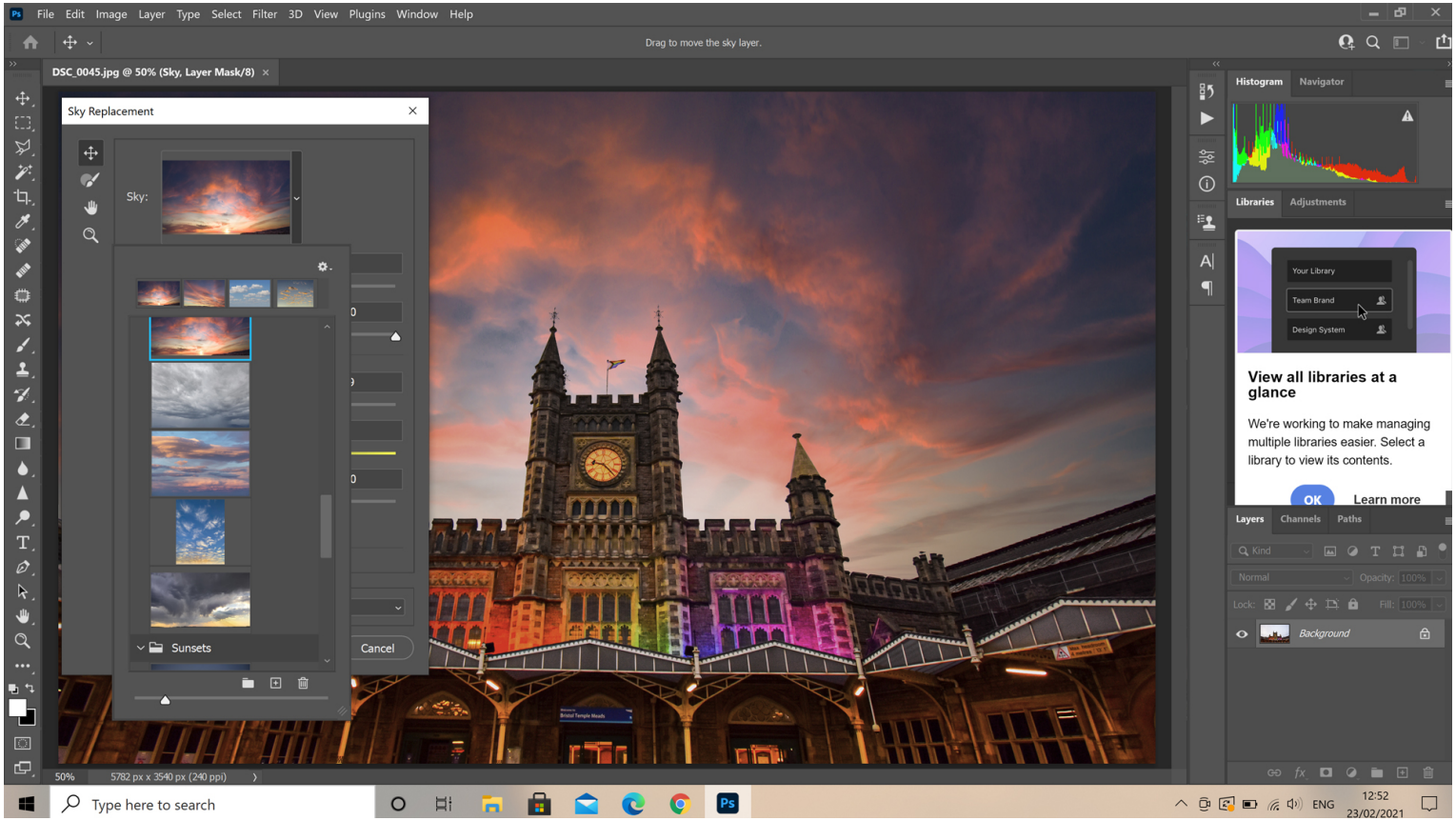
I was born in 1994 in Russia and moved to Canada in 2000, where I went to school. I happily played World of Warcraft during 2007-2010, but one day Blizzard removed the damage component from my beloved warlock's Siphon Life spell. I cried myself to sleep, and on that day I realized what horrors centralized services can bring. I soon decided to quit.

In 2011, searching for a new purpose in life, I discovered Bitcoin. At first, I was skeptical, and did not understand how it could possibly have value without physical backing. But slowly I became more and more interested. I started writing for a blog called Bitcoin Weekly initially at a meek wage of $1.5 per hour, and soon with Mihai Alisie cofounded Bitcoin Magazine.

In 2012, I entered the University of Waterloo; in 2013 I realized that crypto projects were taking up 30h/week of my time, so I dropped out. I went around the world, explored many crypto projects, and finally realized that they were all too concerned about specific applications and not being sufficiently general - hence the birth of Ethereum, which has been taking up my life ever

Application-Specific Computers

What Non-Programmers Think Programming Is. . .



Universal Computation

- Any computing system with, essentially, if statements and ability to read data, is Turing complete
- Any Turing-complete language can perform same tasks as any other!

Universal Computation

- Any computing system with, essentially, if statements and ability to read data, is Turing complete
- Any Turing-complete language can perform same tasks as any other!
- Vitalik's insight: instead of application-specific blockchains, we should build a blockchain universal computer
- No need to build lots of "buttons": give devs a Turing-complete system, they can build their own buttons!

Universal Computation

- Any computing system with, essentially, if statements and ability to read data, is Turing complete
- Any Turing-complete language can perform same tasks as any other!
- Vitalik's insight: instead of application-specific blockchains, we should build a blockchain universal computer
- No need to build lots of "buttons": give devs a Turing-complete system, they can build their own buttons!
- Next, let's talk about the structure of Ethereum, and how it enables universal computation

Why Worry About the Tech?

"If I'm not a developer, why should I worry about the technical details?"

Why Worry About the Tech?

"If I'm not a developer, why should I worry about the technical details?"

- If you "screen" opportunities/investments: lots of BS in the space!
  - Simple understanding of the tech helps you evaluate ideas that are "fits", vs pure marketing

Why Worry About the Tech?

"If I'm not a developer, why should I worry about the technical details?"

- If you "screen" opportunities/investments: lots of BS in the space!
  - Simple understanding of the tech helps you evaluate ideas that are "fits", vs pure marketing
- If you want to start a company, need to have at least a nontechnical understanding
  - What is special about the technology? What can I do that I couldn't do before?

Why Worry About the Tech?

"If I'm not a developer, why should I worry about the technical details?"

- If you "screen" opportunities/investments: lots of BS in the space!
  - Simple understanding of the tech helps you evaluate ideas that are "fits", vs pure marketing
- If you want to start a company, need to have at least a nontechnical understanding
  - What is special about the technology? What can I do that I couldn't do before?
- Hopefully, as you'll see, the tech is also not that hard!

The Structure of Ethereum

- Smart Contracts
- Gas
- User Interface
- Data
- Proof of Stake

Smart Contracts

- A smart contract is:
  - A wallet, which can hold ETH,
  - Behavior determined by code,
  - Can have persistent data
- If you've heard of object oriented programming: smart contracts are a bundle of functions (code), and data, as well as ETH balances

Smart Contract Example: Tokens

- Fun fact: your ETH address, "technically", only "holds" Ethereum – no other tokens!
- Instead, non-ETH tokens are implemented through smart contracts
- Let's briefly walk through how we'd set up a smart contract for a token

Smart Contract Example: Tokens

Smart Contract Example: Tokens

Smart Contract Example: Tokens


```
owner.mint(receiver = Alice, amount = 3)
```

Smart Contract Example: Tokens


```
owner.mint(receiver = Alice, amount = 3)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	3

Smart Contract Example: Tokens


```
Alice.send(receiver = Bob, amount = 2)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	3

Smart Contract Example: Tokens


```
Alice.send(receiver = Bob, amount = 2)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	1
3	Bob	2

Smart Contract Example: Tokens


```
Alice.vote(Action = Yes)
Bob.vote(Action = No)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	1
3	Bob	2
4		
5	Yes	1
6	No	2

Smart Contract Example: Tokens


```
Alice.lend(Amount = 0.3)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	0.7
3	Bob	2
4		
5	Alice's deposits	0.3

Smart Contract Example: Tokens


```
Alice.lend(Amount = 0.3)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	0.7
3	Bob	2
4		
5	Alice's deposits	0.3

Question: what's the difference between lent tokens and non-lent tokens?

Smart Contract Example: Tokens


```
Alice.bet(Amount = 0.4)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	0.6
3	Bob	2
4		
5	Alice's bet	0.4

Question: what's the difference between bet tokens and non-bet tokens?

A Token Contract in Solidity

```
pragma solidity ^0.5.10;

contract Token {

    address public owner;
    mapping (address => uint) public balances;

    constructor() public {
        owner = msg.sender;
    }
    // Creates an amount of new tokens and sends them to an address.
    function mint(address receiver, uint amount) public {

        // Only the contract owner can call this function
        require(msg.sender == owner, "You are not the owner.");
        // Enforces a maximum amount of tokens
        require(amount < 1e60, "Maximum issuance exceeded");
        // Increases the balance of `receiver` by `amount`
        balances[receiver] += amount;
    }

    // Sends an amount of existing tokens from any caller to an address.
    function transfer(address receiver, uint amount) public {
        // The sender must have enough tokens to send
        require(amount <= balances[msg.sender], "Insufficient balance.");

        // Adjusts token balances of the two addresses
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
}
```

Source: ETH documentation

Can Smart Contracts be Changed?

Can Smart Contracts be Changed?

- Code cannot change, but data can
- Trick: use data to reference code!
- Make a "proxy contract" A, which has "implementation" address X, and simply calls the contract at X
- If you change X, you change what A does!

Source: ETH documentation

Can Smart Contracts be Changed?

Picture: forwarding addresses

Can Smart Contracts be Changed?

Potentially important for:

- Security: can devs change code and steal my money?

Can Smart Contracts be Changed?

Potentially important for:

- Security: can devs change code and steal my money?
- Legal implications: can devs conceivably change code, hence are they responsible for behavior of code?

“Throwing Away the Keys”

```
pragma solidity ^0.5.10;

contract Token {

    address public owner;
    mapping (address => uint) public balances;

    constructor() public {
        owner = msg.sender;
    }
    // Creates an amount of new tokens and sends them to an address.
    function mint(address receiver, uint amount) public {

        // Only the contract owner can call this function
        require(msg.sender == owner, "You are not the owner.");
        // Enforces a maximum amount of tokens
        require(amount < 1e60, "Maximum issuance exceeded");
        // Increases the balance of `receiver` by `amount`
        balances[receiver] += amount;
    }

    // Sends an amount of existing tokens from any caller to an address.
    function transfer(address receiver, uint amount) public {
        // The sender must have enough tokens to send
        require(amount <= balances[msg.sender], "Insufficient balance.");

        // Adjusts token balances of the two addresses
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
}
```

Can Smart Contracts be Changed?

Takeaways:

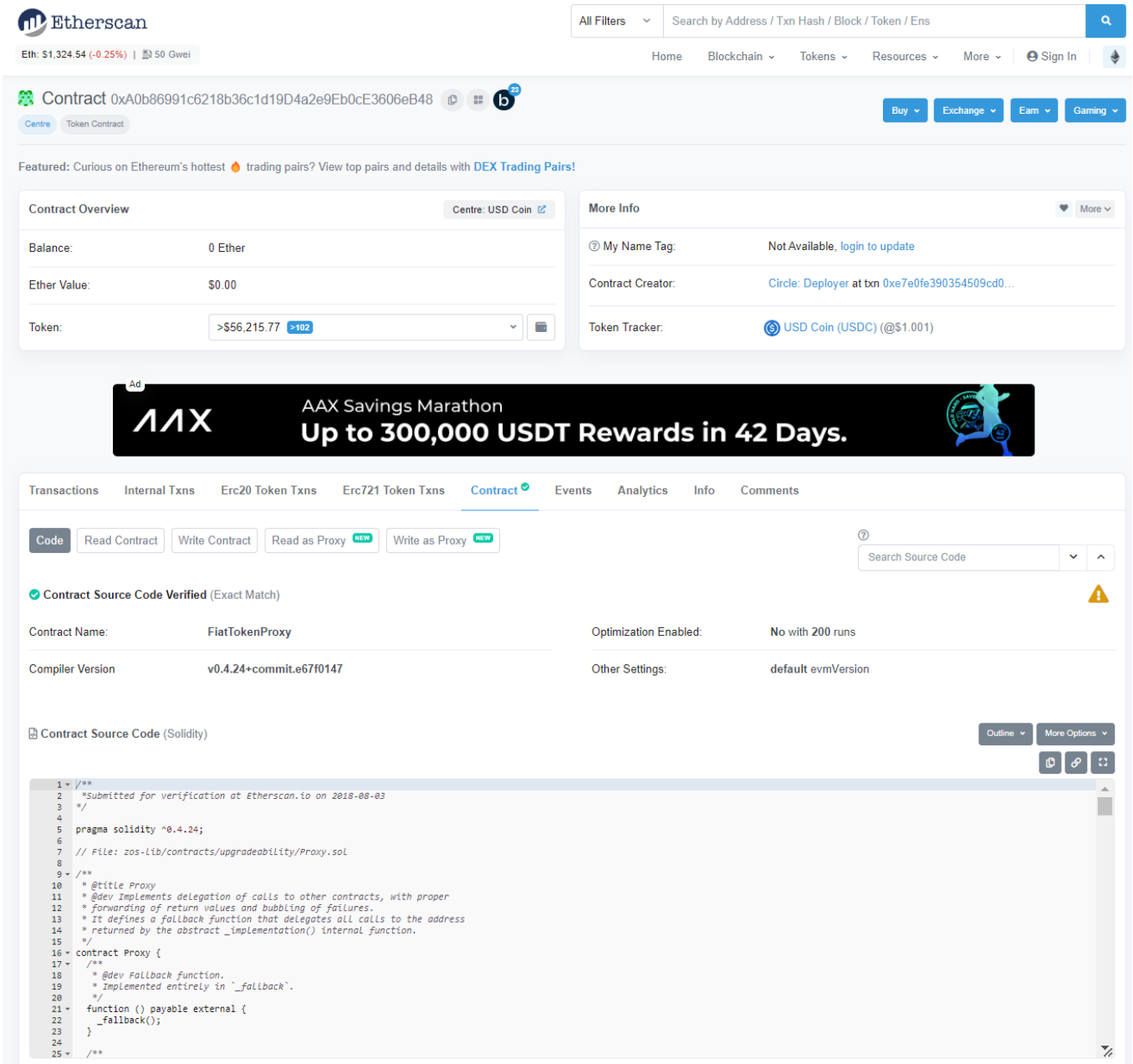
- Smart contracts can be built in a way that makes them upgradable
- But (from the code) you can tell whether a smart contract is upgradable or not
- Devs can commit not to updating a piece of code

Can you tell what the code in a smart contract is?

Can you tell what the code in a smart contract is?

- Smart contracts on ETH store a code hash of compiled EVM code
- Given Solidity code, can check whether compiled code hashes to contract address
- However, can't reverse the hash: can only verify correctness if code is submitted

Can you tell what code in a smart contract is?



Smart Contracts and Regulation

Smart Contracts and Regulation


```
pragma solidity ^0.5.10;

contract Token {

    address public owner;
    mapping (address => uint) public balances;

    constructor() public {
        owner = msg.sender;
    }
    // Creates an amount of new tokens and sends them to an address.
    function mint(address receiver, uint amount) public {

        // Only the contract owner can call this function
        require(msg.sender == owner, "You are not the owner.");
        // Enforces a maximum amount of tokens
        require(amount < 1e60, "Maximum issuance exceeded");
        // Increases the balance of `receiver` by `amount`
        balances[receiver] += amount;
    }

    // Sends an amount of existing tokens from any caller to an address.
    function transfer(address receiver, uint amount) public {
        // The sender must have enough tokens to send
        require(amount <= balances[msg.sender], "Insufficient balance.");

        // Adjusts token balances of the two addresses
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
}
```

Smart Contracts and Regulation

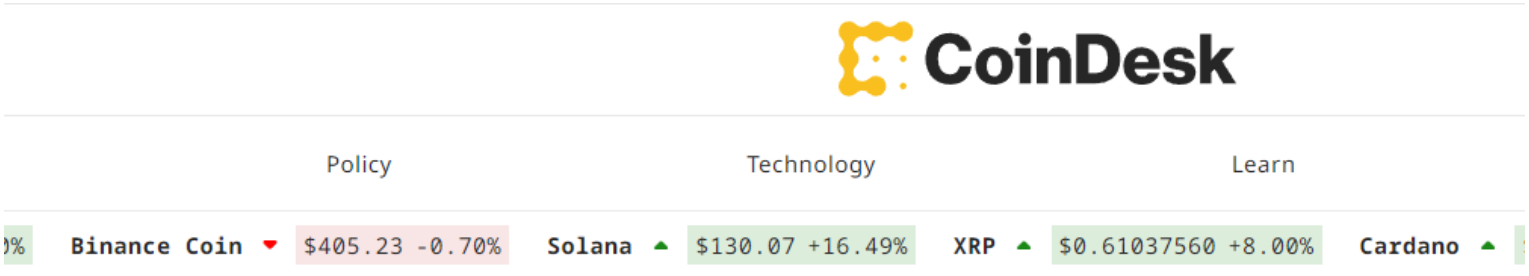
???????

Smart Contracts and Regulation

???????


```
ERROR: self.legalDefense() UNDEFINED
```

Smart Contracts and Regulation



Policy

Netherlands Arrests Suspected Developer of Sanctioned Crypto-Mixing Service Tornado Cash

The country's Fiscal Information and Investigation Service hasn't ruled out making more arrests.

HOME < NEWS < MARKETS

Crypto Exchange Uniswap Hit With Class Action Lawsuit Alleging Wrongdoing

Developers can embed a Uniswap trading window in any app with one line of code, while a class action lawsuit alleges the exchange promotes unregistered securities

BY MACAULEY PETERSON / APRIL 19, 2022 12:17 PM

Smart Contracts and Regulation

A class action lawsuit against developers and venture capital backers of decentralized digital assets exchange Uniswap alleges because the protocol allows users to freely list and trade tokens, its creators are responsible for "rampant fraud on the exchange," and it needs to register as a broker-dealer with the Financial Industry Regulatory Authority, or FINRA.

The plaintiff in the case is Nessa Risley, a North Carolina resident who claims to have purchased about $8,545 worth of obscure ERC-20 tokens via Uniswap in May and June of 2021. The suit was filed in the Southern District of New York.

"Uniswap has offered and sold unregistered securities," the lawsuit claims, and, consequently, the people who developed and funded the software that facilitates the exchange owe restitution to anyone who has ever used Uniswap.

The suit names Hayden Adams, Uniswap's creator, as a defendant, along with Universal Navigation Inc., formerly known as Uniswap LLC, the company he founded. Other defendants are venture capital firms Paradigm, Andreessen Horowitz and Union Square Ventures.

Smart Contracts and Regulation

A class action complaint against Uniswap was tossed on Tuesday, Aug. 29 after the judge found that some of the claims were "devoid of factual support."

Judge Katherine Polk Failla oversaw the case — she is also overseeing the US Securities and Exchange Commission's case against Coinbase — and issued the ruling on the dismissal.

"Due to the Protocol's decentralized nature, the identities of the Scam Token issuers are basically unknown and unknowable, leaving Plaintiffs with an identifiable injury but no identifiable defendant," the judge wrote.

Read more: SEC sues Coinbase for alleged securities violations

She added that the plaintiffs launched the suit "hoping that this Court might overlook the fact that the current state of cryptocurrency regulation leaves them without recourse." But that does not allow them to blame Uniswap for their injury.

How Do We Stop Smart Contracts?

- How to ensure:
  - Programs don't run for too long, getting miners stuck?
  - Programs don't use too much storage, running miners out of "hard drive" space?

How Do We Stop Smart Contracts?

- How to ensure:
  - Programs don't run for too long, getting miners stuck?
  - Programs don't use too much storage, running miners out of "hard drive" space?
- Basic idea: charge people for resources they use
- Next, we'll talk about gas

Compiled Code

THE EVM

For the EVM to be able to run your contract it needs to be in **bytecode**. Compilation turns this:

Show less | Copy

```
pragma solidity 0.4.24;

contract Greeter {

    function greet() public constant returns (string) {
        return "Hello";
    }

}

```

into this

```
PUSH1 0x80 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH2 0x41
```

What if we do this?

```
1
2 while(1 = 1) {
3     return "Round and round...";
4 }
5
6 for(i in 1:100000000) {
7     a[i] = 1;
8 }
9
```

Pricing Scarce Computation Resources (Pre-London)

- When you run smart contract code, every ETH miner has to run it!
- When you edit smart contract data, every ETH miner has to store it!

Pricing Scarce Computation Resources (Pre-London)

- When you run smart contract code, every ETH miner has to run it!
- When you edit smart contract data, every ETH miner has to store it!
- Core idea: users pay for the computation + storage resources they use, using ETH
- "Computational resources" used by a function call measured in units of "gas"

Pricing Scarce Computation Resources (Pre-London)

- When you run smart contract code, every ETH miner has to run it!
- When you edit smart contract data, every ETH miner has to store it!
- Core idea: users pay for the computation + storage resources they use, using ETH
- "Computational resources" used by a function call measured in units of "gas"
- Often unclear how much gas a transaction will take. . . ("halting problem")
- Tx's specify "gas limit": once exceeded, TX fails (but still put into chain!)
- Tx's specify "gas price" per unit gas, paid to miners: previously, miners incentivized to include tx's with highest gas price

Gas Tables

THE EVM

For the EVM to be able to run your contract it needs to be in **bytecode**. Compilation turns this:

Show less Copy

```
pragma solidity 0.4.24;

contract Greeter {

    function greet() public constant returns (string) {
        return "Hello";
    }

}

```

into this

```
PUSH1 0x80 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH2 0x41
```

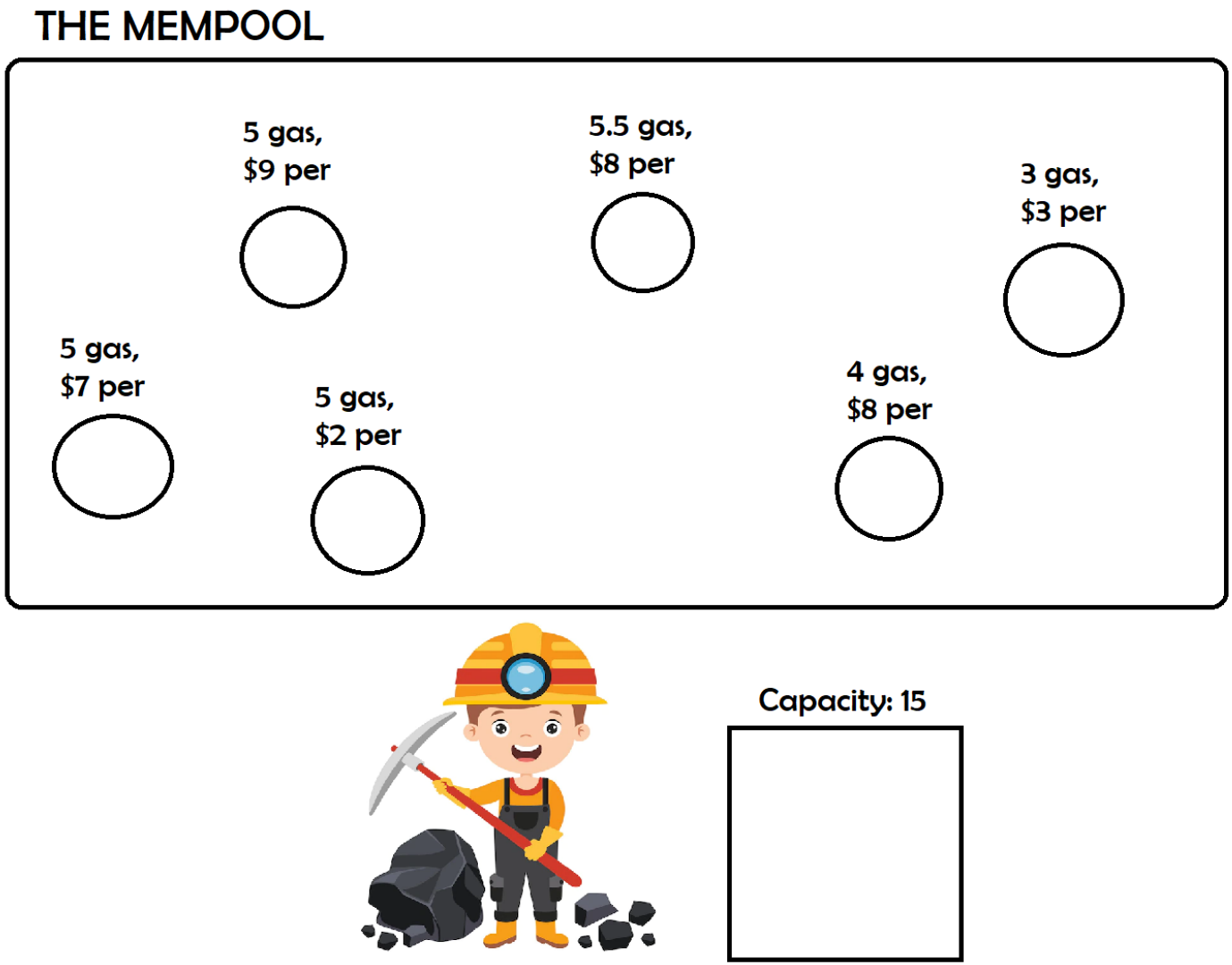
Source

Gas Tables

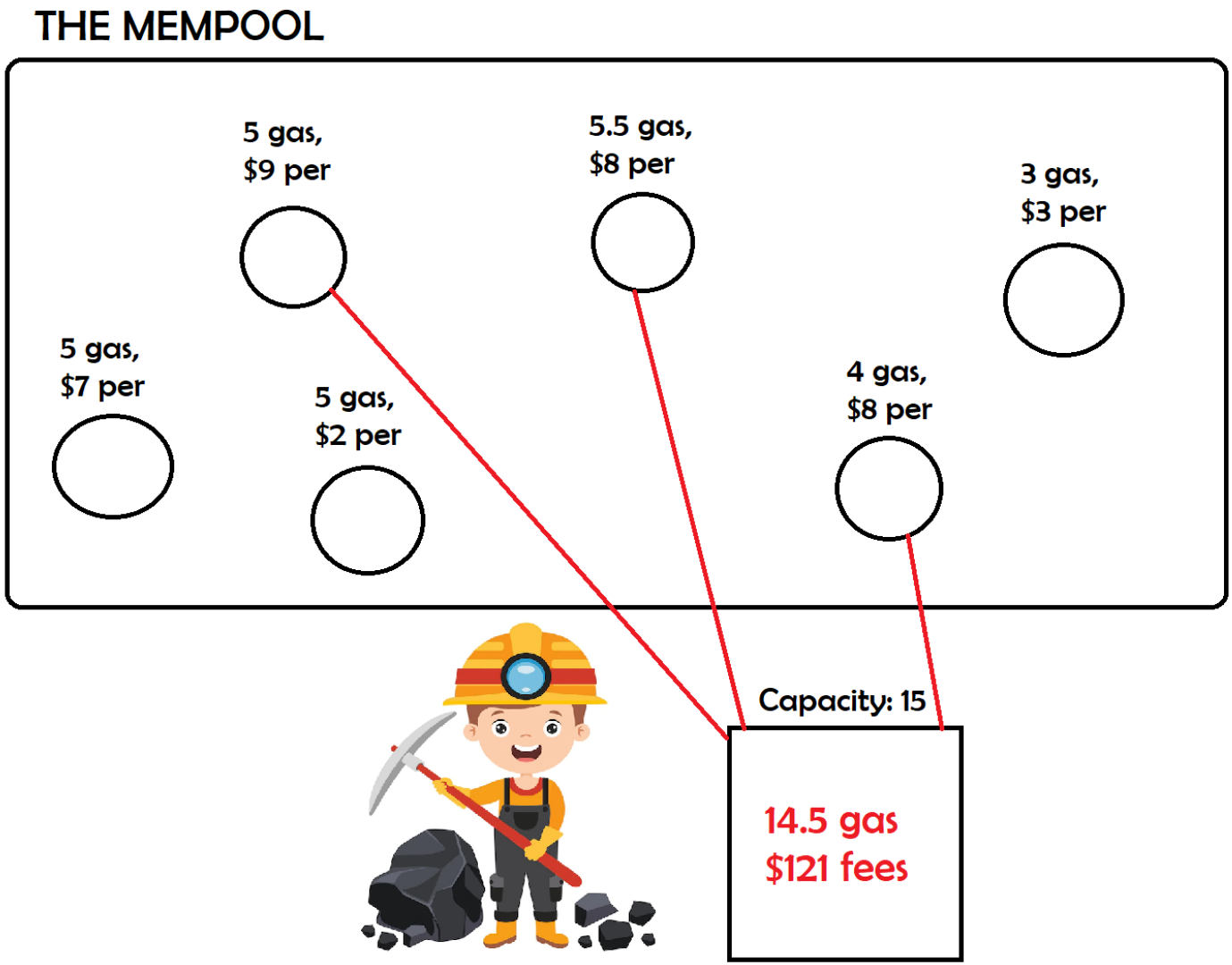
Stack	Name	Gas	Initial Stack	Resulting Stack
00	STOP	0		
01	ADD	3	a, b	a + b
02	MUL	5	a, b	a * b
03	SUB	3	a, b	a - b
04	DIV	5	a, b	a // b
05	SDIV	5	a, b	a // b
06	MOD	5	a, b	a % b
07	SMOD	5	a, b	a % b
08	ADDMOD	8	a, b, N	(a + b) % N
09	MULMOD	8	a, b, N	(a * b) % N
0A	EXP	A1↗	a, b	a ** b
0B	SIGNEXTEND	5	b, x	SIGNEXTEND(x, b)
0C-0F	*invalid*			
10	LT	3	a, b	a < b
11	GT	3	a, b	a > b
12	SLT	3	a, b	a < b
13	SGT	3	a, b	a > b
14	EQ	3	a, b	a == b
15	ISZERO	3	a	a == 0

Source

Gas and Miners



Gas and Miners



London, EIP-1559

- Under original gas system, hard to predict gas prices! Need to check "market clearing price" in mempool at any time
- In Aug 2021 "London" Ethereum update, gas system revised:
  - "Base fee" adjusted through continuous auction, burned instead of paid to miners
  - "Priority fee" paid to miners
- "Base fee" makes it easier to predict cost of a tx
- For regular users, doesn't make a huge difference

Gas Fees and Smart Contracts

- BB's actions may cost ETH miners compute + storage. But BB is a bot!
- BB only does things when human wallets ask it to...

Gas Fees and Smart Contracts

- BB's actions may cost ETH miners compute + storage. But BB is a bot!
- BB only does things when human wallets ask it to...
- ...So BB does what it's asked, then sends you a gas bill
- Human using BB has to pay for computation + data BB uses

Gas

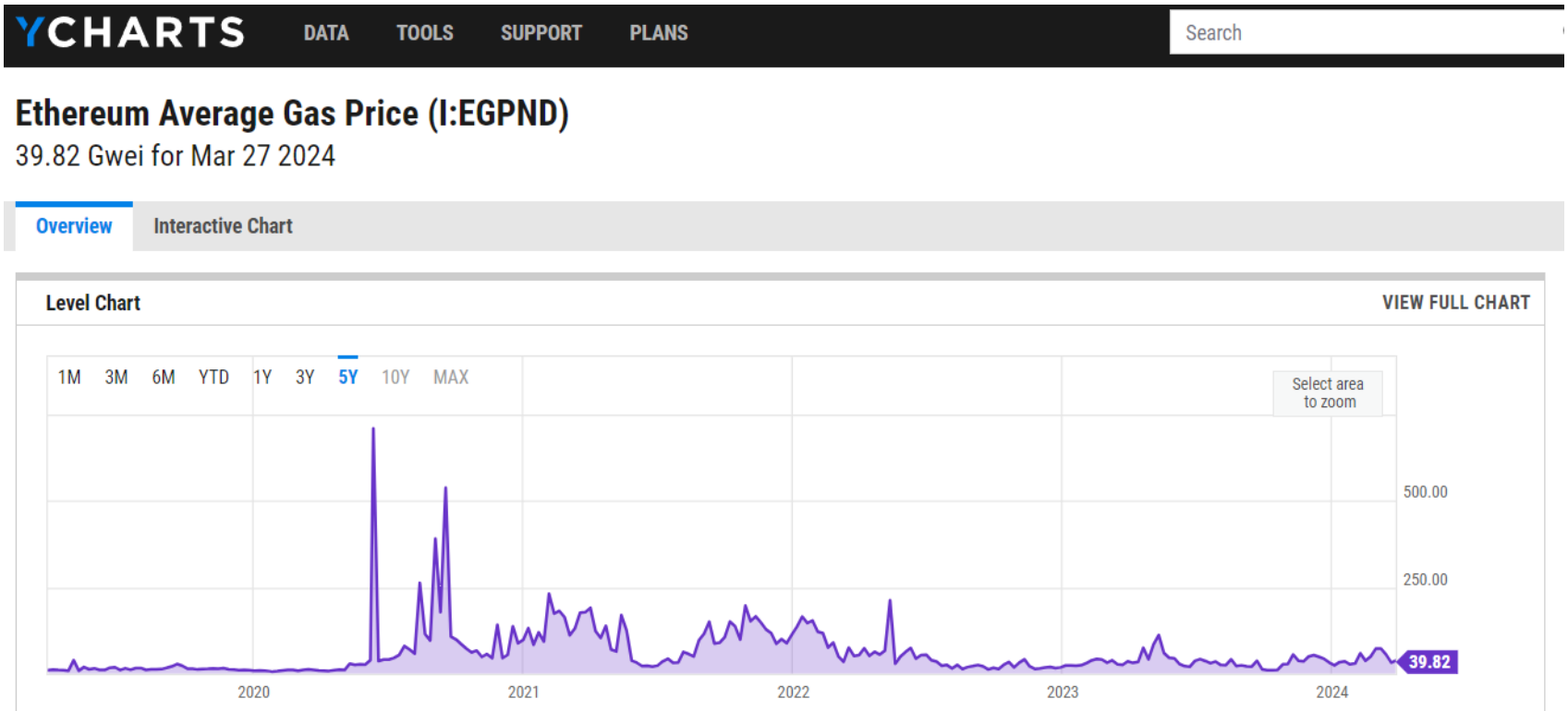

```
Alice.send(receiver = Bob, amount = 2)
```

	A	B
1	Name	ALZcoin Balance
2	Alice	1
3	Bob	2

Question: are gas fees for `Alice.send()` different if Bob holds ALZcoin?

Thanks Twitter for helping me with this question

Gas Prices Over Time



Source

Gas Prices and Transaction Demand

COINTELEGRAPH
The future of money

BTC	ETH	BNB	SOL
$19,116	$1,290	$282	$32
-1.12%	-2.45%	+0.12%	-2.18%

News Markets Magazine People Cryptopedia Research Video

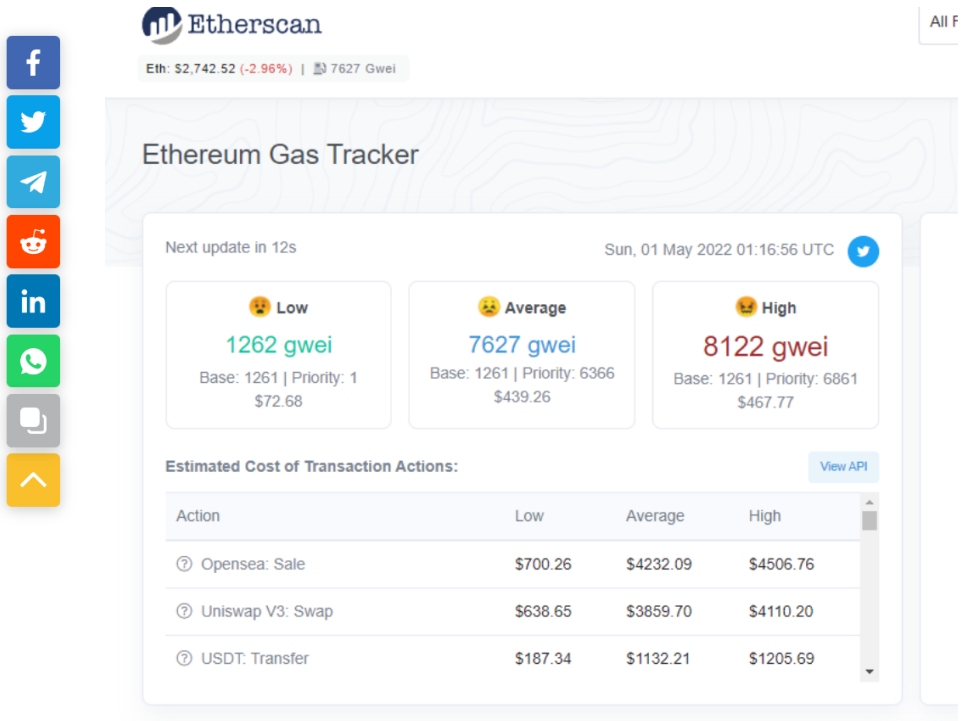
ARIJIT SARKAR

MAY 01, 2022

ETH gas price surges as Yuga Labs cashes in $300M selling Otherside NFTs

While the Otherdeed NFTs could be minted only in APE, it also required ETH for gas fees.

Gas Prices and Transaction Demand

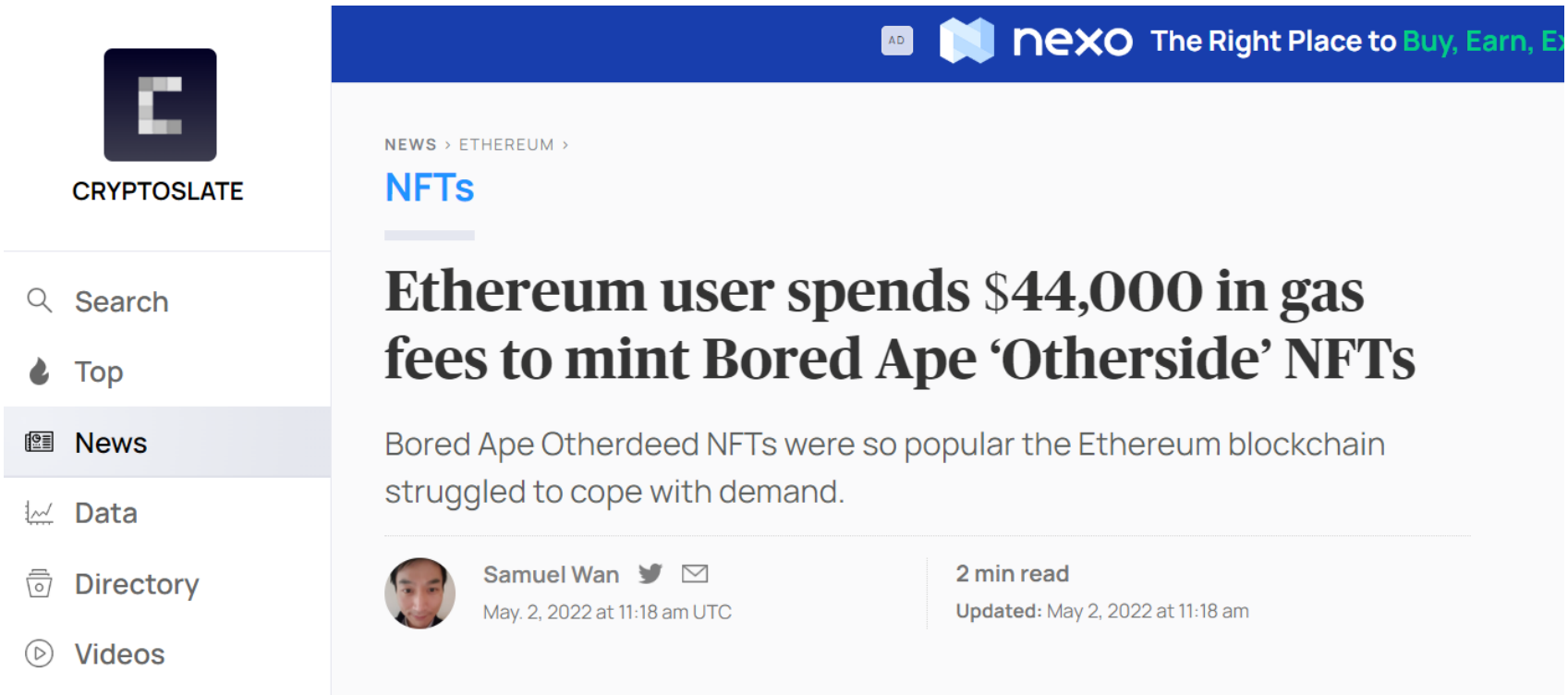


Ethereum gas tracker. Source: Etherscan

The above screenshot was shared by Redditor u/jeux99 sharing their experience with high gas fees at the time, asking:

> **"Why is gas $450 right now??? I've seen high gas fees, but nothing like this before!"**

Gas Prices and Transaction Demand



Capacity of Ethereum

- Ethereum currently processes around 15 transactions per second
- This is pretty bad! Visa is 24,000 tps!
  - Every ETH miner has to run every transaction, and keep a copy of all data!
- Decentralization very expensive, in terms of computational efficiency!
- Proof-of-stake doesn't help throughput
- But, rollups (later in lecture) should

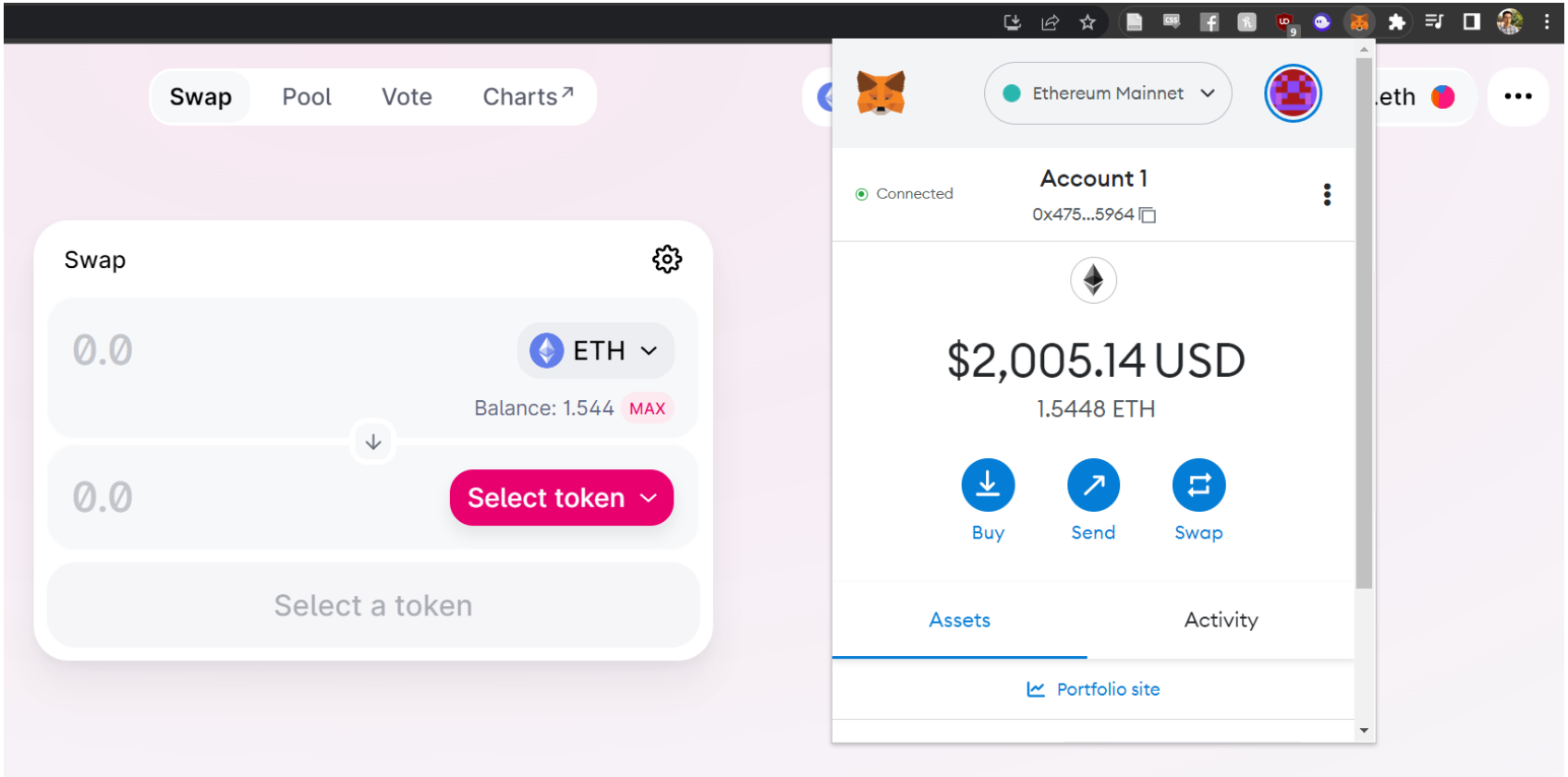
Gas Fees: Summary

- You have to pay to do stuff (sends, smart contracts, etc.) on Ethereum
- The more computation/storage you use, the more you pay
- Price depends on overall level of transaction demand
  - When network is "congested" and everyone wants to transact, gas prices high
- Next subject: the Ethereum **user interface**

User Interface

- Like Bitcoin, interact with ETH through wallet software, which helps you manage private keys, sign transactions, etc.
- By far most popular ETH wallet software is Metamask
- Metamask is set up as a browser extension
- **Warning:** there are many scammers pretending to be Metamask customer support! Just try posting "metamask" on Twitter...

Metamask


Swap
Pool
Vote
Charts
Swap
0.0
ETH
Balance: 1.544
MAX
0.0
Select token
Select a token
Ethereum Mainnet
Connected
Account 1
0x475...5964
$2,005.14 USD
1.5448 ETH
Buy
Send
Swap
Assets
Activity
Portfolio site

Metamask: Private Keys

BIP39 Mnemonic

utility dove tragic roast sleep split alley doll uniform syrup jacket bleak

☐ Show split mnemonic cards

BIP39 Passphrase (optional)

BIP39 Seed

299b025ee28d80c171e46ba746d81e3ed71ce667e791f3182fdea01ebac52c35edcf116120611b3170521bef40cfd223b8d5478f1a97162d769ea23965bd6ff2

Coin

BTC - Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3eMg7utUFGVqz5H2wr61J523iPc2Kp1365DkHepG3XVDHKKGjp4T5bkRxEp3142axkfDo4iPUwCbnvhUZkexZXRRnP51qXD

Rule Number 1 of Blockchain Security

Rule Number 1 of Blockchain Security

Never,

Rule Number 1 of Blockchain Security

Never,
Never,

Rule Number 1 of Blockchain Security

Never,
Never,
Never,

Rule Number 1 of Blockchain Security

Never,
Never,
Never,
Never,

Rule Number 1 of Blockchain Security

Never,
Never,
Never,
Never,
Never give out your seed phrase!

Shamir's Secret Sharing Scheme

Shamir's Secret Sharing Scheme

See here

Hardware Wallets

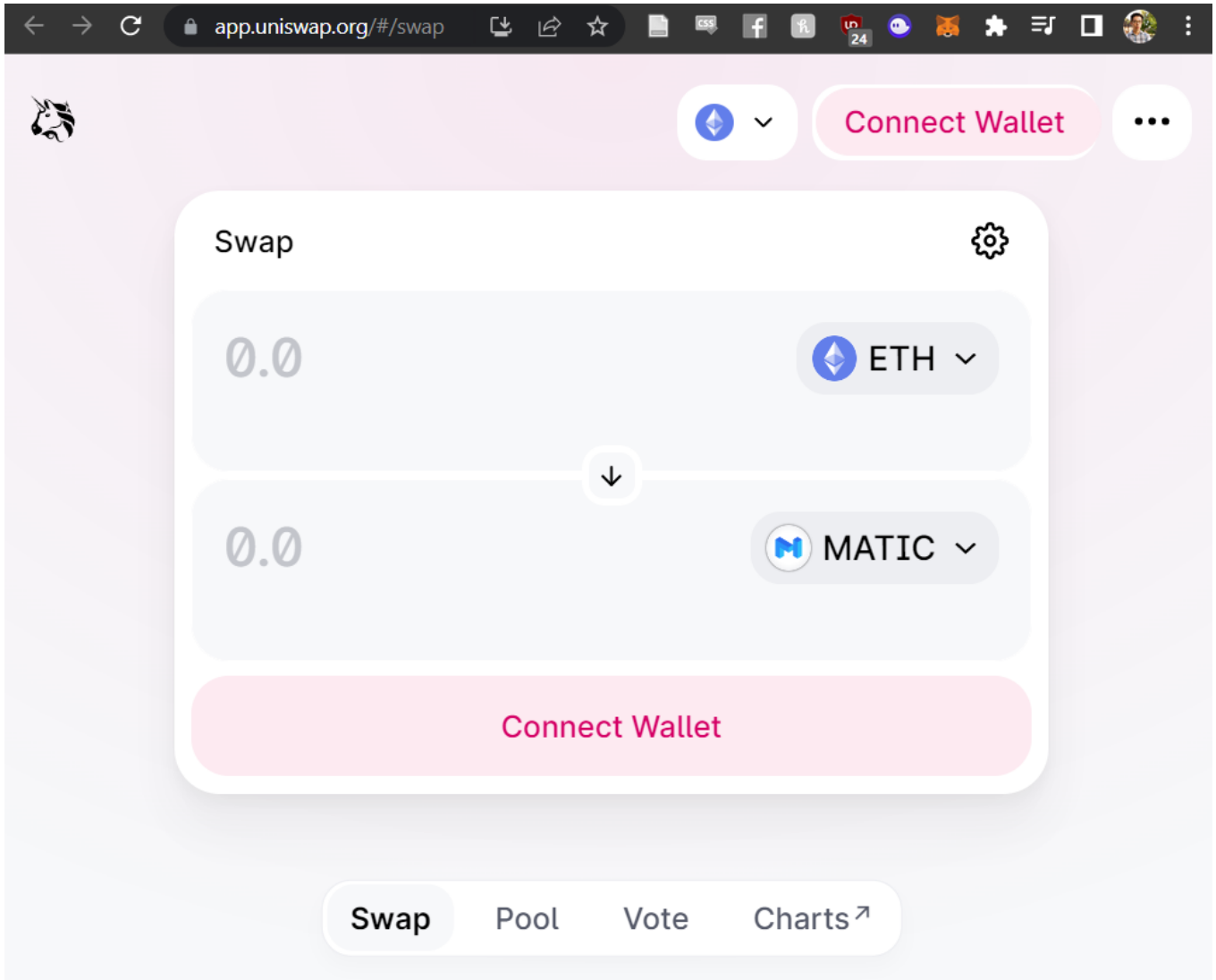
- For better security, use a hardware wallet
- Popular brands include Trezor and Ledger
  - Common sense: don't buy used! Closed-box from a reputable merchant, and if you're paranoid, reset firmware before using
- If you give away your seed phrase you still lose!

Hardware Wallets

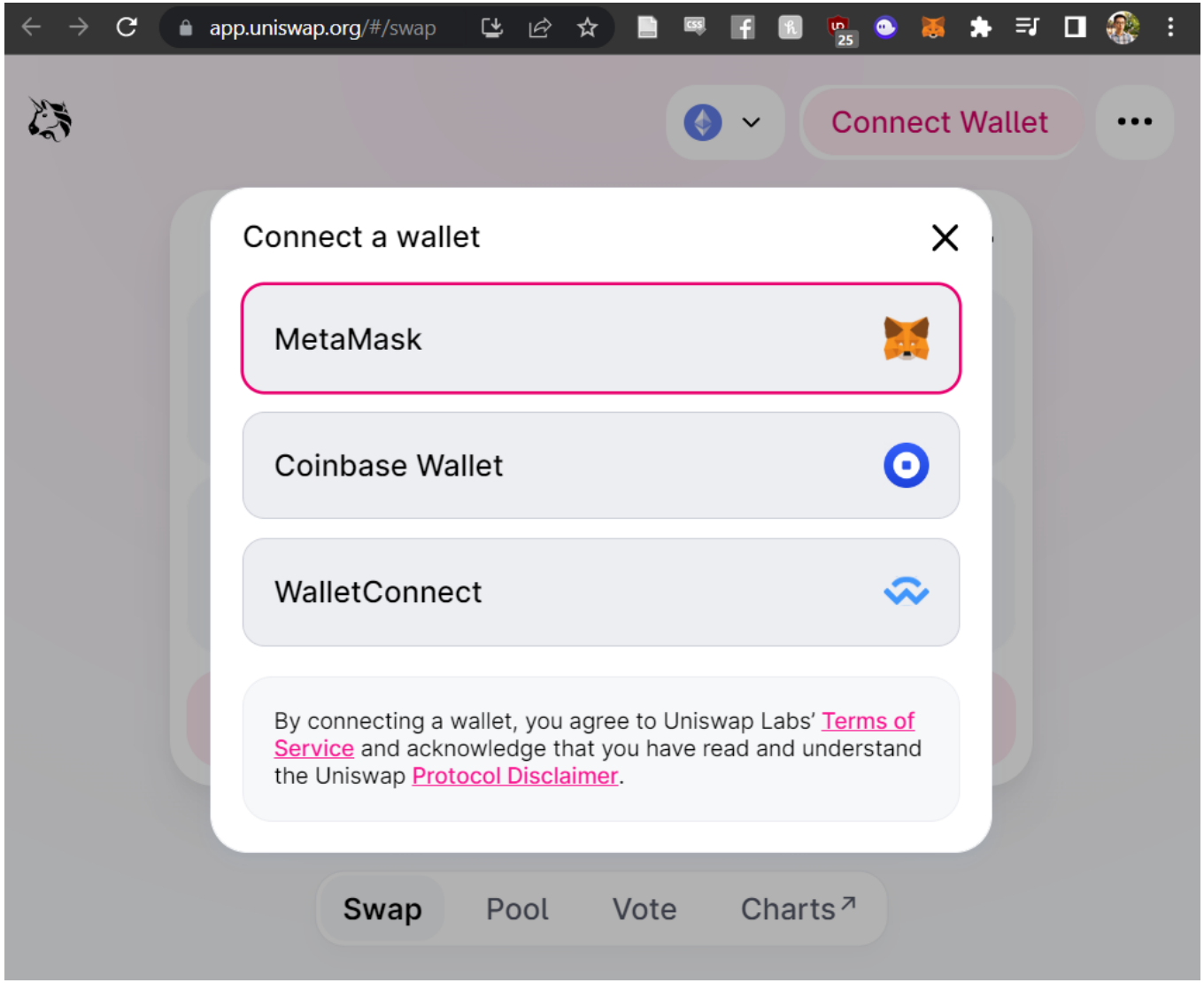
- For better security, use a hardware wallet
- Popular brands include Trezor and Ledger
  - Common sense: don't buy used! Closed-box from a reputable merchant, and if you're paranoid, reset firmware before using
- If you give away your seed phrase you still lose!
- Moral of story: be careful with your crypto!

Metamask: Funds Sending Example

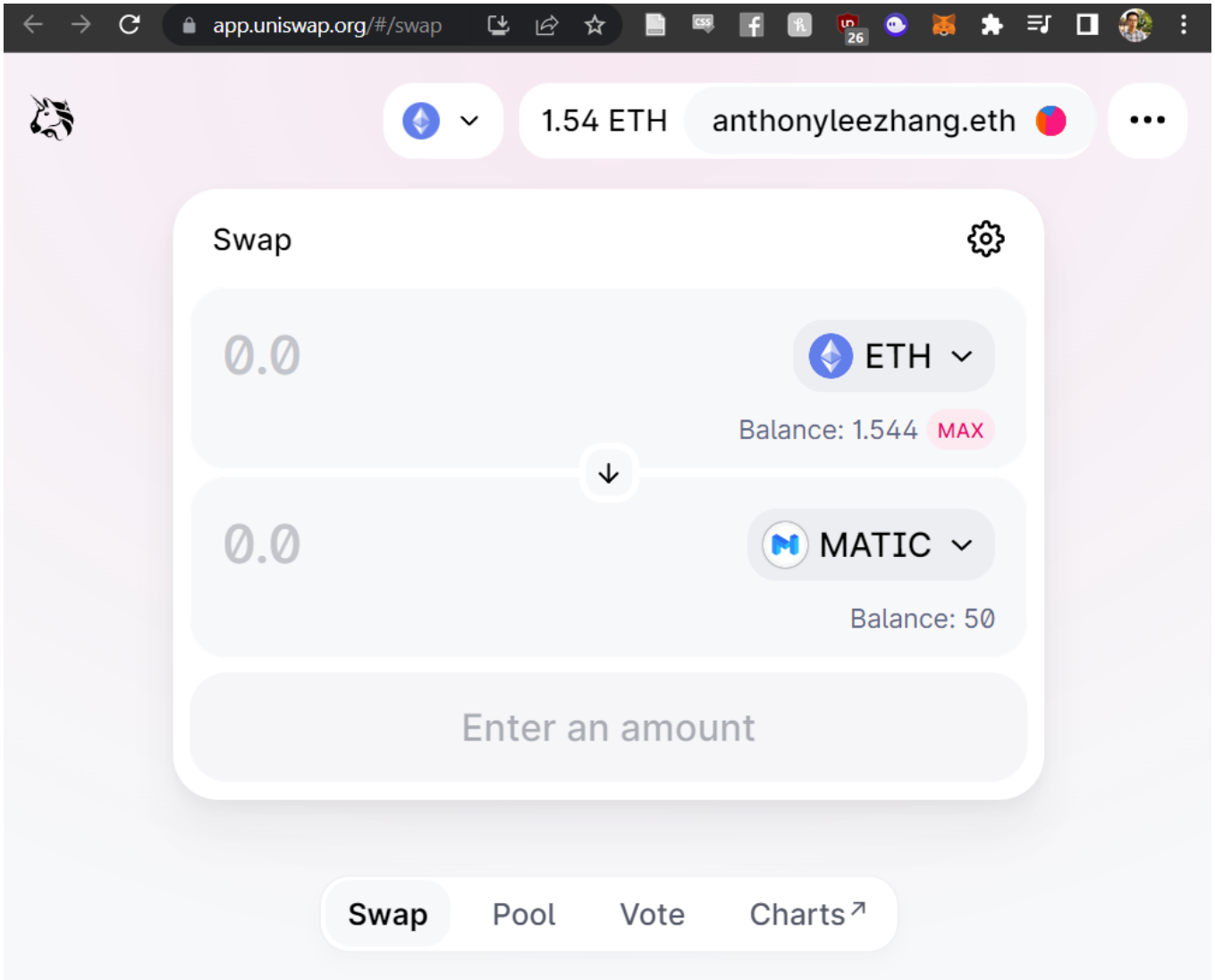
Uniswap Example



Uniswap Example



Uniswap Example



Cookies

- Why does it make sense to set up a wallet as a browser extension?
- Cookies are bits of data stored in your computer by websites, to remember "state"
  - How do websites "remember" you logged in?
  - Settings (dark mode, font size)?

Cookies

- Why does it make sense to set up a wallet as a browser extension?
- Cookies are bits of data stored in your computer by websites, to remember "state"
  - How do websites "remember" you logged in?
  - Settings (dark mode, font size)?
- But since cookies are local, you can manipulate them!
  - Clear cookies
  - "Fake" cookies

Super Cookies!

- Your blockchain wallet has a bunch of data (ETH balance, ERC20 tokens, NFTs...)
- When you connect wallet to a website, it can see all the data

Super Cookies!

- Your blockchain wallet has a bunch of data (ETH balance, ERC20 tokens, NFTs. . .)
- When you connect wallet to a website, it can see all the data
- Stored publicly on ETH blockchain – you can't fake it!

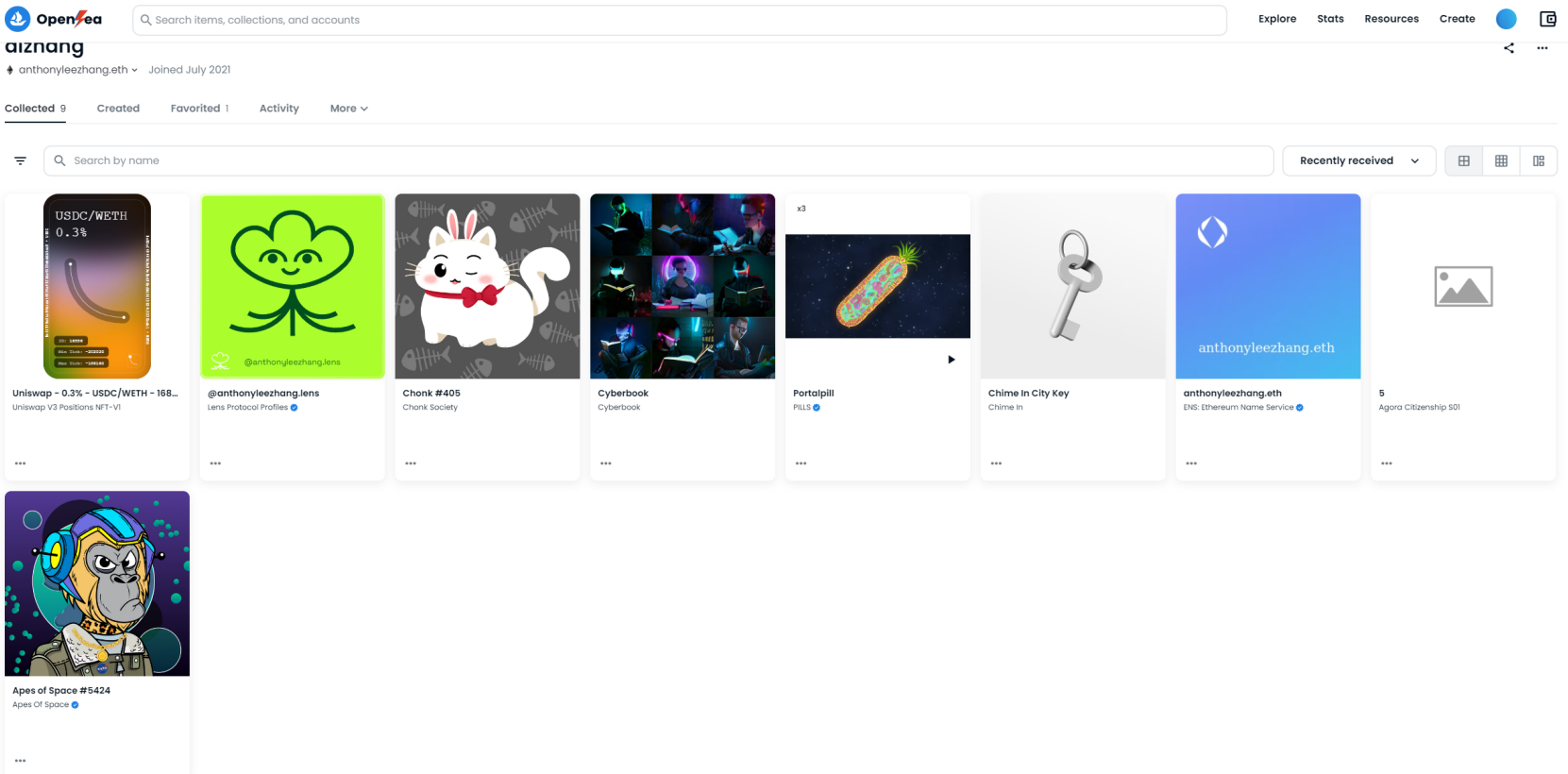
Super Cookies!

- Your blockchain wallet has a bunch of data (ETH balance, ERC20 tokens, NFTs. . .)
- When you connect wallet to a website, it can see all the data
- Stored publicly on ETH blockchain – you can't fake it!
- Blockchain tokens are "super cookies"
- When you log in to a dapp frontend with your wallet, you give it access to your super cookies

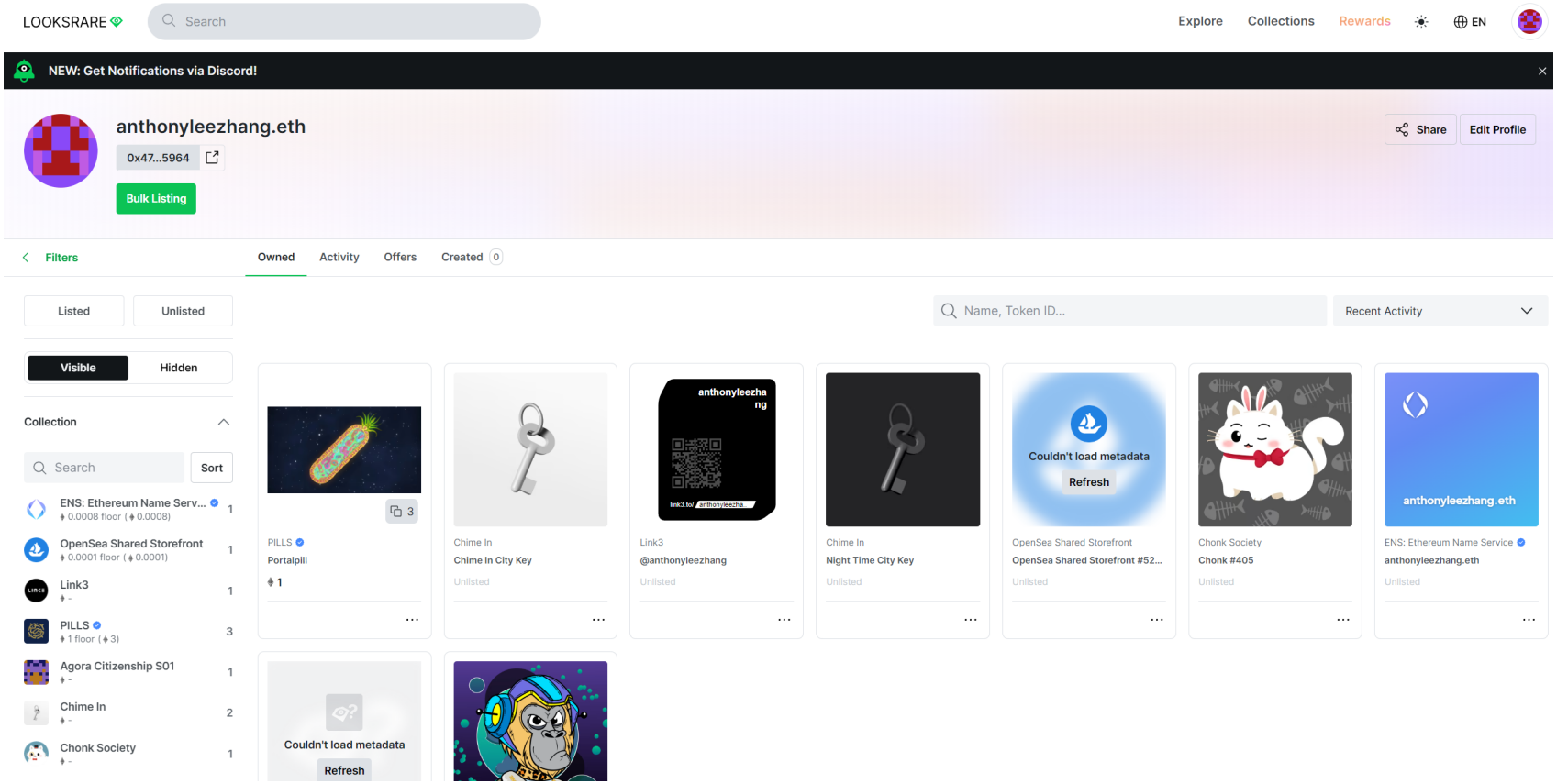
Super Cookies!

- Your blockchain wallet has a bunch of data (ETH balance, ERC20 tokens, NFTs...)
- When you connect wallet to a website, it can see all the data
- Stored publicly on ETH blockchain – you can't fake it!
- Blockchain tokens are "super cookies"
- When you log in to a dapp frontend with your wallet, you give it access to your super cookies
- Decentralized applications are fundamentally code on the blockchain...
- The "super cookie" design mentality facilitates creating nice frontends representing your wallet's interaction with the code

Super Cookies!



Super Cookies!



Native Composability

- Super cookies give us native composability
- In web2, app functions and data are closed by default
  - FB, Goog, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so

Native Composability

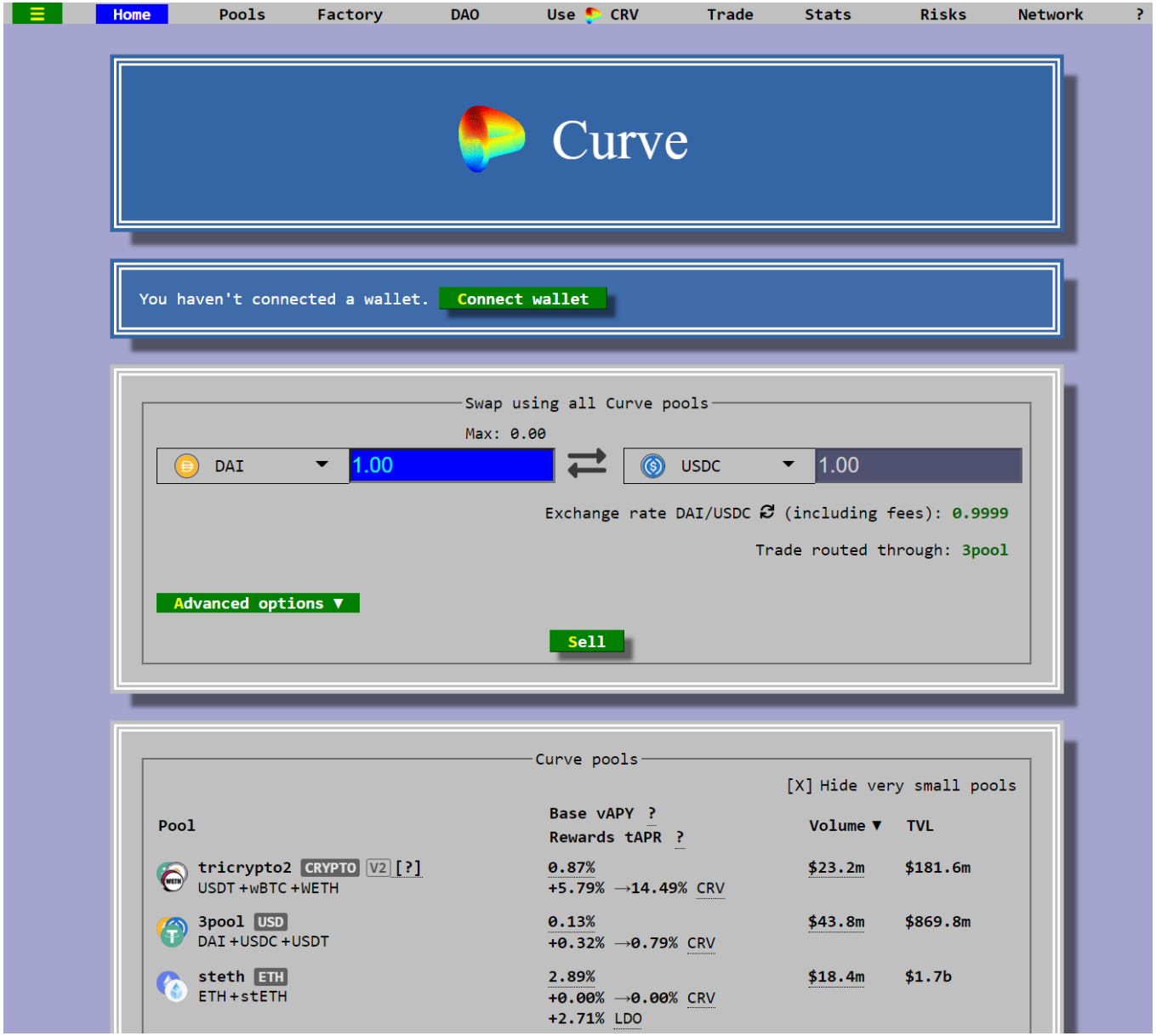
- Super cookies give us native composability
- In web2, app functions and data are closed by default
  - FB, Goog, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so
- In web3, app functions + data are open by default!
  - Very hard for Uniswap to "stop" your app from calling Uniswap functions!
  - All data is on chain: everyone can see every app's data!
  - Will be important for "vampire attacks" in tokenomics lecture in a few weeks

Native Composability

- Super cookies give us native composability
- In web2, app functions and data are closed by default
  - FB, Goog, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so
- In web3, app functions + data are open by default!
  - Very hard for Uniswap to "stop" your app from calling Uniswap functions!
  - All data is on chain: everyone can see every app's data!
  - Will be important for "vampire attacks" in tokenomics lecture in a few weeks
- Harder to construct "walled garden ecosystems", lower barriers to entry + less incumbent advantage

See "Appendix: Composability" in Saffron Huang's post here

There's a Long Way to Go...



Project Ideas: User Interfaces, User Experiences

Still very early – this stuff is too nerdy for 99% of humankind!

- Being (on average) closer to the 99%, you have a comparative advantage over the engineers
- UI/UX design is not just "pretty pictures and buttons"!
- How can UIs be made more understandable and secure?
  - What data to display? Users shouldn't have to worry about low-level details of mining, blocks...
  - Better contact books? DNS? Nobody wants to work with these: 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045
  - Auto, ML-based security/bug checks? "Big number" checks? "Approval windows?"
  - Examples: Exponential, Sequence, Zypsy, and others
- UIs currently very desktop-focused
  - Mobile-native? See Solana phone
  - What new applications are enabled by mobile-native web3?

Project Ideas: User Interfaces, User Experiences

Still very early – this stuff is too nerdy for 99% of humankind!

- Being (on average) closer to the 99%, you have a comparative advantage over the engineers
- UI/UX design is not just "pretty pictures and buttons"!
- How can UIs be made more understandable and secure?
  - What data to display? Users shouldn't have to worry about low-level details of mining, blocks...
  - Better contact books? DNS? Nobody wants to work with these: 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045
  - Auto, ML-based security/bug checks? "Big number" checks? "Approval windows?"
  - Examples: Exponential, Sequence, Zypsy, and others
- UIs currently very desktop-focused
  - Mobile-native? See Solana phone
  - What new applications are enabled by mobile-native web3?
- Expect future UIs to look very different from current ones
  - Ender's game: "the enemy's gate is down"


Paul Graham
@paulg
These early railway carriages are a good illustration of how much old stuff gets dragged along into the first versions of new things. At first even the inventors of trains couldn't think of them as more than sequences of linked horse carriages.

Web3 Identity

- What's in a physical wallet?
  - Cash, credit cards, and identity cards!
- An ID card is an item which:
  - Proves who you are (student, gym member...)
  - Gives you certain rights (discounted tickets, gym access...)
- ID cards are not transferrable!
- We can create web3 ID cards through non-transferable tokens
- May 2022 Weyl-Ohlhaver-Buterin paper: soulbound tokens as the basis of web3 identity

Project Ideas: SBTs and Web3 Identity

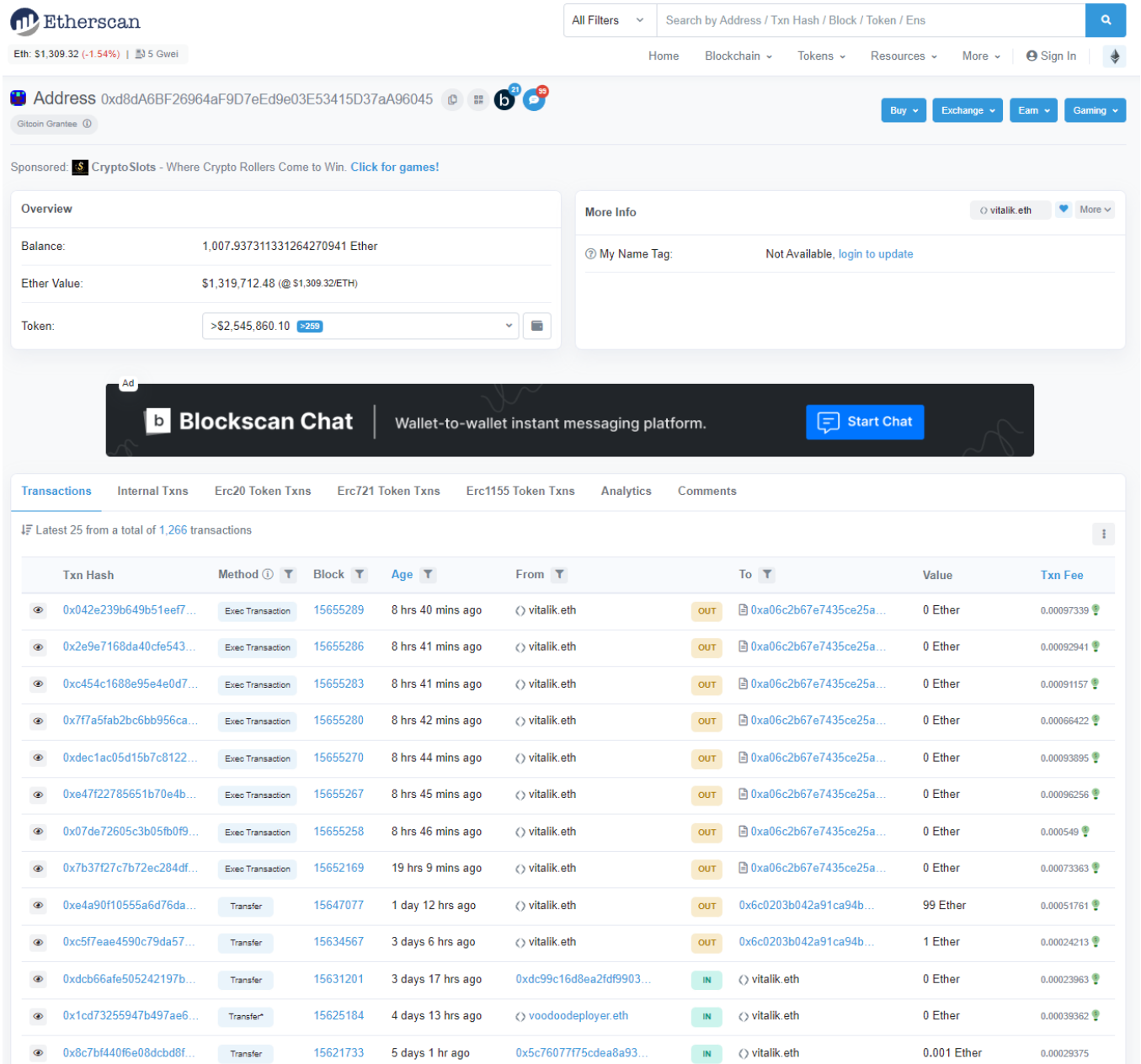
Identity very young, essentially no apps yet, so a good area for class projects! Many taken from WOB paper

- What are good SBT use cases?
  - Diplomas? Employment history?
  - "Social credit scoring"? Rewards for good deeds?
  - Some examples: Otterspace, Disco.xyz, Lens, and others
- How should SBTs work?
  - Who gets to bestow SBTs?
  - Who gets to remove SBTs? Privacy? "Scarlet letter" SBTs?
  - How do we solve "walking away from my soul"?
- In a world where SBTs are ubiquitous, what functions are enabled that can't exist yet?
  - SBT-based uncollateralized lending?
  - SBT-ML and recommendation filtering?
  - SBT-gated social organization? Private clubs? Dating apps?
- More broadly, what are some implications of "native composability" that the world hasn't realized yet?

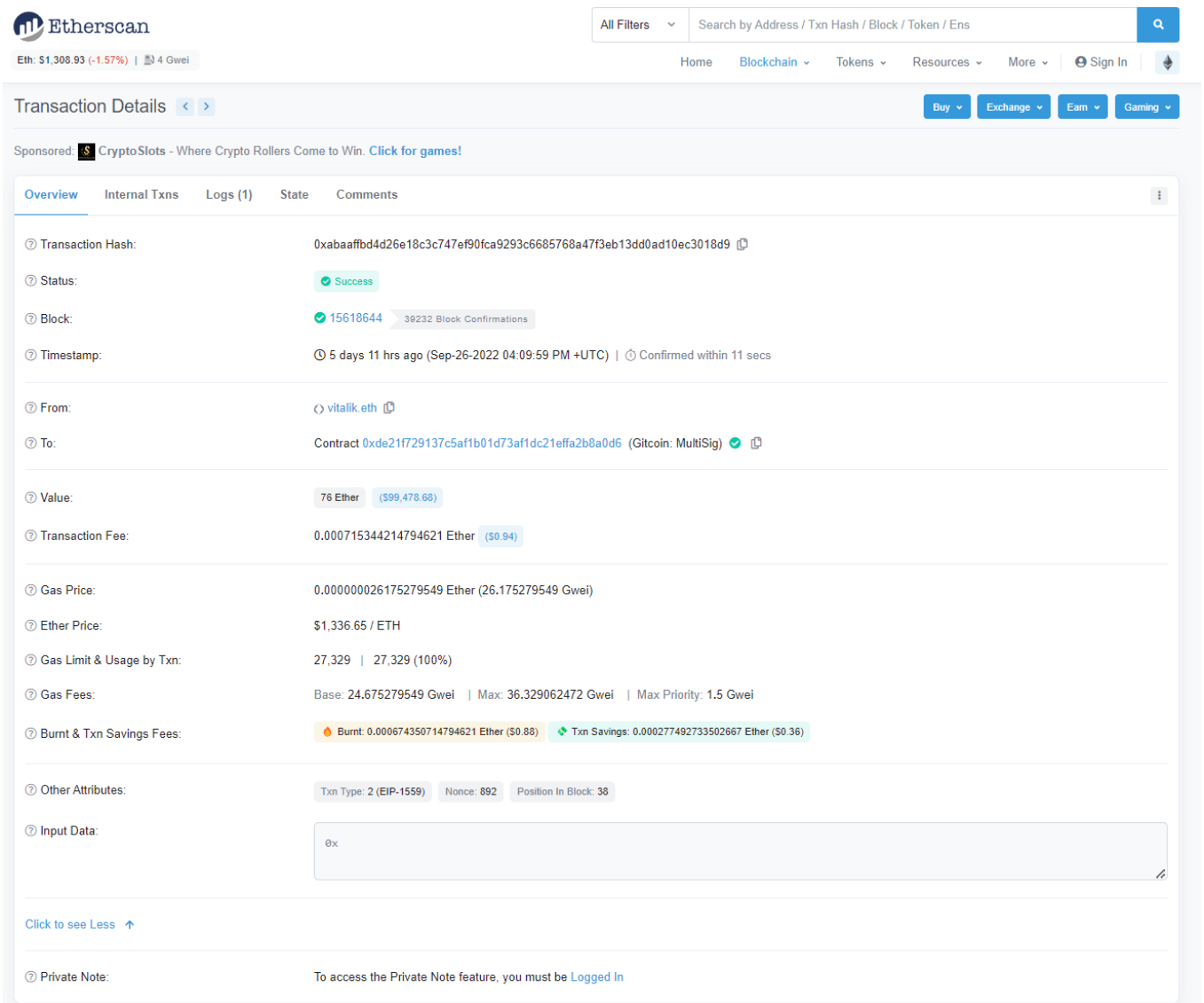
Ethereum Data

- All ETH data is public! However, quite painful to work with
- Sizable industry has emerged to organize + display ETH data

Etherscan


Etherscan
All Filters
Search by Address / Txn Hash / Block / Token / Ens
Eth: $1,309.32 (-1.54%) | 5 Gwei
Home
Blockchain
Tokens
Resources
More
Sign In
Address 0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045
Gitcoin Grantee
Buy
Exchange
Earn
Gaming
Sponsored: CryptoSlots - Where Crypto Rollers Come to Win. Click for games!
Overview
Balance: 1,007.937311331264270941 Ether
Ether Value: $1,319,712.48 (@ $1,309.32/ETH)
Token: >$2,545,860.10 >259
More Info
vitalik.eth
More
My Name Tag: Not Available, login to update
Ad
Blockscan Chat
Wallet-to-wallet instant messaging platform.
Start Chat
Transactions
Internal Txns
Erc20 Token Txns
Erc721 Token Txns
Erc1155 Token Txns
Analytics
Comments
Latest 25 from a total of 1,266 transactions
Txn Hash
Method
Block
Age
From
To
Value
Txn Fee
0x042e239b649b51eef7... Exec Transaction 15655289 8 hrs 40 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00097339
0x2e9e7168da40cfe543... Exec Transaction 15655286 8 hrs 41 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00092941
0xc454c1688e95e4e0d7... Exec Transaction 15655283 8 hrs 41 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00091157
0x7f7a5fab2bc6bb956ca... Exec Transaction 15655280 8 hrs 42 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00066422
0xdec1ac05d15b7c8122... Exec Transaction 15655270 8 hrs 44 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00093895
0xe47f22785651b70e4b... Exec Transaction 15655267 8 hrs 45 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00096256
0x07de72605c3b05fb0f9... Exec Transaction 15655258 8 hrs 46 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.000549
0x7b37f27c7b72ec284df... Exec Transaction 15652169 19 hrs 9 mins ago vitalik.eth OUT 0xa06c2b67e7435ce25a... 0 Ether 0.00073363
0xe4a90f10555a6d76da... Transfer 15647077 1 day 12 hrs ago vitalik.eth OUT 0x6c0203b042a91ca94b... 99 Ether 0.00051761
0xc5f7eae4590c79da57... Transfer 15634567 3 days 6 hrs ago vitalik.eth OUT 0x6c0203b042a91ca94b... 1 Ether 0.00024213
0xdcb66afe505242197b... Transfer 15631201 3 days 17 hrs ago 0xdc99c16d8ea2fdf9903... IN vitalik.eth 0 Ether 0.00023963
0x1cd73255947b497ae6... Transfer 15625184 4 days 13 hrs ago voodoodeployer.eth IN vitalik.eth 0 Ether 0.00039362
0x8c7bf440f6e08dcbd8f... Transfer 15621733 5 days 1 hr ago 0x5c76077f75cdea8a93... IN vitalik.eth 0.001 Ether 0.00029375

Etherscan


Etherscan
Eth: $1,308.93 (-1.57%) | 4 Gwei
All Filters
Search by Address / Txn Hash / Block / Token / Ens
Home
Blockchain
Tokens
Resources
More
Sign In
Transaction Details
Buy
Exchange
Earn
Gaming
Sponsored: CryptoSlots - Where Crypto Rollers Come to Win. Click for games!
Overview
Internal Txns
Logs (1)
State
Comments
Transaction Hash:
0xabaaffbd4d26e18c3c747ef90fca9293c6685768a47f3eb13dd0ad10ec3018d9
Status:
Success
Block:
15618644
39232 Block Confirmations
Timestamp:
5 days 11 hrs ago (Sep-26-2022 04:09:59 PM +UTC) | Confirmed within 11 secs
From:
vitalik.eth
To:
Contract 0xde21f729137c5af1b01d73af1dc21effa2b8a0d6 (Gitcoin: MultiSig)
Value:
76 Ether
($99,478.68)
Transaction Fee:
0.000715344214794621 Ether
($0.94)
Gas Price:
0.000000026175279549 Ether (26.175279549 Gwei)
Ether Price:
$1,336.65 / ETH
Gas Limit & Usage by Txn:
27,329 | 27,329 (100%)
Gas Fees:
Base: 24.675279549 Gwei | Max: 36.329062472 Gwei | Max Priority: 1.5 Gwei
Burnt & Txn Savings Fees:
Burnt: 0.000674350714794621 Ether ($0.88)
Txn Savings: 0.000277492733502667 Ether ($0.36)
Other Attributes:
Txn Type: 2 (EIP-1559)
Nonce: 892
Position In Block: 38
Input Data:
0x
Click to see Less
Private Note:
To access the Private Note feature, you must be Logged In

Dune

Search... Discover Favorites My Creations ••• Dune We're hiring! × Docs Discord Community New Query Sign in

@datanut / Aave, MakerDAO, & Compound Finance - Deposits, Loans, LTV 352 ☆ Share

#Aave #MakerDao #Compound #Compound Finance #makerdao #aave #AAVE #MKR #COMP #aave #mkr #comp #LTV #loan to value #deposits #loans #DeFi #defi #Defi #amm #AMM #vs #versus

FYSA: The queries are not pulling correct information for Aave

Deposited and Loaned-out — Aave, MakerDAO, & Compound Finance

Aave Deposits & Outstanding Loans Timeseries

@datanut

Aave V2 timeseries of total deposits & outstanding loans in USD

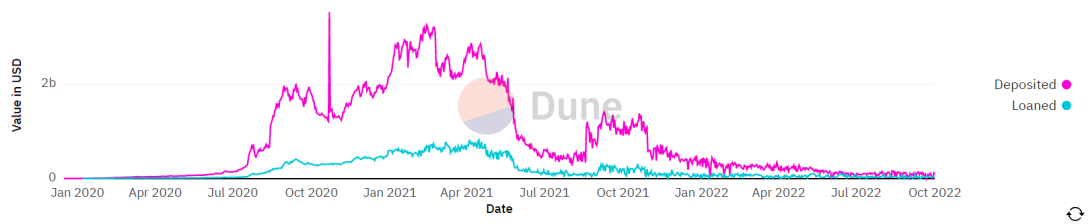
Day	Deposited	Loaned
2022-10-01 00:00	$88,048,258	$26,211,357
2022-09-30 00:00	$114,994,106	
2022-09-29 00:00	$29,102,718	
2022-09-28 00:00	-$401,182	$51,441,253
2022-09-27 00:00	$59,327,721	$25,971,195

1,001 rows « ‹ Page 1 › »

Aave Deposits & Outstanding Loans Timeseries

@datanut

Aave V2 timeseries of total deposits & outstanding loans in USD



MakerDAO Deposits & Outstanding Loans - Last 12 Months

@datanut

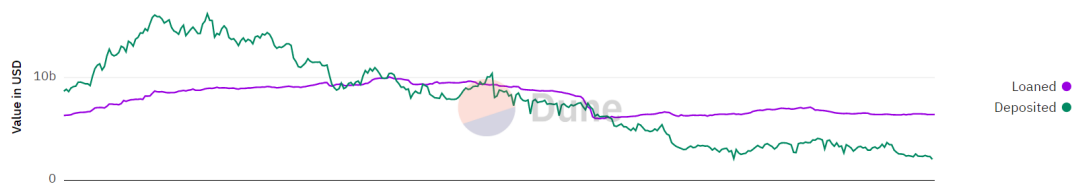
Visualization of MakerDAO deposits and outstanding loans over the last year

Day	Protocol	Loaned	Deposited
2021-10-02 00:00	MakerDAO	$ 6,318,783,239	$ 8,672,840,061
2021-10-03 00:00	MakerDAO	$ 6,341,056,270	$ 8,870,685,493
2021-10-04 00:00	MakerDAO	$ 6,356,128,722	$ 8,641,122,424
2021-10-05 00:00	MakerDAO	$ 6,386,710,879	$ 8,993,018,165

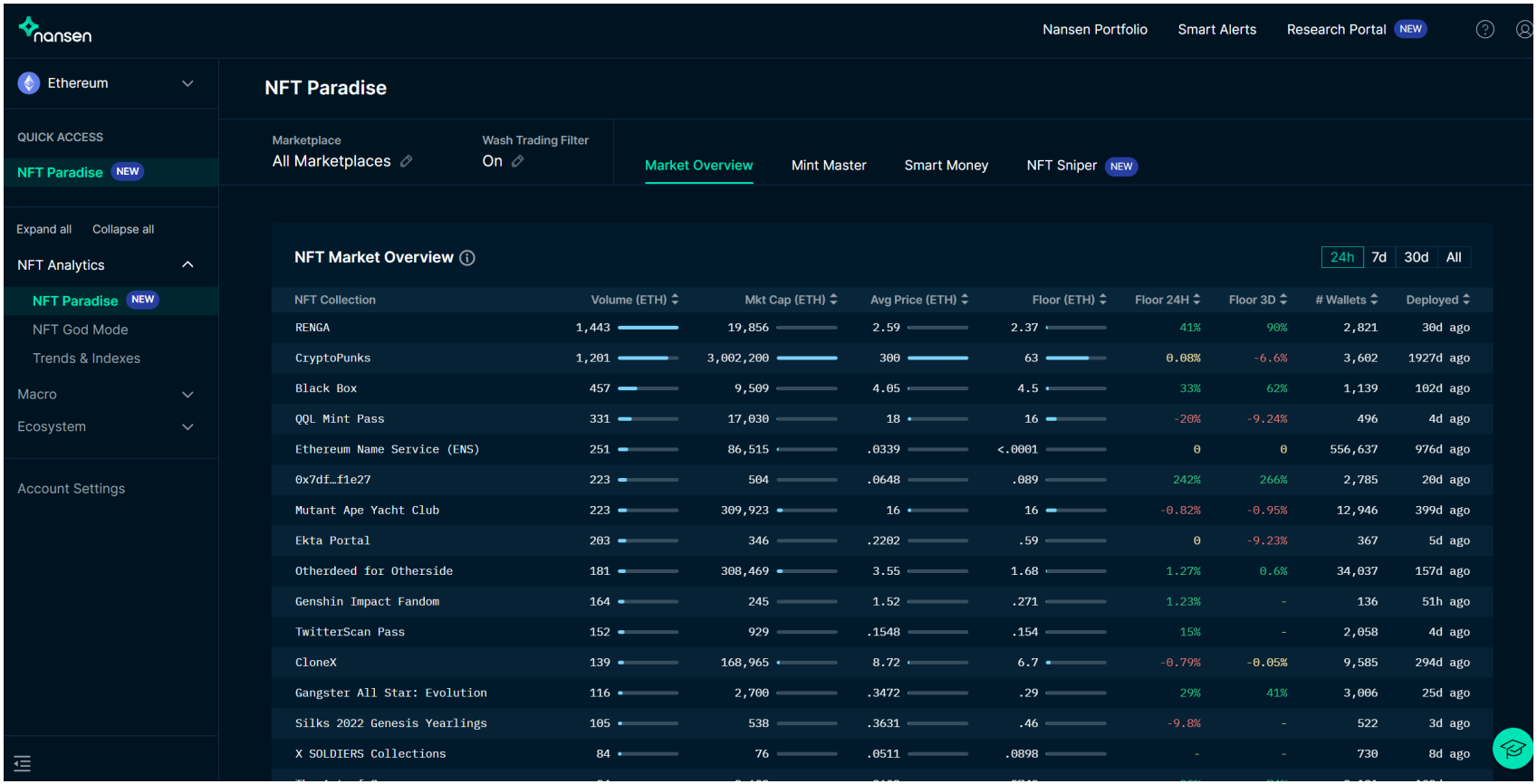
MakerDAO Deposits & Outstanding Loans - Last 12 Months

@datanut

Visualization of MakerDAO deposits and outstanding loans over the last year

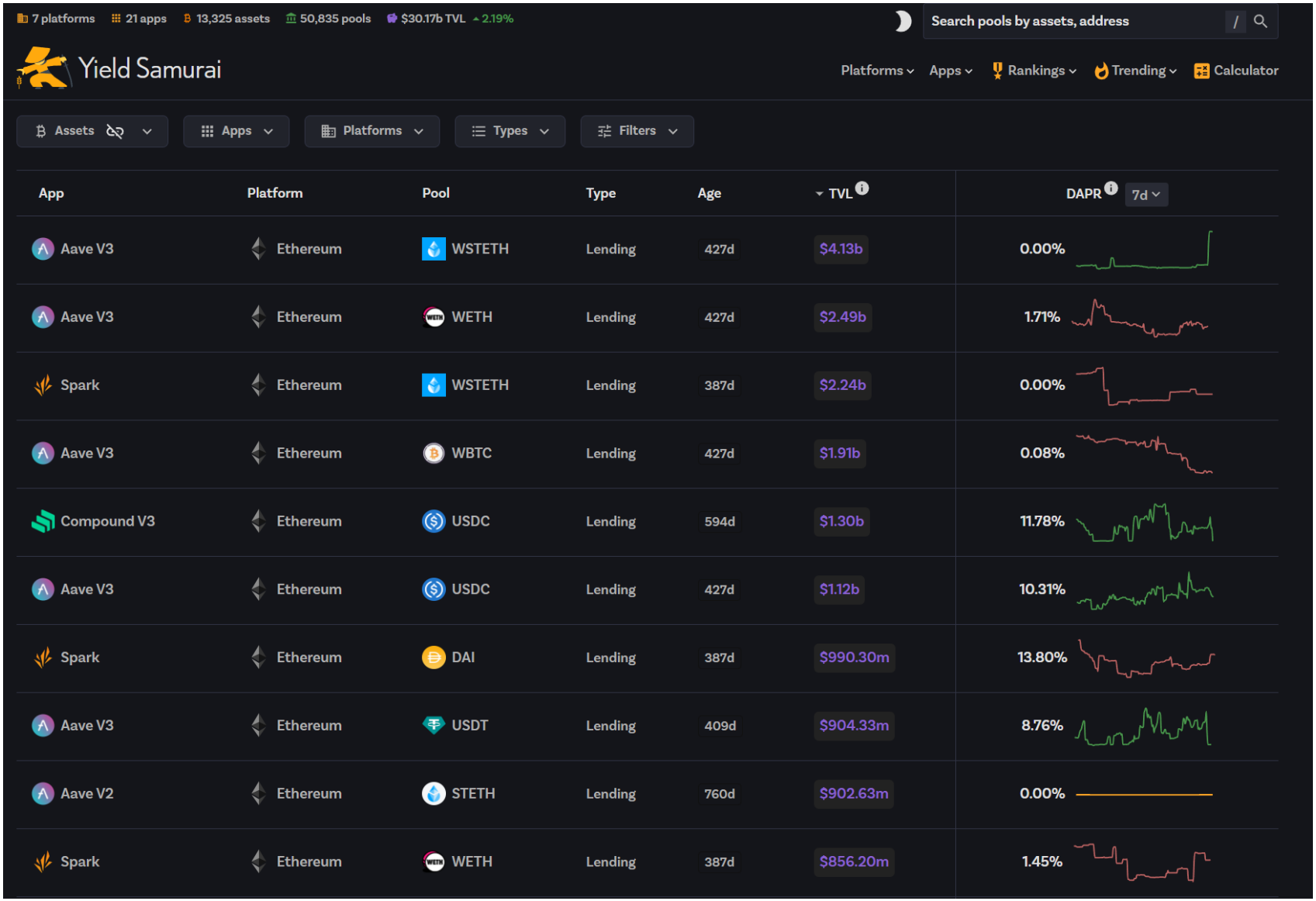


Nansen



NFT Collection	Volume (ETH)	Mkt Cap (ETH)	Avg Price (ETH)	Floor (ETH)	Floor 24H	Floor 3D	# Wallets	Deployed
RENGA	1,443	19,856	2.59	2.37	41%	90%	2,821	30d ago
CryptoPunks	1,201	3,002,200	300	63	0.08%	-6.6%	3,602	1927d ago
Black Box	457	9,509	4.05	4.5	33%	62%	1,139	102d ago
QQL Mint Pass	331	17,030	18	16	-20%	-9.24%	496	4d ago
Ethereum Name Service (ENS)	251	86,515	.0339	<.0001	0	0	556,637	976d ago
0x7df…f1e27	223	504	.0648	.089	242%	266%	2,785	20d ago
Mutant Ape Yacht Club	223	309,923	16	16	-0.82%	-0.95%	12,946	399d ago
Ekta Portal	203	346	.2202	.59	0	-9.23%	367	5d ago
Otherdeed for Otherside	181	308,469	3.55	1.68	1.27%	0.6%	34,037	157d ago
Genshin Impact Fandom	164	245	1.52	.271	1.23%	-	136	51h ago
TwitterScan Pass	152	929	.1548	.154	15%	-	2,058	4d ago
CloneX	139	168,965	8.72	6.7	-0.79%	-0.05%	9,585	294d ago
Gangster All Star: Evolution	116	2,700	.3472	.29	29%	41%	3,006	25d ago
Silks 2022 Genesis Yearlings	105	538	.3631	.46	-9.8%	-	522	3d ago
X SOLDIERS Collections	84	76	.0511	.0898	-	-	730	8d ago

Yield Samurai



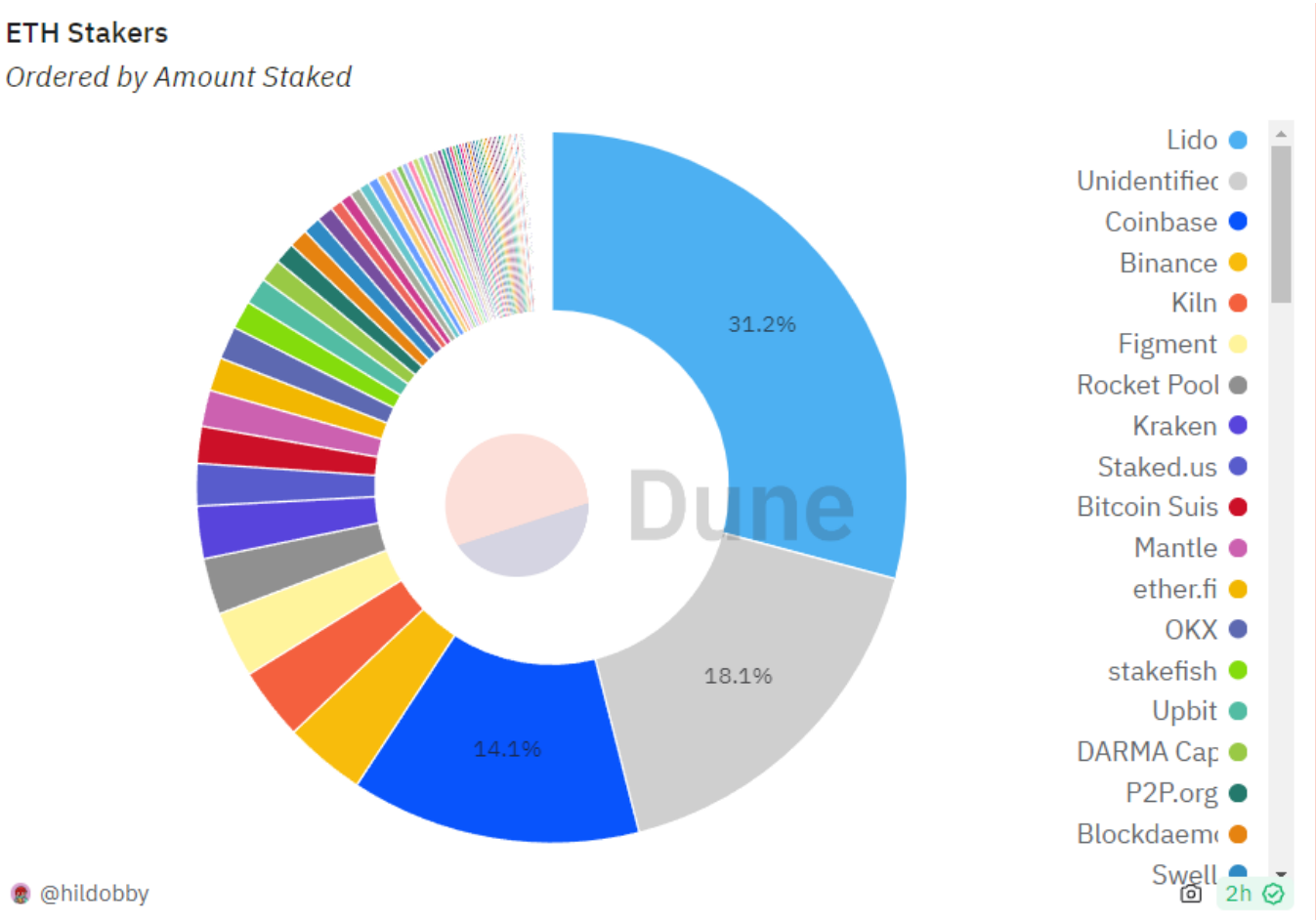
Project Ideas: ETH Data Analytics

- No data costs: literally everything is public!
- Potentially good area for class projects!
  - (Slightly outdated as-of 2022) Recent examples: TransposeData, others
- Core components:
  - Familiarity with big data pipelines: AWS/Google cloud...
  - Organize data into useful format: dashboards, ML analytics...
  - Find a target market: devs, traders...

Proof of Stake

- Originally, ETH mining proof-of-work, similar to BTC
- On Sept 15 2022, ETH switched to proof of stake
- Users deposit ("stake") 32 ETH into a special smart contract
- Stakers randomly selected (prop. to stake) to propose new blocks
- If a staker is caught trying to do "bad things" (e.g. propose 2 inconsistent blocks), they are "slashed": staked ETH is removed by smart contract
- Most newer blockchains (SOL, LUNA, AVAX) use proof-of-stake

Staking is Very Concentrated!



Source: Dune

Staking is Very Concentrated!

ETH Stakers

Ordered by Amount Staked

#	Entity	Category	ETH Staked	Validators	Marketshare	1WΔ
1	Lido	Liquid Staking	9,818,140	307k	31.2%	0%
2	Coinbase	CEXs	4,433,345	139k	14.1%	1%
3	Binance	CEXs	1,219,360	38k	3.9%	-9%
4	Kiln	Staking Pools	1,081,056	34k	3.4%	3%
5	Figment	Staking Pools	992,096	31k	3.1%	1%
6	Rocket Pool	Liquid Staking	838,007	26k	2.7%	-1%
7	Kraken	CEXs	779,009	24k	2.5%	0%
8	Staked.us	Staking Pools	620,668	19k	2.0%	5%
9	Bitcoin Suisse	CEXs	540,438	17k	1.7%	0%

Source: Dune

Why Does PoS Matter?

- If you're building on Ethereum, what's the most important takeaways from the PoW-PoS shift?
- Relatively little. . . everything largely keeps working as before

Why Does PoS Matter?

- If you're building on Ethereum, what's the most important takeaways from the PoW-PoS shift?
- Relatively little. . . everything largely keeps working as before
- If you work on MEV/ordering-sensitive topics, some important shifts
- Some philosophical centralization concerns
- However, most of the time you can ignore PoS

Things We Missed

- Details of staking, slashing
  - Not super relevant for application-layer
- Miner extractable value, transaction ordering...
  - Interesting but niche topic, will discuss briefly in AMMs class
- That's it for Ethereum! On to the competition...

ETH L2s

ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled

ETH L2s

ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on "rollup" is exactly what would happen on ETH main chain! Two methods:
  - **Optimistic rollup** (Optimism, Arbitrum, Coinbase Base): Can "challenge" L2 transactions, will (essentially) run on L1 if challenged
  - **ZK-rollup** (zkSync, StarkWare, Polygon): Some math black magic proves validity of transactions

ETH L2s

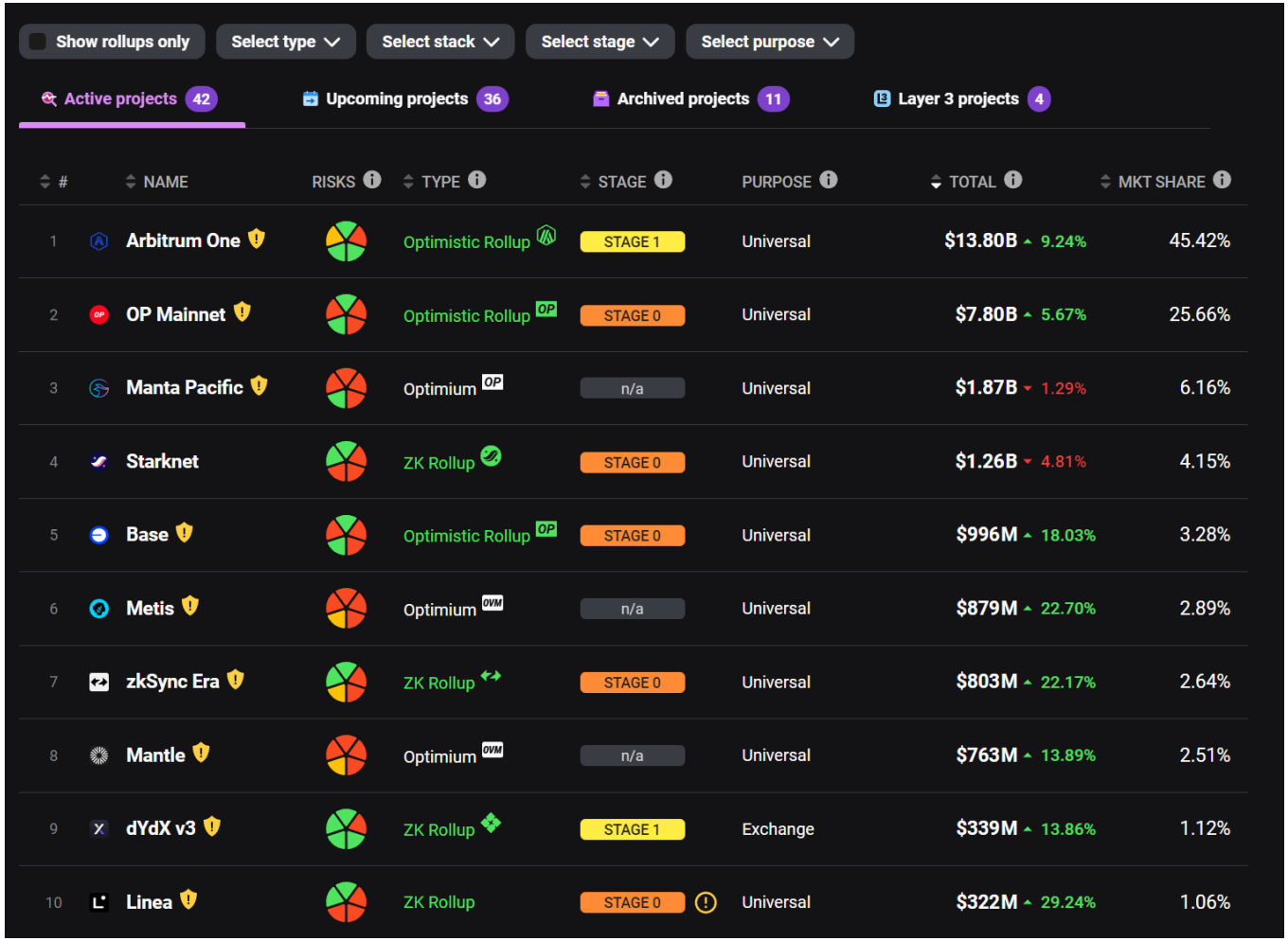
ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on "rollup" is exactly what would happen on ETH main chain! Two methods:
  - **Optimistic rollup** (Optimism, Arbitrum, Coinbase Base): Can "challenge" L2 transactions, will (essentially) run on L1 if challenged
  - **ZK-rollup** (zkSync, StarkWare, Polygon): Some math black magic proves validity of transactions
- Industry state:
  - $30B locked! ETH market cap is $408B, stables ~$141B
  - Optimistic rollups somewhat bigger than ZKs

ETH L2s

Source: L2beat

ETH L2s



Source: L2beat

Other L1s

Proliferation of other "L1's", doing similar things to Ethereum. Some notable ones:

- Avalanche, Solana
- Luna (now dead)
- Cosmos, Polkadot, Polygon
- Tron, Binance Smart Chain
- Aptos, Sui
- Appchains: dydx
- Others?

L1 design tradeoffs

- Some more centralized than others
  - Solana, Binance smart chain, Tron (?)
- Many technical innovations:
  - Solana "proof of history"
  - Avalanche "snowball algorithm"
- Ability to create "sidechains" or "app-specific chains"
  - Avalanche, Cosmos, Polkadot
- Native integration with applications, e.g. stablecoins
  - Luna...
- Interoperability among blockchains/ease of bridging
  - Polygon

Other L1s

- ETH still largest by market cap (behind BTC)
- Many newer L1's "faster" and "cheaper" than ETH
- L1's "centralized" in terms of development/funding: often large "ecosystem funds" to promote using/building on
  - More in ecosystem lecture
- However, still few compelling applications on alt-L1's (with some exceptions...)
- ETH market leader for now, but hard to say how things develop in future

Other L1s

- ETH still largest by market cap (behind BTC)
- Many newer L1's "faster" and "cheaper" than ETH
- L1's "centralized" in terms of development/funding: often large "ecosystem funds" to promote using/building on
  - More in ecosystem lecture
- However, still few compelling applications on alt-L1's (with some exceptions...)
- ETH market leader for now, but hard to say how things develop in future
- **Project ideas**: I'd slightly lean against proposing a new L1/L2 for class project
  - IMO, more an engineering problem than a business/law one
  - But if you think of a unique take, go for it!

The DAO Incident

- In 2016, org called "The DAO" raised $150mil USD of ETH
- Hacker exploited a bug and stole $60mil...

The DAO Incident

- In 2016, org called "The DAO" raised $150mil USD of ETH
- Hacker exploited a bug and stole $60mil...
- ETH developers proposed a "hard fork": roll back Ethereum to before hack happened, and update the code to fix the bug!
- But the "non-forked" chain continues to exist, as "Ethereum Classic"

Centralization and Governance

- Even a "decentralized" chain like ETH, in practice has influential "central" parties (developers)
- "Centralized" chains, who run chain validation themselves, have even more power
- Should chain operators/influencers have th power to unilaterally influence chain outcomes?
- Currently, as far as I can tell, little regulatory guidance

Centralization and Governance

- Even a "decentralized" chain like ETH, in practice has influential "central" parties (developers)
- "Centralized" chains, who run chain validation themselves, have even more power
- Should chain operators/influencers have th power to unilaterally influence chain outcomes?
- Currently, as far as I can tell, little regulatory guidance

Policy questions

- What are the roles and obligations of chain operators?
- How much discretion should chain operators have to rollback changes?


I mean, what's the point?
Sow.

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives. . .)
  - Firms (Employment, trade agreements. . .)
  - RSOs, religions, governments. . .
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!
- Trust derives from a system for promise enforcement: the legal system and the government's monopoly on violence

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!
- Trust derives from a system for promise enforcement: the legal system and the government's monopoly on violence
- But many people can't use these systems!

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!
- Trust derives from a system for promise enforcement: the legal system and the government's monopoly on violence
- But many people can't use these systems!
  - Non-US groups in low state capacity countries

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!
- Trust derives from a system for promise enforcement: the legal system and the government's monopoly on violence
- But many people can't use these systems!
  - Non-US groups in low state capacity countries
  - Criminal organizations

The Market For Promises

I attempt an answer in a blog post

- Many pieces of human society are based on promises
  - Financial assets (stocks, loans/bonds, derivatives...)
  - Firms (Employment, trade agreements...)
  - RSOs, religions, governments...
- Promises involve trust! Finance, firms, and organizations only work if people keep their promises!
- Trust derives from a system for promise enforcement: the legal system and the government's monopoly on violence
- But many people can't use these systems!
  - Non-US groups in low state capacity countries
  - Criminal organizations
  - "Small" organizations (RSOs, community groups...)

The Market For Promises

- BB is an alternative promise enforcement technology!

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)
- BB can't steal Alice's money, without Alice's private key

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)
- BB can't steal Alice's money, without Alice's private key
- BB can't change Alice's tx's, without Alice's key

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)
- BB can't steal Alice's money, without Alice's private key
- BB can't change Alice's tx's, without Alice's key
- All miners/validators can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)
- BB can't steal Alice's money, without Alice's private key
- BB can't change Alice's tx's, without Alice's key
- All miners/validators can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees
- Miners could try to boycott Alice's tx's...

The Market For Promises

- BB is an alternative promise enforcement technology!
- BB sees valid tx's submitted by Alice (sends, votes, bets...)
- BB can't steal Alice's money, without Alice's private key
- BB can't change Alice's tx's, without Alice's key
- All miners/validators can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees
- Miners could try to boycott Alice's tx's...
  - But there's many other miners happy to collect Alice's gas fees, and BB can't fight longest chain

Blockchains and Access

- Relative to court systems, blockchains are low-cost, and have very low barriers to access
- Anyone with an internet connection can make promises on blockchains!
- Costs fairly low, rel. to hiring lawyers + going to court in high-income countries
- Anyone can access: criminal organizations, RSOs...

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives
  - Generalized voting mechanisms

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives
  - Generalized voting mechanisms
- Some core problems:

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives
  - Generalized voting mechanisms
- Some core problems:
  - Referencing real world assets is hard

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives
  - Generalized voting mechanisms
- Some core problems:
  - Referencing real world assets is hard
  - Conditioning promises on real world events also hard: oracle problems

Limits of the Market

- Blockchains can only keep promises involving on-chain assets and events
- If there exist valuable on-chain assets, this is a pretty big set of promises!
  - Generalized financial derivatives
  - Generalized voting mechanisms
- Some core problems:
  - Referencing real world assets is hard
  - Conditioning promises on real world events also hard: oracle problems
- But the simple M/N multisig is a powerful technology!

Blockchains and Discretion

- Governments and courts are discretionary by default
  - Cons: costly, takes time, errors, corruption...
  - Pros: "rule of reason", better handling of edge cases

Blockchains and Discretion

- Governments and courts are discretionary by default
  - Cons: costly, takes time, errors, corruption...
  - Pros: "rule of reason", better handling of edge cases
- Blockchains are nondiscretionary by default
  - Pros: low-cost, "instant" outcomes
  - Cons: cannot apply "rule of reason", unforeseen cases can be handled badly, and hard to reverse!

See my blog post on discretion

Code is Law. . . ?

CoinDesk

Policy Technology Web3 L

oin $282.22 -0.62% Binance USD $0.999974 +0.01% Cardano $0.429997 -0.85% Stellar $0.121040 +5.76% S

After 'Stealing' $16M, This Teen Hacker Seems Intent on Testing 'Code Is Law' in the Courts

Will DeFi's unofficial ethos hold up in court? A Canadian math prodigy could be betting his future on just that.

Andrew Thurman

Oct 22, 2021 at 4:40 p.m. CDT Updated Oct 22, 2021 at 5:57 p.m. CDT Layer 2

(Tingey Injury Law Firm/Unsplash)

Convergent Evolution

- BB's default is non-discretionary, but discretion can be built!
- In particular, you can build a court system in BB
- "Cases" tried before a (token-voting? Dictatorial?) court, possibility of discretionary "overrides" of rules
  - "Kill-switches" or "freeze switches" built into a number of defi protocols
  - "DAO court trials" basis for an insurance protocol, Nexus Mutual

Convergent Evolution

- BB's default is non-discretionary, but discretion can be built!
- In particular, you can build a court system in BB
- "Cases" tried before a (token-voting? Dictatorial?) court, possibility of discretionary "overrides" of rules
  - "Kill-switches" or "freeze switches" built into a number of defi protocols
  - "DAO court trials" basis for an insurance protocol, Nexus Mutual
- "Convergent evolution" of promise enforcement systems
  - Full discretion, no discretion both imperfect: we build towards something in the middle

The Market For Promises: Project Ideas

- Blockchains and discretion:
  - How do we build discretion? Token courts? Other clever mechanisms?
  - What applications benefit most from discretion? Insurance? Defi "kill-switches"? Web3 gaming?
- The real world asset (RWA) problem:
  - How do we "glue" RWAs to the blockchain? (Many firms working on)
  - Improved oracles? (Chainlink clear market leader, Pyth a competitor)
- The boundaries of the market:
  - What are forms of rule-based social organization, not served well by the traditional promise enforcement mechanisms, that blockchains could do a better job for?
  - Build a product for these people!