Ethereum and Smart Contracts

MGT 4074 Fintech & Crypto Tokens, Section A, Spring 2025

Joseph Hall

Georgia Institute of Technology

Sep 22, 2025

Reading

For **Wednesday**:

Please read "The Market for Promises" by Anthony Lee Zhang
https://anthonyleezhang.substack.com/p/the-market-for-promises

In the News

Can Ethereum remain the go-to "utility" blockchain?

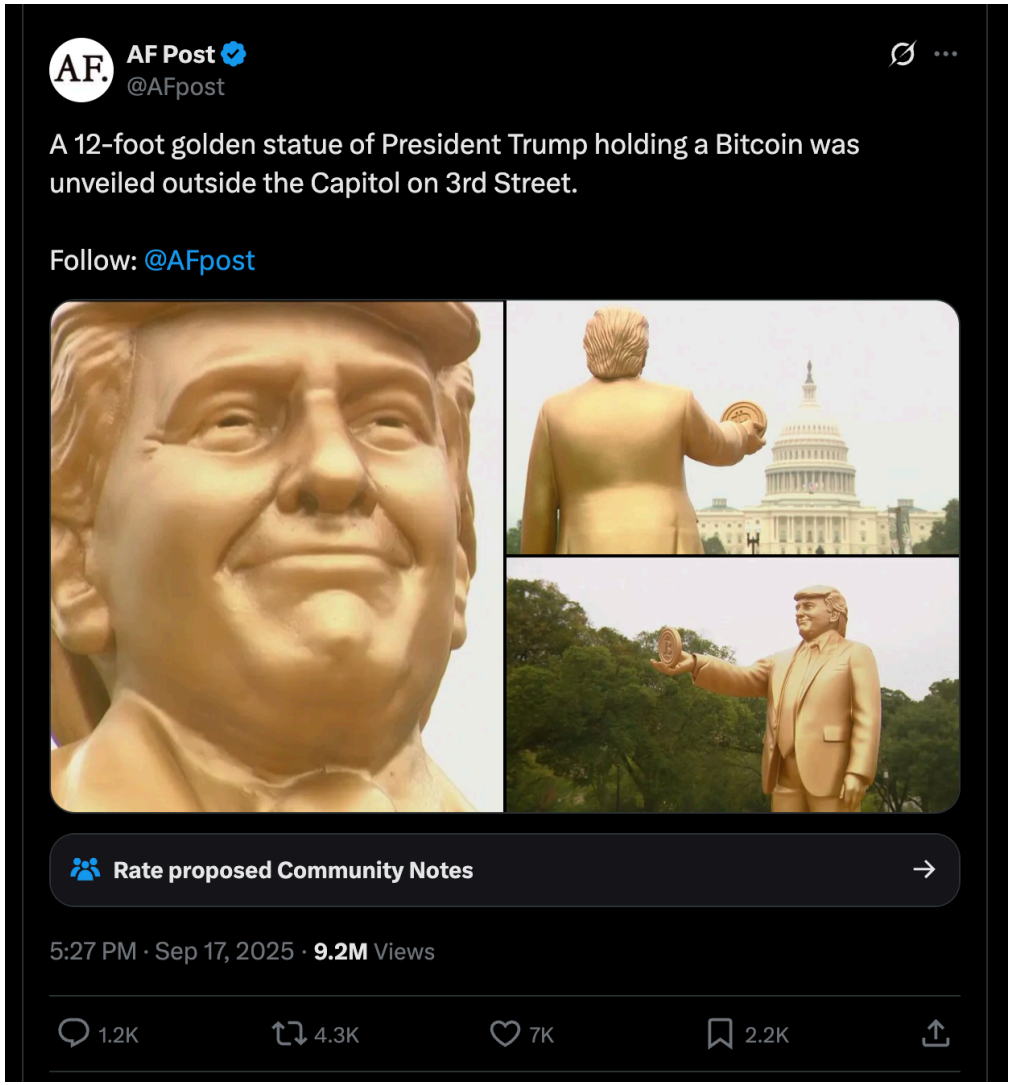
by Nikolaos Panigirtzoglou, Mika Inkinen, Mayur Yeole, and Krutik P Mehta of JP Morgan "Flows & Liquidity"

Uniswap is one of ethereum's largest gas consuming protocols, and a migration from ethereum could induce substantial loss for ethereum's fee pool. This trend of dapps migrating along with their users to layer 2s or alternative layer 1s or them creating their own chains for scalability and cost-effectiveness, could have a negative impact on ethereum by reducing activity in the main network, leading to lower transaction revenue and validators' earnings, and making ethereum inflationary from a supply point of view as fewer transactions imply reduced token burning. The ethereum network appears to lag competitors' growth, in particular **Solana, which saw exponential growth in its user base due to surge in memecoin activity.**

In the News

Despite all the above challenges, **the ethereum ecosystem appears to be still dominant in stablecoin, DeFi, and tokenization spaces.** It remains to be seen whether the ethereum network manages to maintain its advantage/dominance in these spaces. To boost institutional interest around ethereum, the Ethereum Foundation has supported and partially funded Etherealize, with the aim of educating and marketing smart contract functionality. Etherealize also aims to increase the tokenization of real world assets on ethereum. Notable examples of institutions involved with tokenization on ethereum are the European Investment Bank which has issued digital bonds on the ethereum blockchain, BBVA utilizing Visa's tokenized asset platform for ethereum-based tokens with pilot projects slated for 2025, and Blackrock and Franklin Templeton increasing their tokenization efforts on the ethereum network. Tokenization initiatives could play a significant role in bringing further institutional demand to the ethereum network but competition from other networks is likely to remain intense in the foreseeable future.

Also in the News



Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Outline

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

Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Vitalik Buterin

- Born in Kolomna, Russia, 1994, 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

Universal Computers

- 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 Computers

- 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 Computers

- 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

Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Why learn technical details as a business major?

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

Why learn technical details as a business major?

"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 learn technical details as a business major?

"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 learn technical details as a business major?

"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 not *that* hard

The Structure of Ethereum

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

Smart Contracts

"A smart contract is essentially an automated agent that lives on the Ethereum network, has an Ethereum address and balance, and can send and receive transactions. A contract is "activated" every time someone sends a transaction to it, at which point it runs its code, perhaps modifying its internal state or even sending some transactions, and then shuts down."
-Ethereum Whitepaper, Vitalik Buterin (2014)

Smart Contracts

- A smart contract is:
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write

Smart Contracts

- A smart contract is:
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write
- If you've heard of object oriented programming: smart contracts are a bundle of functions (code), data, as well as ETH balances

Smart Contracts

- A smart contract is:
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write
- If you've heard of object oriented programming: smart contracts are a bundle of functions (code), data, as well as ETH balances
- The most popular coding language which compiles Ethereum script code (a minimal Turing-complete language akin to assembly) is called **Solidity**

Smart Contracts

- A smart contract is:
  - A wallet, which can hold Ether (ETH),
  - Functions it can call when requested as determined by its code,
  - (optionally) a source of data to which it can read and write
- If you've heard of object oriented programming: smart contracts are a bundle of functions (code), data, as well as ETH balances
- The most popular coding language which compiles Ethereum script code (a minimal Turing-complete language akin to assembly) is called **Solidity**

Deploying a smart contract or calling its functions requires a **gas fee**: ETH must be paid to the network to run the code.

Smart Contract Example: Tokens

- An ETH address, "technically", only "holds" Ether ("ETH") natively – no other tokens!
- An ETH address can be assigned non-ETH tokens through smart contracts
- A smart contract can define tokens using the **ERC-20** standard
  - So-called because it was originally the 20th submission to "Ethereum Requests for Comments"

Is ETH intended to store value?

Unlike BTC, its scarcity is not strict. This is reflected in prices:

Is ETH intended to store value?

Unlike BTC, its scarcity is not strict. This is reflected in prices:

- This is by design: ETH itself is a currency to pay gas fees to run smart contracts

Is ETH intended to store value?

Unlike BTC, its scarcity is not strict. This is reflected in prices:

- This is by design: ETH itself is a currency to pay gas fees to run smart contracts
- Think of ETH like PACE credits at GATech: kept in short supply only to ensure people don't abuse computing resources

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

Smart contracts which issue tokens must adhere to this standard to be interoperable with dapps (decentralized apps)

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

Smart contracts which issue tokens must adhere to this standard to be interoperable with dapps (decentralized apps)

The ERC-20 Standard requires that a smart contract issuing tokens have certain functions including:

- Report the name and symbol of the token

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

Smart contracts which issue tokens must adhere to this standard to be interoperable with dapps (decentralized apps)

The ERC-20 Standard requires that a smart contract issuing tokens have certain functions including:

- Report the name and symbol of the token
- Transfer tokens from one wallet to another

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

Smart contracts which issue tokens must adhere to this standard to be interoperable with dapps (decentralized apps)

The ERC-20 Standard requires that a smart contract issuing tokens have certain functions including:

- Report the name and symbol of the token
- Transfer tokens from one wallet to another
- Report the balance of a wallet

The ERC-20 Standard

The real power of the Ethereum network is the ability to create and issue new tokens with arbitrary programmable properties using **The ERC-20 Standard**

Smart contracts which issue tokens must adhere to this standard to be interoperable with dapps (decentralized apps)

The ERC-20 Standard requires that a smart contract issuing tokens have certain functions including:

- Report the name and symbol of the token
- Transfer tokens from one wallet to another
- Report the balance of a wallet
- Report the total supply of the token

The full standard from eips.ethereum.org

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?

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 to never update a piece of code by hard-coding functions into the public solidity code

Can Smart Contracts be Changed?

Takeaways:

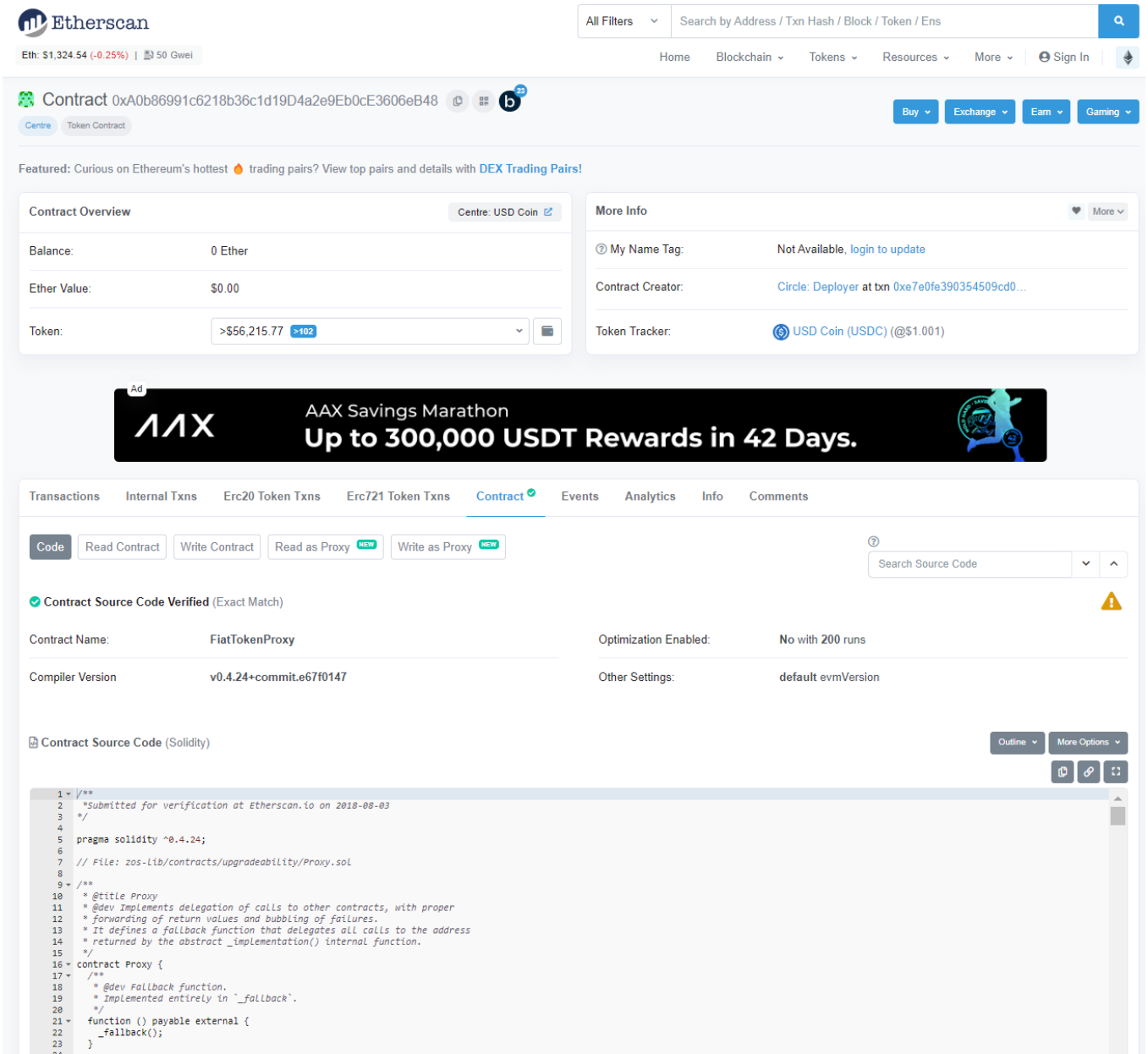
- Smart contracts can be built in a way that makes them upgradable
- But (from the code) you can tell whether a smart contract is upgradable or not
- Devs can commit to never update a piece of code by hard-coding functions into the public solidity code
- **or**, Devs can avoid committing to that promise by writing functions that reference other sources of data (which can in principle be indecipherable to the public)
- Thus, developers face a **tradeoff**: contracts may be either *upgradeable and private* or *public and immutable* – they can never be both.

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

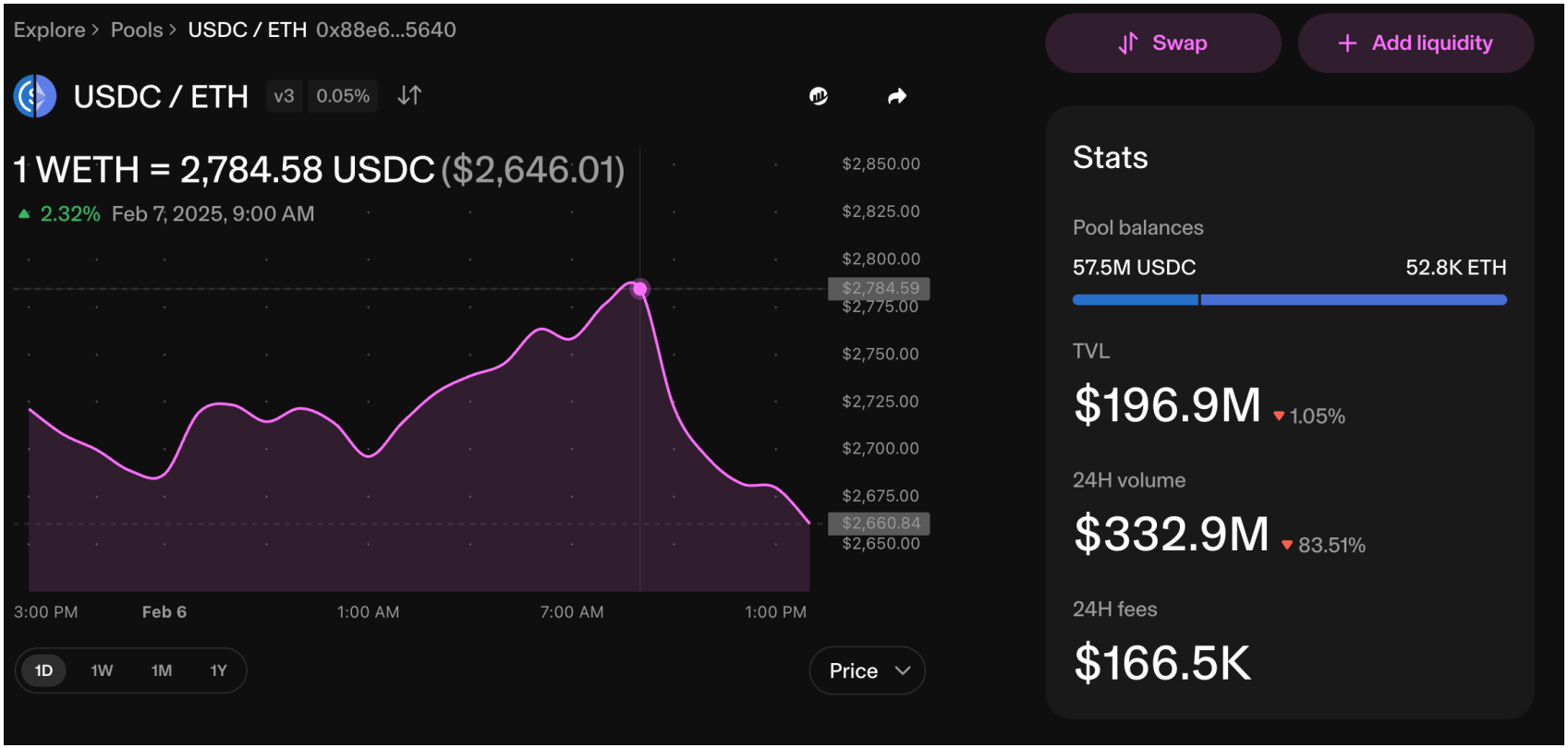
Can you tell what the code in a smart contract is?

- 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
- Developers can voluntarily publish their code (and anyone can verify that it matches the compiled code hash)

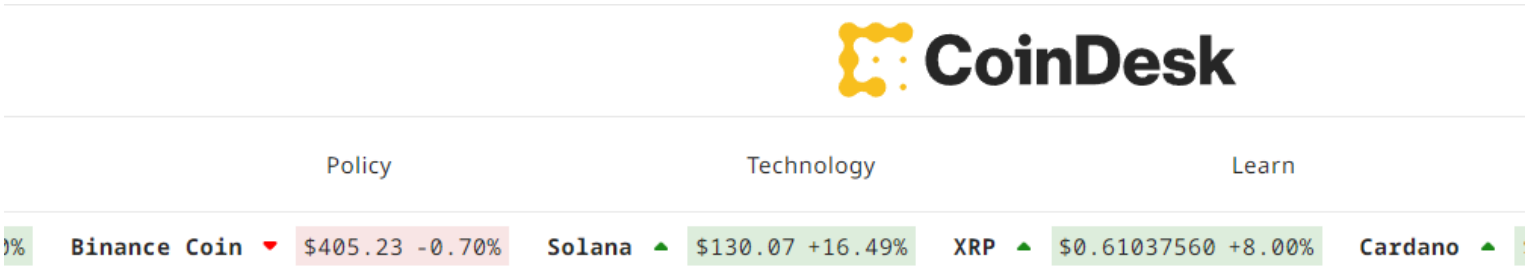
Can you tell what code in a smart contract is?



Uniswap is (essentially) a Smart Contract



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.

Smart Contracts and Regulation

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

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.

Is Uniswap a Securities Exchange?

From Uniswap's letter to the SEC:

The Protocol Is an Automated Market Maker Technology Controlled by No Individual or Entity.

The Protocol is an autonomous set of "smart contracts" that run on the Ethereum network—that is, software on the Ethereum blockchain programmed to automatically execute trades, akin to a pre-programmed digital vending machine. The Protocol is the first widely successful automated market maker ("AMM"), and relies on LPs contributing liquidity into a liquidity pool that generally contains two specific assets. Liquidity pools represent the quantity of assets that users in the aggregate are willing to have swapped at prices determined using a constant-product market maker formula ($x*y = k$), which automatically rebalances with swaps as the ratios of various assets fluctuate. The formula ensures that the product of x and y, representing the balance of the two tokens in any pool, equals a constant, k. Because the relative price of the assets can be changed only through trading, divergences between the Protocol price and external prices create market opportunities. The combination of the formula plus the rebalancing mechanism thus ensures that Protocol prices always trend toward the market clearing price.

Welcome! Today is Wednesday September 24, 2025

No quiz today, roll call instead.
Homework 3 has been published to Canvas. It is due a week from Monday (10/6) at the start of class.

Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Gudied Discussion: the Market for Promises

Q: How would we summarize Anthony's argument?

Gudied Discussion: the Market for Promises

Q: How would we summarize Anthony's argument?
A: Since Smart Contracts/DeFi is naturally a substitute for effective governments, the future of DeFi will be built in places with ineffective governments.

Gudied Discussion: the Market for Promises

Q: How would we summarize Anthony's argument?
A: Since Smart Contracts/DeFi is naturally a substitute for effective governments, the future of DeFi will be built in places with ineffective governments.
Q: What are arguments for and against this

Gudied Discussion: the Market for Promises

Q: How would we summarize Anthony's argument?
A: Since Smart Contracts/DeFi is naturally a substitute for effective governments, the future of DeFi will be built in places with ineffective governments.
Q: What are arguments for and against this
For:

- Dysfunctional legal systems make DeFi's neutrality more valuable (demand side)
- Low state capacity = weak ability to suppress blockchain adoption (supply side)

Gudied Discussion: the Market for Promises

Q: How would we summarize Anthony's argument?
A: Since Smart Contracts/DeFi is naturally a substitute for effective governments, the future of DeFi will be built in places with ineffective governments.
Q: What are arguments for and against this
For:

- Dysfunctional legal systems make DeFi's neutrality more valuable (demand side)
- Low state capacity = weak ability to suppress blockchain adoption (supply side)

Against:

- Poor infrastructure, connectivity, and literacy hinder DeFi uptake.
- Capital and liquidity still concentrate in developed markets.

The Market For Promises

Anthony Lee Zhang's blog post

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

The Market For Promises

Anthony Lee Zhang's 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

Anthony Lee Zhang's blog post

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

The Market For Promises

Anthony Lee Zhang's blog post

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

The Market For Promises

Anthony Lee Zhang's blog post

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

Anthony Lee Zhang's blog post

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

Anthony Lee Zhang's blog post

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

Anthony Lee Zhang's blog post

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

Anthony Lee Zhang's blog post

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

- BankBot ("BB") is an alternative promise enforcement technology!

The Market For Promises

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

The Market For Promises

- BankBot ("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

- BankBot ("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

- BankBot ("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 stakers can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees

The Market For Promises

- BankBot ("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 stakers can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees
- Stakers could try to boycott Alice's tx's...

The Market For Promises

- BankBot ("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 stakers can do is "execute" Alice's tx's, putting them in the chain and collecting gas fees
- Stakers could try to boycott Alice's tx's...
  - But there's many other stakers 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

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 and events is hard

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 ALZ blog post on discretion

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)
  - An oracle is third party system trusted to tell blockchains what has happened in the real world (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!

Roadmap

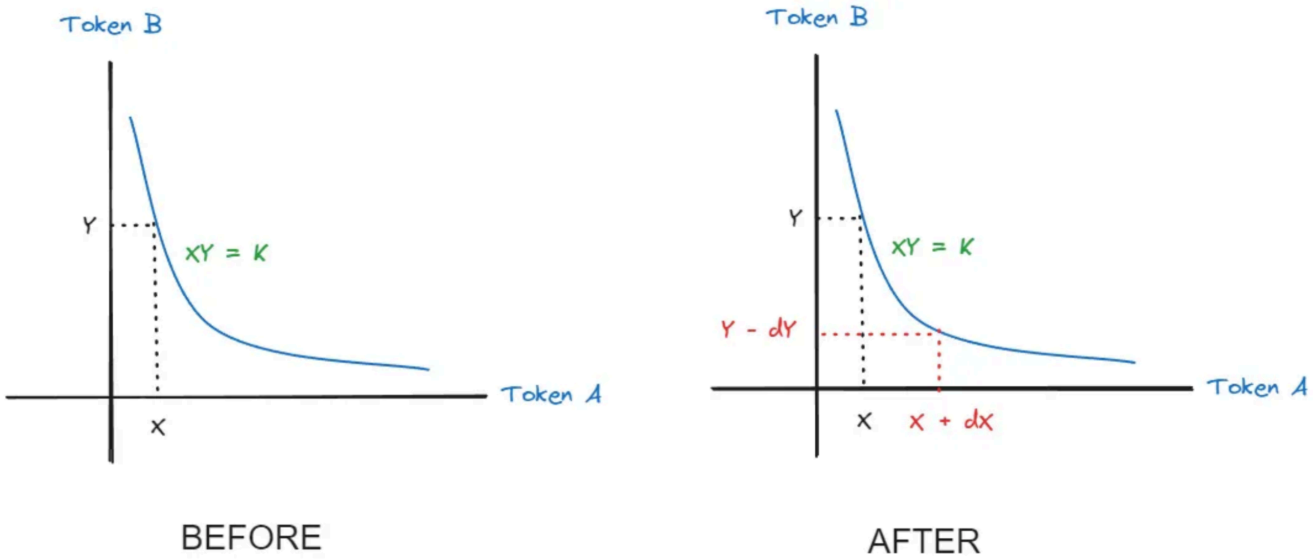
1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. Competition

Explore Uniswap

https://app.uniswap.org/explore/pools

Constant Product Automated Market Making

Liquidity Providers deposit X units of Token A and Y units of Token B. They earn fees when the pool is used.



Before and after each transaction (a swap or a liquidity injection), the **constant product rule** $XY = K$ must hold. Image Credit: Pari Tomar

Constant Product Rule Math

Q: Let X and Y be the number of type-x and type-y tokens. When I trade dx type-x tokens, how many type-y tokens will I receive (what is dy)?

Constant Product Rule Math

Q: Let X and Y be the number of type-x and type-y tokens. When I trade dx type-x tokens, how many type-y tokens will I receive (what is dy)?
The equation

$$X \cdot Y = K$$

becomes

$$(X + dx) \cdot (Y - dy) = K$$

Constant Product Rule Math

Q: Let X and Y be the number of type-x and type-y tokens. When I trade dx type-x tokens, how many type-y tokens will I receive (what is dy)?
The equation

$$X \cdot Y = K$$

becomes

$$(X + dx) \cdot (Y - dy) = K$$

Substitute $K = X \cdot Y$ and use algebra to isolate dy:

$$dy = \frac{Y \cdot dx}{X + dx}$$

Constant Product Rule Math

Q: When you increase dx, does the price move *in your favor* or *against you*?

Constant Product Rule Math

Q: When you increase dx, does the price move *in your favor* or *against you*?

A: Look at the equation and ask what happens when you **double** dx:

Constant Product Rule Math

Q: When you increase dx, does the price move *in your favor* or *against you*?
A: Look at the equation and ask what happens when you **double** dx: the numerator doubles, but the denominator increases as well – so dy **less than doubles** – the price moves *against you*.

Constant Product Rule Math

Q: When you increase dx, does the price move *in your favor* or *against you*?
A: Look at the equation and ask what happens when you **double** dx: the numerator doubles, but the denominator increases as well – so dy **less than doubles** – the price moves *against you*.
Q: When the liquidity of the pool increases (higher K), does this effect (the price moves against you) get stronger or weaker?

Constant Product Rule Math

Q: When you increase dx, does the price move *in your favor* or *against you*?
A: Look at the equation and ask what happens when you **double** dx: the numerator doubles, but the denominator increases as well – so dy **less than doubles** – the price moves *against you*.
Q: When the liquidity of the pool increases (higher K), does this effect (the price moves against you) get stronger or weaker?
A: Let X and Y be extremely large relative to dx and dy. Now, $X + dx \approx X$. In this case, dx and dy are *approximately linear* – the price movement is close to zero. **More liquidity means that prices move against you less**.

How do we police the smart contract ecosystem?

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

How do we police the smart contract ecosystem?

- How to ensure:
  - Programs don't run for too long, getting stakers stuck?
  - Programs don't use too much storage, running stakers out of "hard drive" space?
- Basic idea: charge people for resources they use
- Next, we'll talk about gas
- 10^{-18} ETH is called one **Wei** (for Wei Dai)
- 10^{-9} ETH is called one **Gwei** ("Giga-Wei")

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

```

Pricing Scarce Computation Resources

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

Pricing Scarce Computation Resources

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

- When you run smart contract code, every ETH staker has to run it!
- When you edit smart contract data, every ETH staker 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")

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g.

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g. Can you define a function $\mathrm{halts(g)}$ which returns TRUE if the program halts and FALSE if it will run forever?

E.g., if g is

$\mathrm{while(1==1)\{}$

$\mathrm{print(“Another\ Overtime\ in\ the\ Georgia\text{-}Tech\ Game!”)\}}$

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g.
Can you define a function $\mathrm{halts(g)}$ which returns TRUE if the program halts and FALSE if it will run forever?

E.g., if g is

$\mathrm{while(1==1)\{}$

$\mathrm{print(“Another\ Overtime\ in\ the\ Georgia\text{-}Tech\ Game!”)\}}$

Then $\mathrm{halts}(g) = \mathrm{FALSE}$ – g does not halt.

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g.
Can you define a function $\mathrm{halts(g)}$ which returns TRUE if the program halts and FALSE if it will run forever?

E.g., if g is
$\mathrm{while(1==1)\{}$
$\mathrm{print(“Another\ Overtime\ in\ the\ Georgia\text{-}Tech\ Game!”)\}}$

Then $\mathrm{halts}(g) = \mathrm{FALSE}$ – g does not halt.

Church (1936): No - $\mathbf{halts}(g)$ cannot exist.

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g. Can you define a function $\mathrm{halts(g)}$ which returns TRUE if the program halts and FALSE if it will run forever?

E.g., if g is

$\mathrm{while(1==1)\{}$

$\mathrm{print(“Another\ Overtime\ in\ the\ Georgia\text{-}Tech\ Game!”)\}}$

Then $\mathrm{halts}(g) = \mathrm{FALSE}$ – g does not halt.

Church (1936): No - $\mathbf{halts}(g)$ cannot exist.

The shortest possible proof: suppose such a function $\mathrm{halts}(g)$ exists. Then let g be:

The Halting Problem

Consider an algorithm (a set of instructions for a computer) g. Can you define a function $\mathrm{halts(g)}$ which returns TRUE if the program halts and FALSE if it will run forever?

E.g., if g is

$\mathrm{while(1==1)\{}$

$\mathrm{print(“Another\ Overtime\ in\ the\ Georgia\text{-}Tech\ Game!”)\}}$

Then $\mathrm{halts}(g) = \mathrm{FALSE}$ – g does not halt.

Church (1936): No - $\mathbf{halts}(g)$ cannot exist.

The shortest possible proof: suppose such a function $\mathrm{halts}(g)$ exists. Then let g be:

```
def g():
    if halts(g):
        loop_forever()
```

Unlike BTC, ETH has native gas fees

"In Bitcoin, there are no mandatory transaction fees. Transactions can optionally include fees which are paid to miners, and it is up to the miners to decide what fees they are willing to accept. In Bitcoin, such a mechanism is already imperfect...In Ethereum, because of its Turing-completeness, a purely voluntary fee system would be catastrophic. Instead, Ethereum will have a system of mandatory fees, including a transaction fee and six fees for contract computations."
-Ethereum Whitepaper, Vitalik Buterin (2014)

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

Ethereum Virtual Machine Native Gas Costs

evm.codes

Gas Fees and Smart Contracts

Meet BankBot ("BB"), a friendly hypothetical smart contract

Gas Fees and Smart Contracts

Meet BankBot ("BB"), a friendly hypothetical smart contract

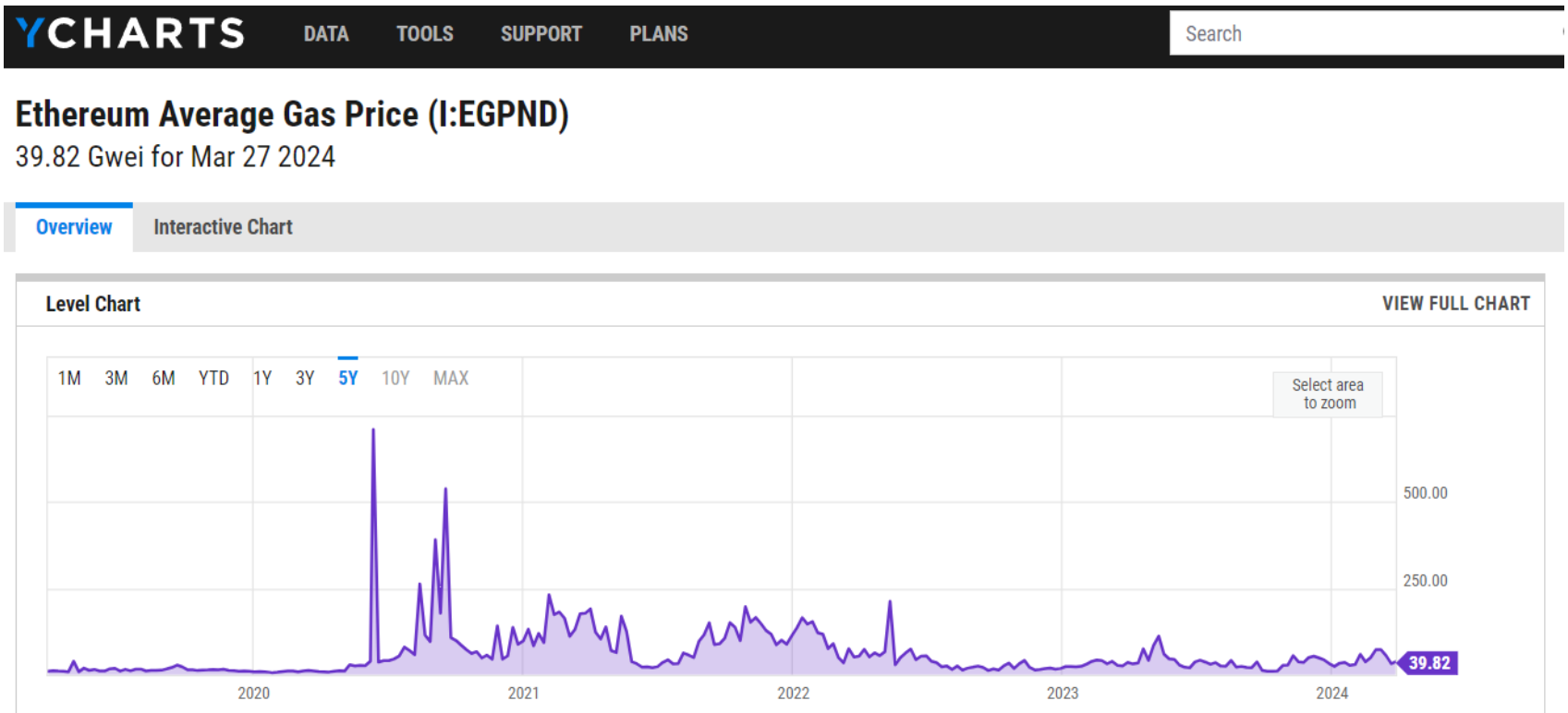
- BB's actions may cost ETH stakers compute + storage. But BB is a bot!
- BB only does things when human wallets ask it to...

Gas Fees and Smart Contracts

Meet BankBot ("BB"), a friendly hypothetical smart contract

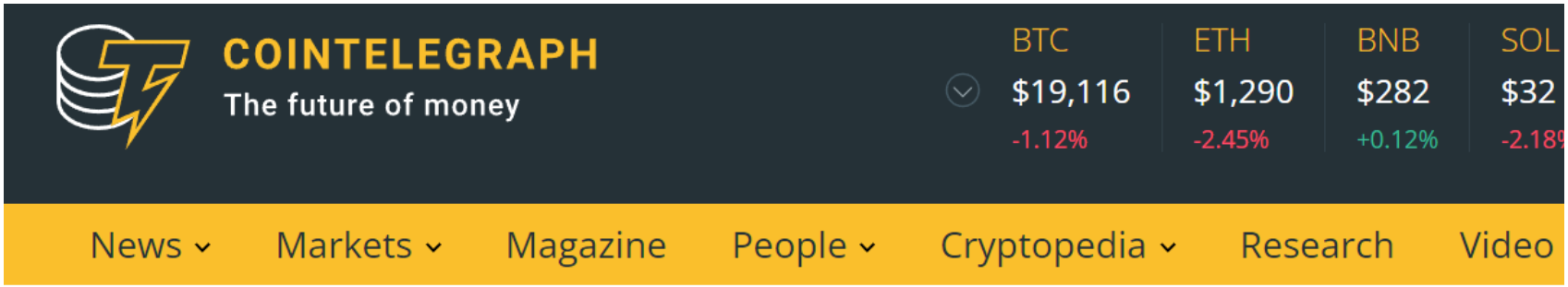
- BB's actions may cost ETH stakers compute + storage. But BB is a bot!
- BB only does things when human wallets ask it to...
- ...So BB only turns on if you pay for gas *up front*

Gas Prices Over Time



Source

Gas Prices and Transaction Demand

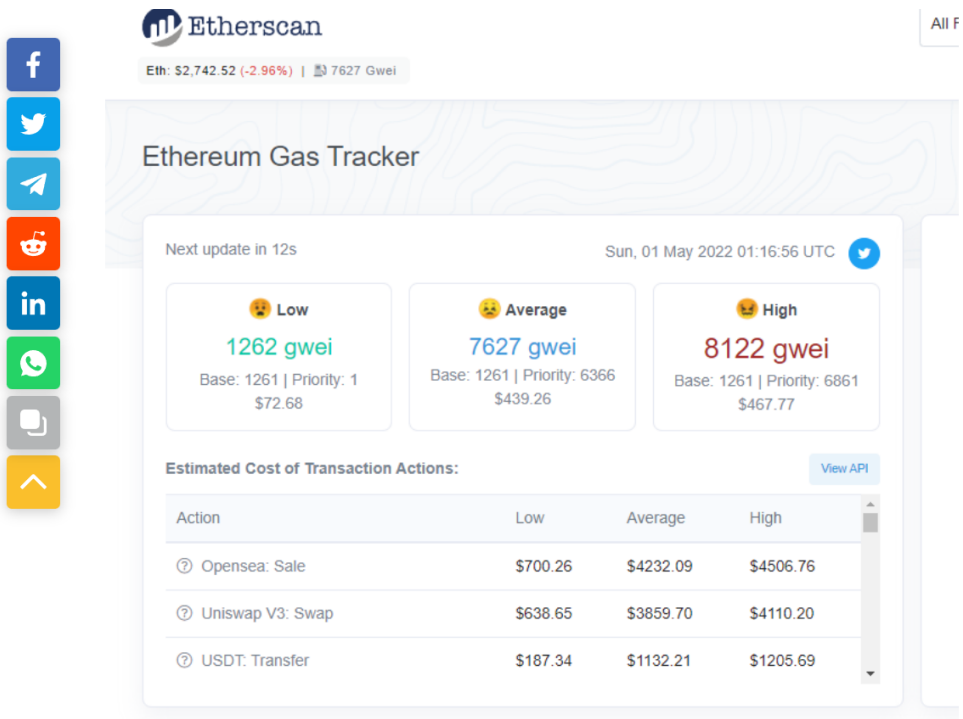


ARIJIT SARKAR MAY 01, 2022

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

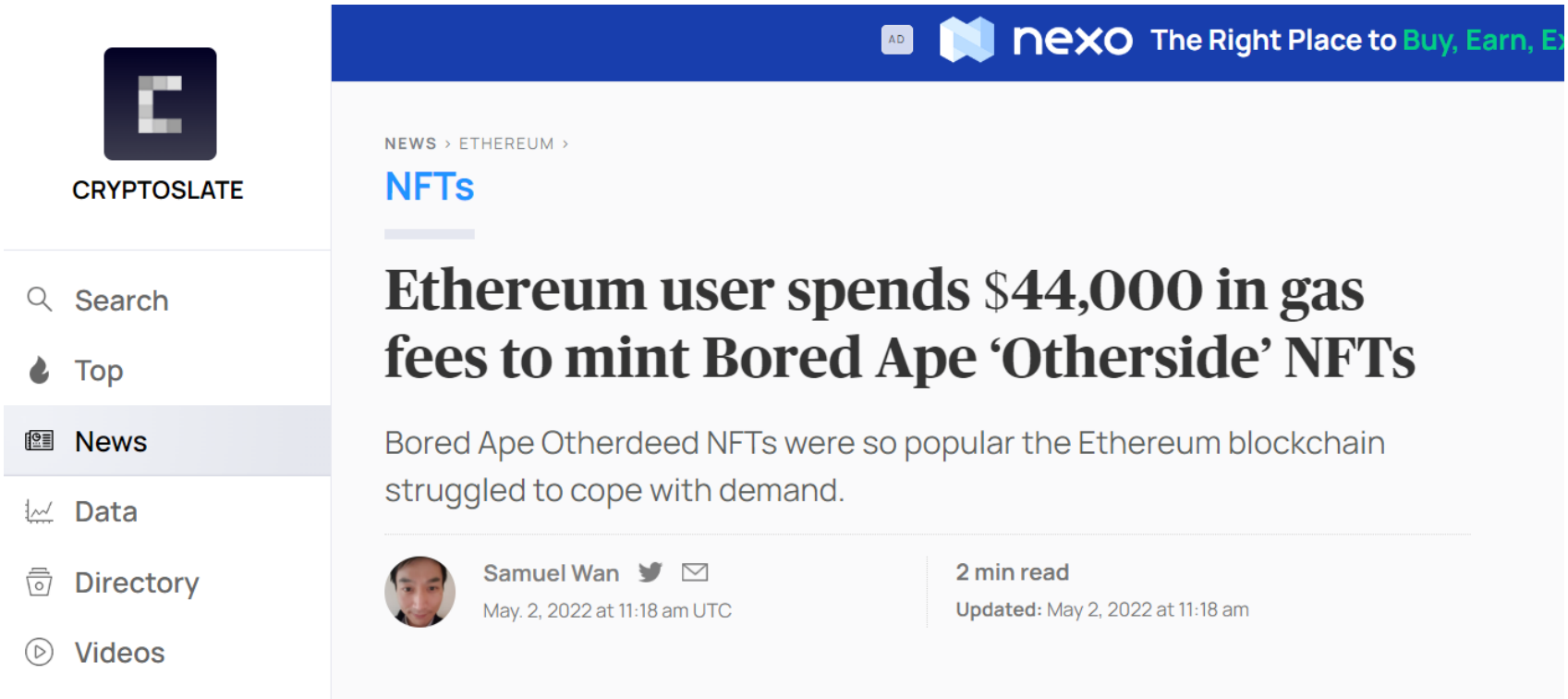


Ethereum gas tracker. Source: Etherscan

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 staker 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
  - Rollups do, which we will cover

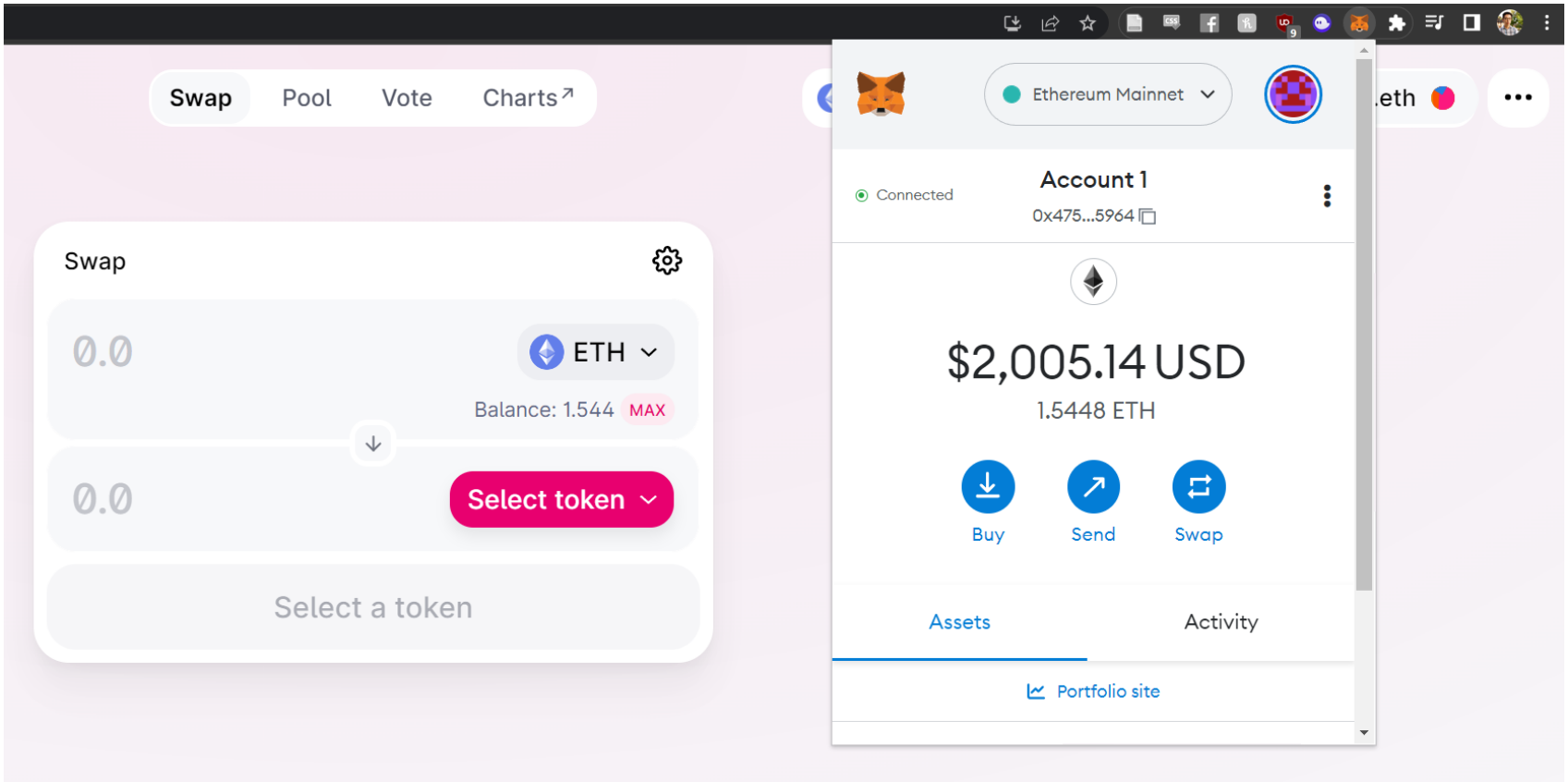
Gas Fees: Summary

- 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!

Rule Number 1 of Blockchain Security

Never,
Never,
Never,
Never,
Never give out your seed phrase!
EVEN IF THEY SAY THEY LOVE YOU

Shamir's Secret Sharing Scheme

Shamir's Secret Sharing Scheme

See here

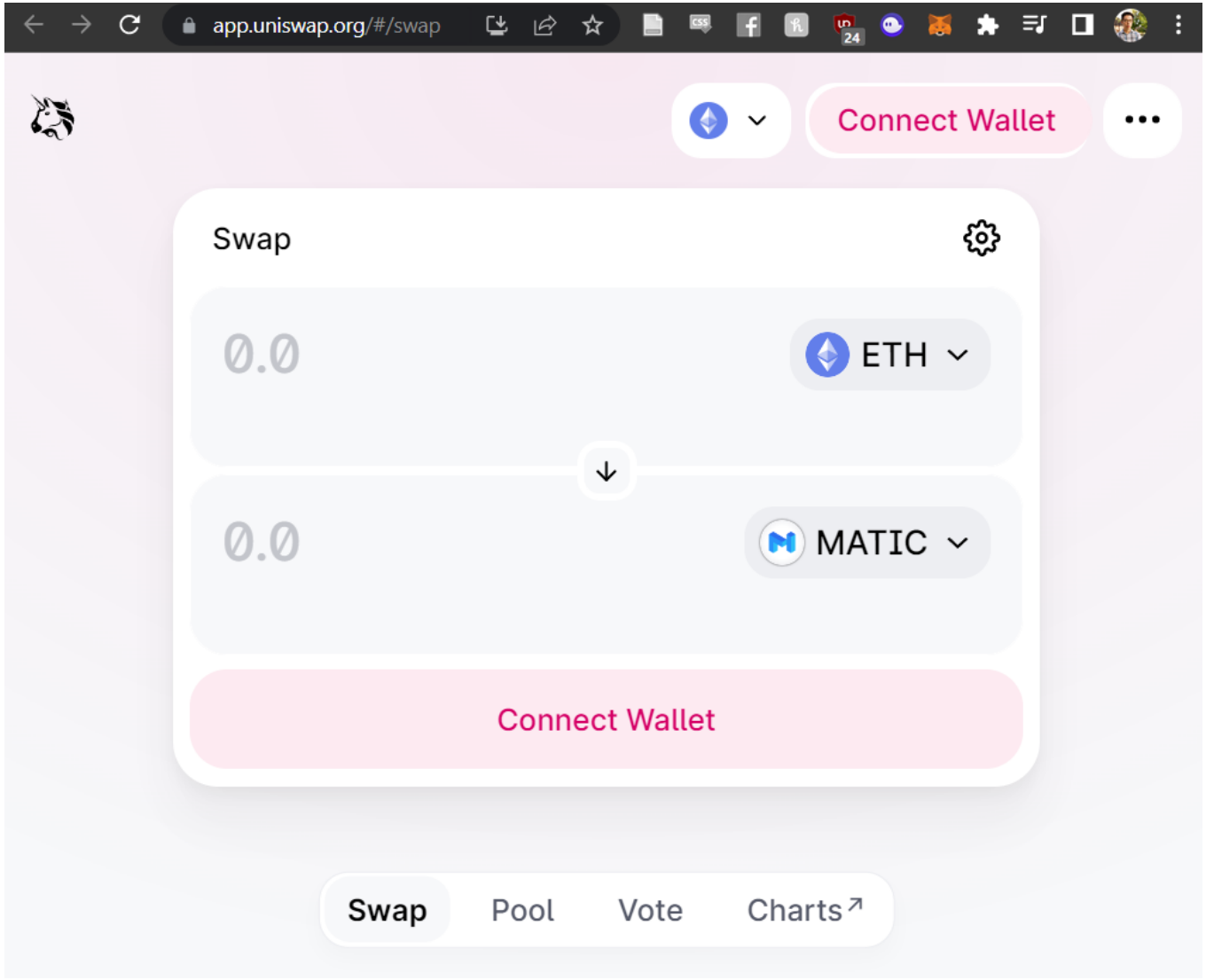
Hardware Wallets

- 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!

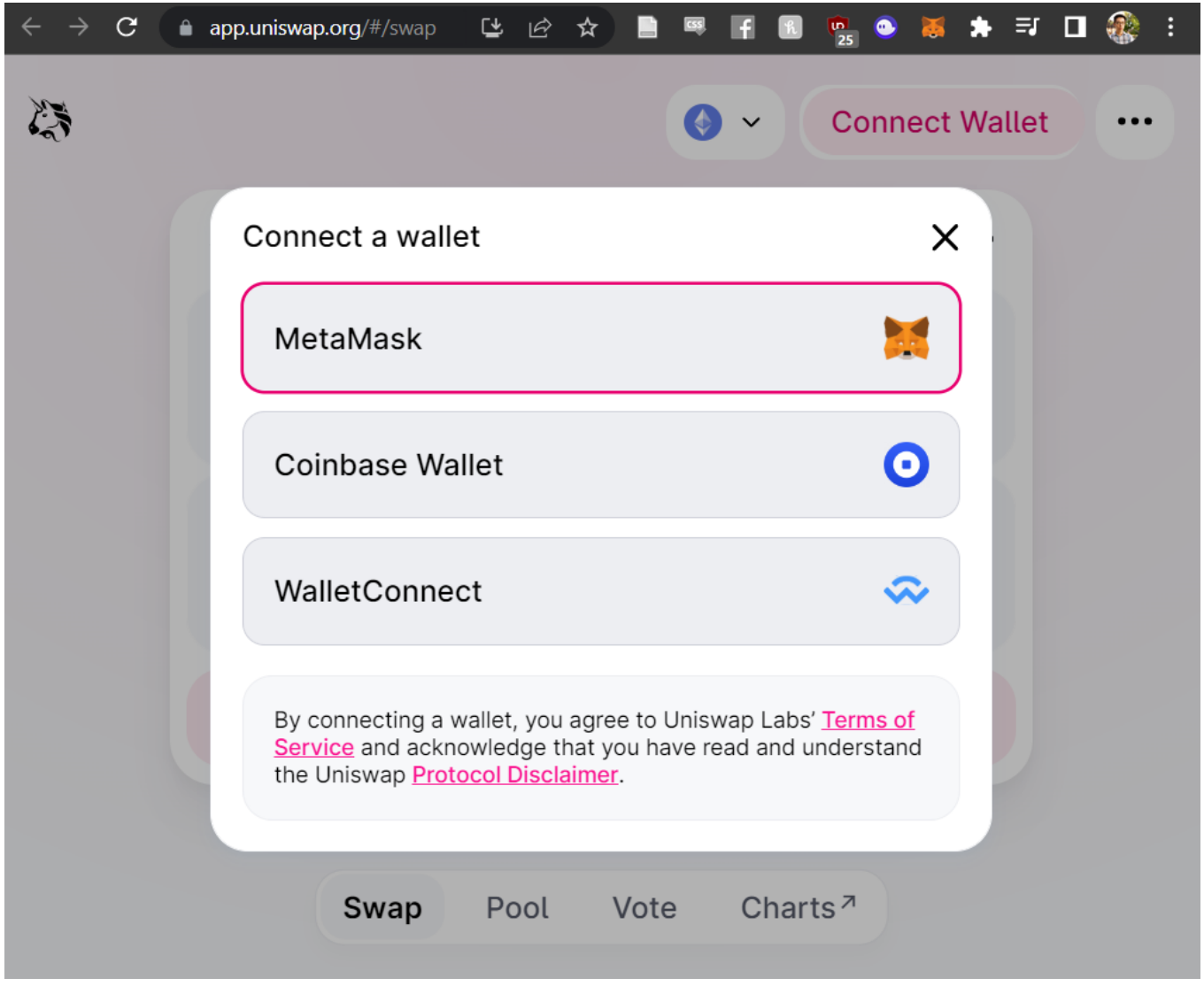
Hardware Wallets

- 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!

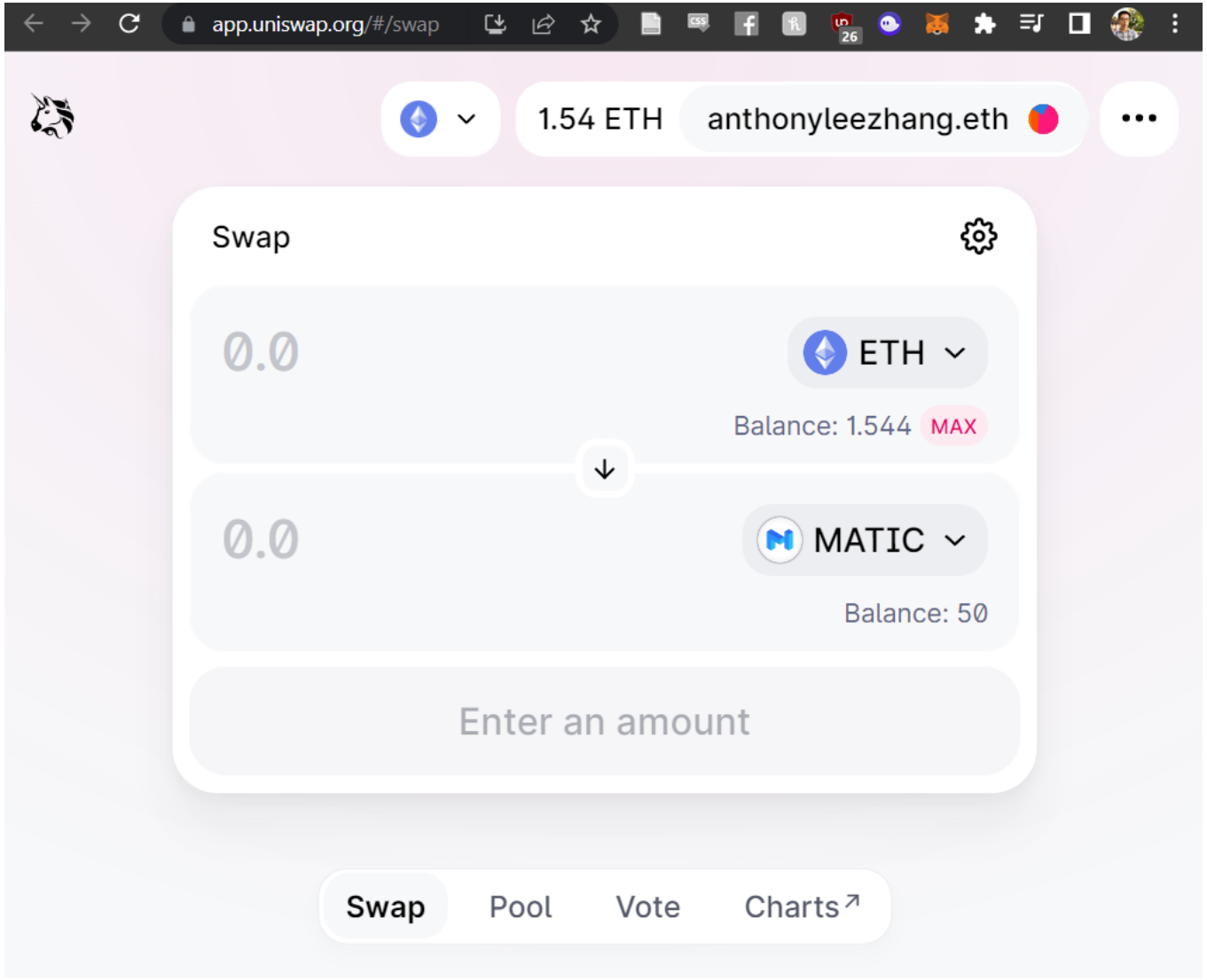
Uniswap Example



Uniswap Example



Uniswap Example



Native Composability

- Web3 (DeFi) gives 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

- Web3 (DeFi) gives 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!

Native Composability

- Web3 (DeFi) gives 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!
- Harder to construct "walled garden ecosystems", lower barriers to entry + less incumbent advantage

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

Project Ideas: User Interfaces, User Experiences

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

- 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?

Faster Horses

Web3 Identity

- What's in a physical wallet?

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

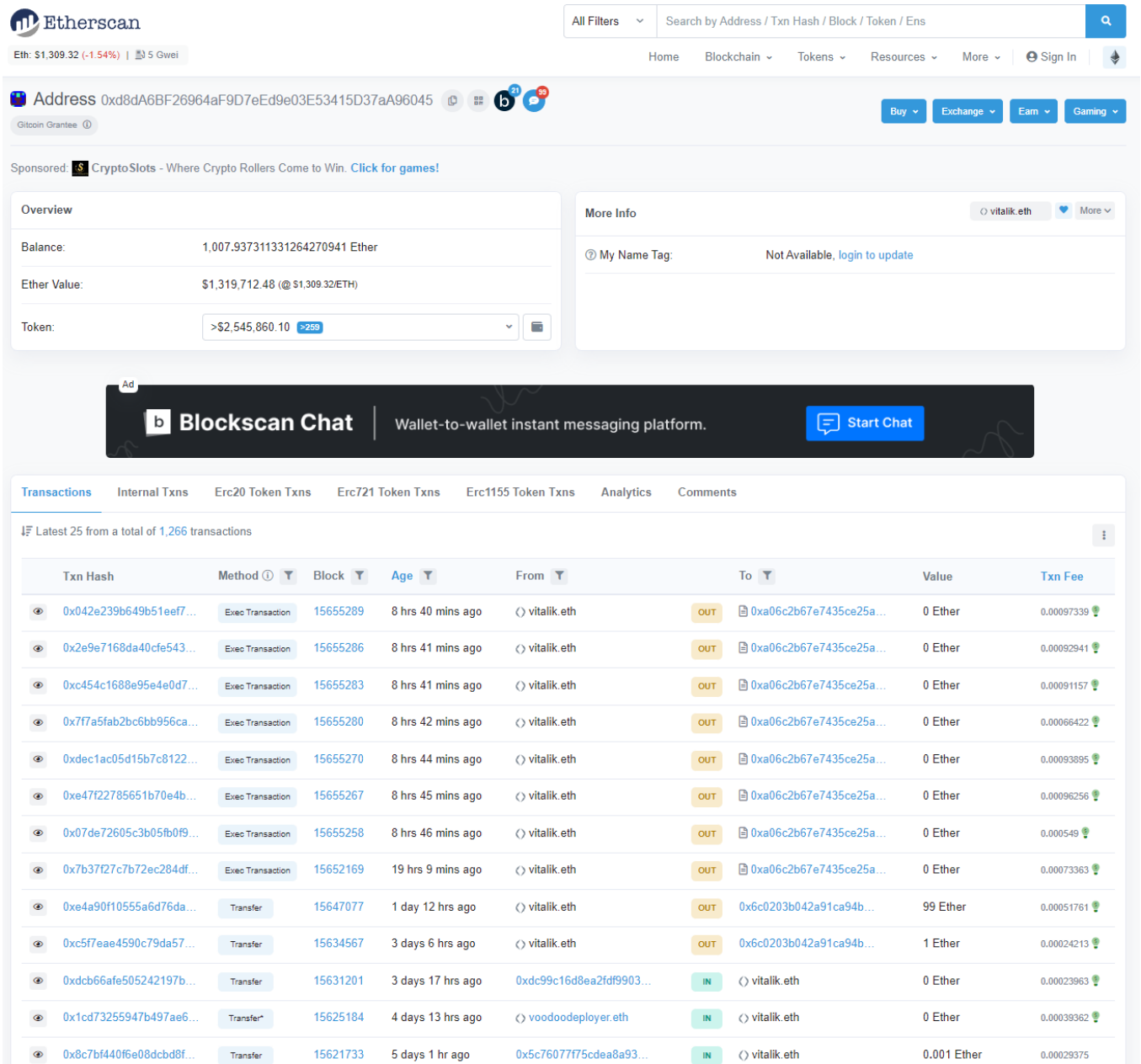
Identity very young, essentially no apps yet, so a good area for class projects! Many taken from WOB paper

- 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?

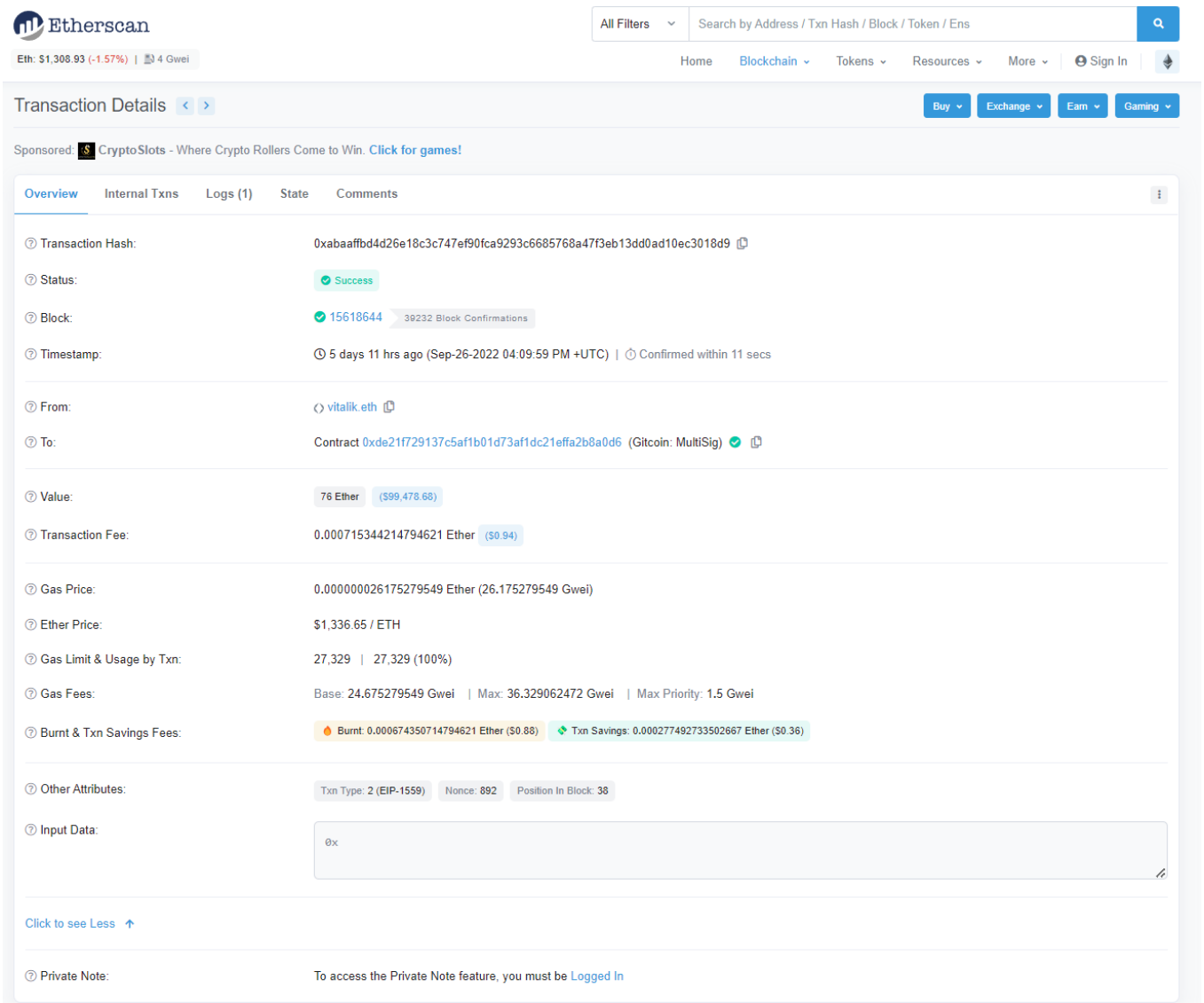
Ethereum Data

- 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

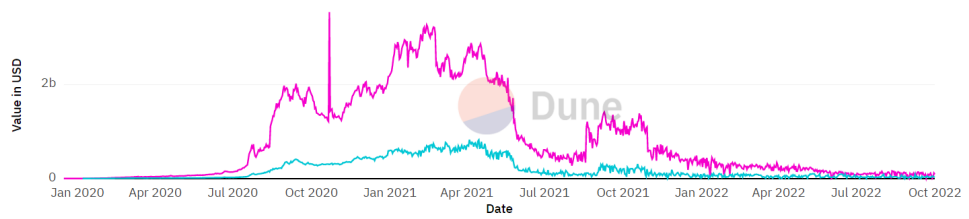
Aave V2 timeseries of total deposits & outstanding loans in USD

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



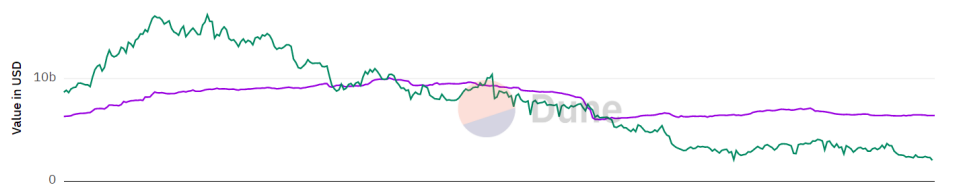
MakerDAO Deposits & Outstanding Loans - Last 12 Months @datanut

Visualization of MakerDAO deposits and outstanding loans over the last year

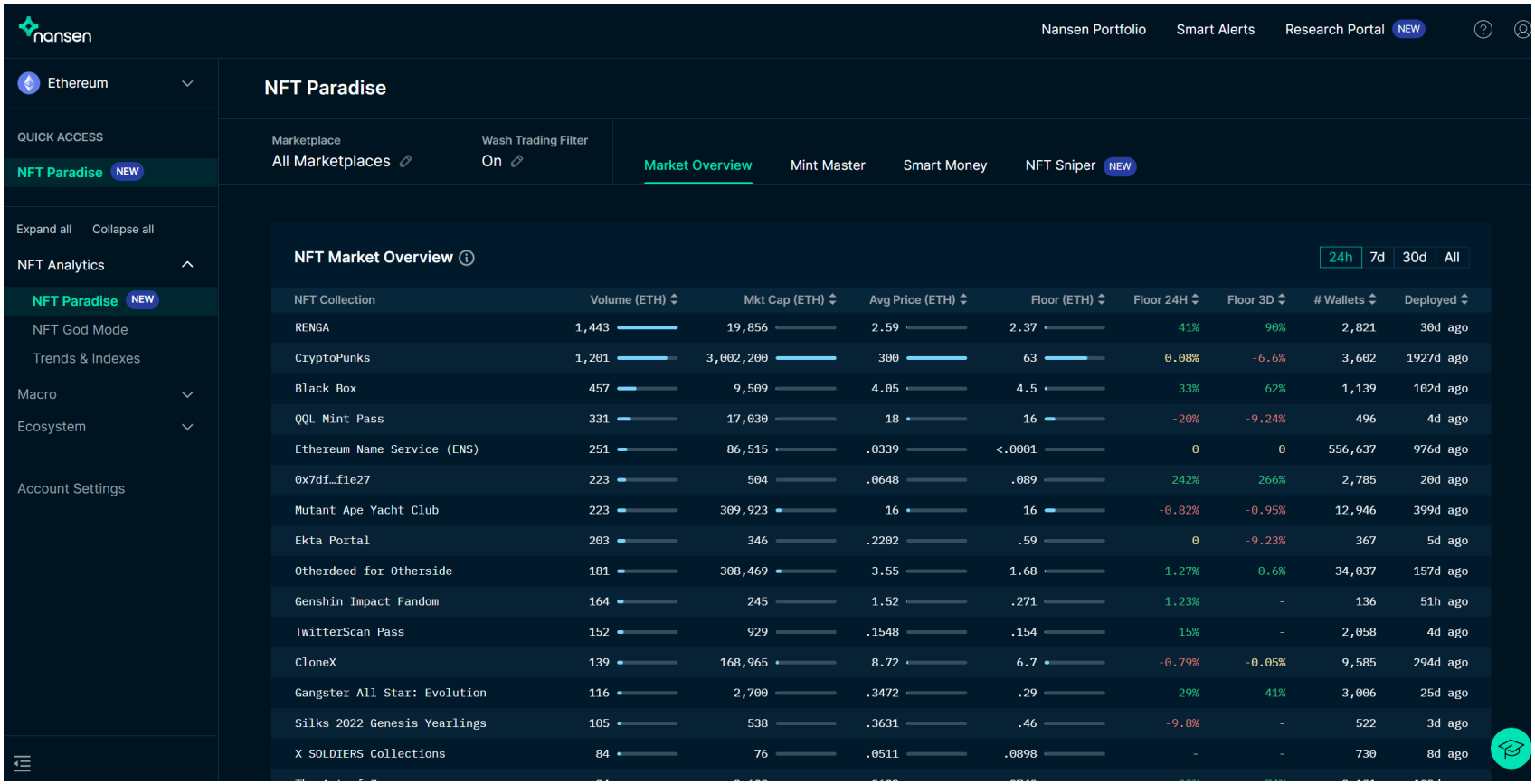
Day	Protocol	Loaned	Deposited
2021-10-02 00:00	MakerDAO	$ 6,318,783,239	$ 8,672,840,061
2021-10-03 00:00	MakerDAO	$ 6,341,056,270	$ 8,870,685,493
2021-10-04 00:00	MakerDAO	$ 6,356,128,722	$ 8,641,122,424
2021-10-05 00:00	MakerDAO	$ 6,386,710,879	$ 8,993,018,165

MakerDAO Deposits & Outstanding Loans - Last 12 Months @datanut

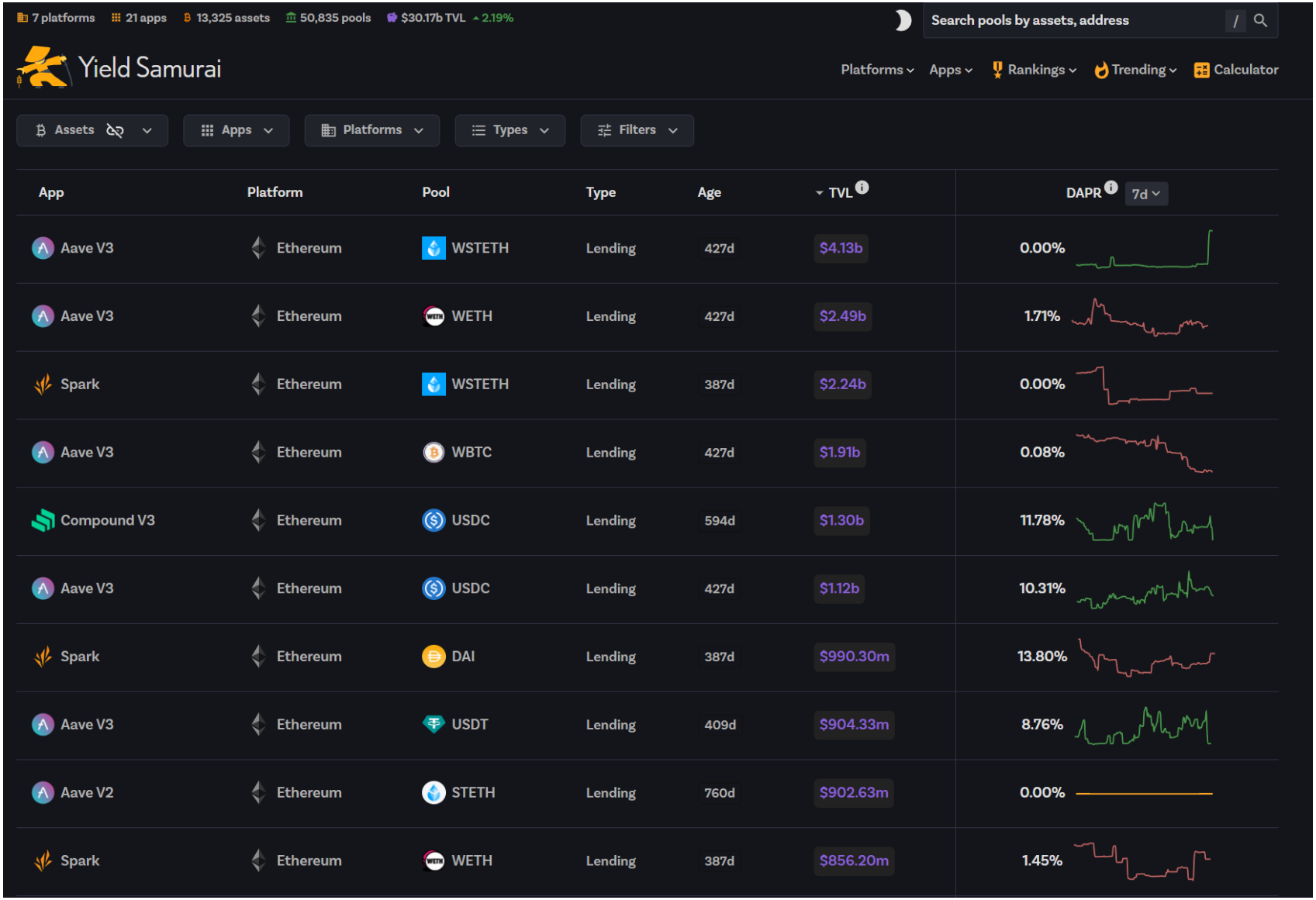
Visualization of MakerDAO deposits and outstanding loans over the last year



Nansen


nansen
Nansen Portfolio
Smart Alerts
Research Portal NEW
Ethereum
QUICK ACCESS
NFT Paradise NEW
Expand all
Collapse all
NFT Analytics
NFT Paradise NEW
NFT God Mode
Trends & Indexes
Macro
Ecosystem
Account Settings
NFT Paradise
Marketplace
All Marketplaces
Wash Trading Filter
On
Market Overview
Mint Master
Smart Money
NFT Sniper NEW
NFT Market Overview
24h 7d 30d All
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

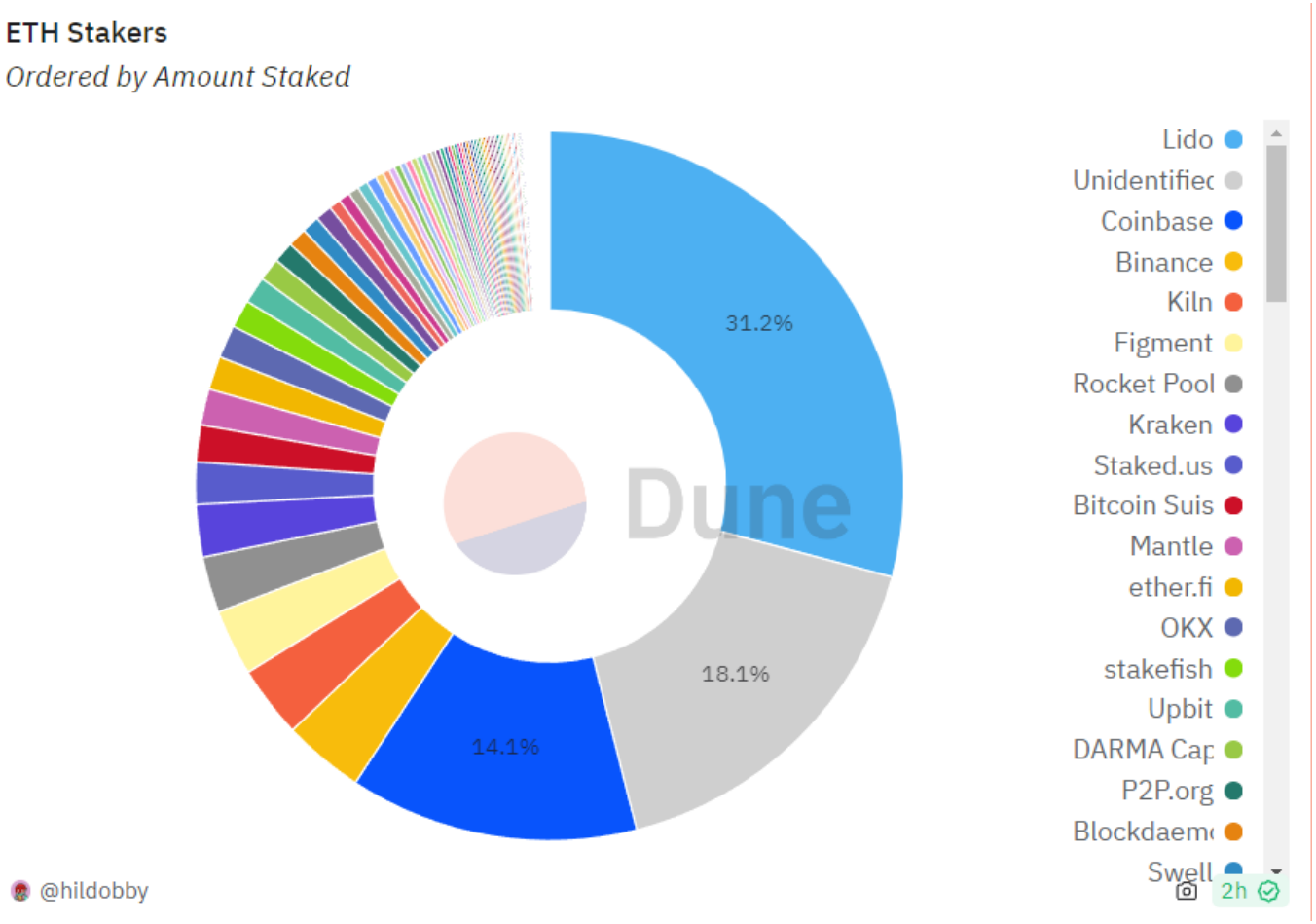
Yield Samurai



Proof of Stake

- Originally, ETH mining proof-of-work, similar to BTC
- On Sept 15 2022, ETH switched to proof of stake – called **"The Merge"**
- Reduced energy consumption by **over 99%**!
- 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

Roadmap

1. Intro
2. History
3. Structure
   - Smart Contracts
4. The Market For Promises
5. Smart Contracts, Cont.
   - Gas Fees
   - Gas
   - User Interface
   - Data
   - Proof of Stake
6. 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

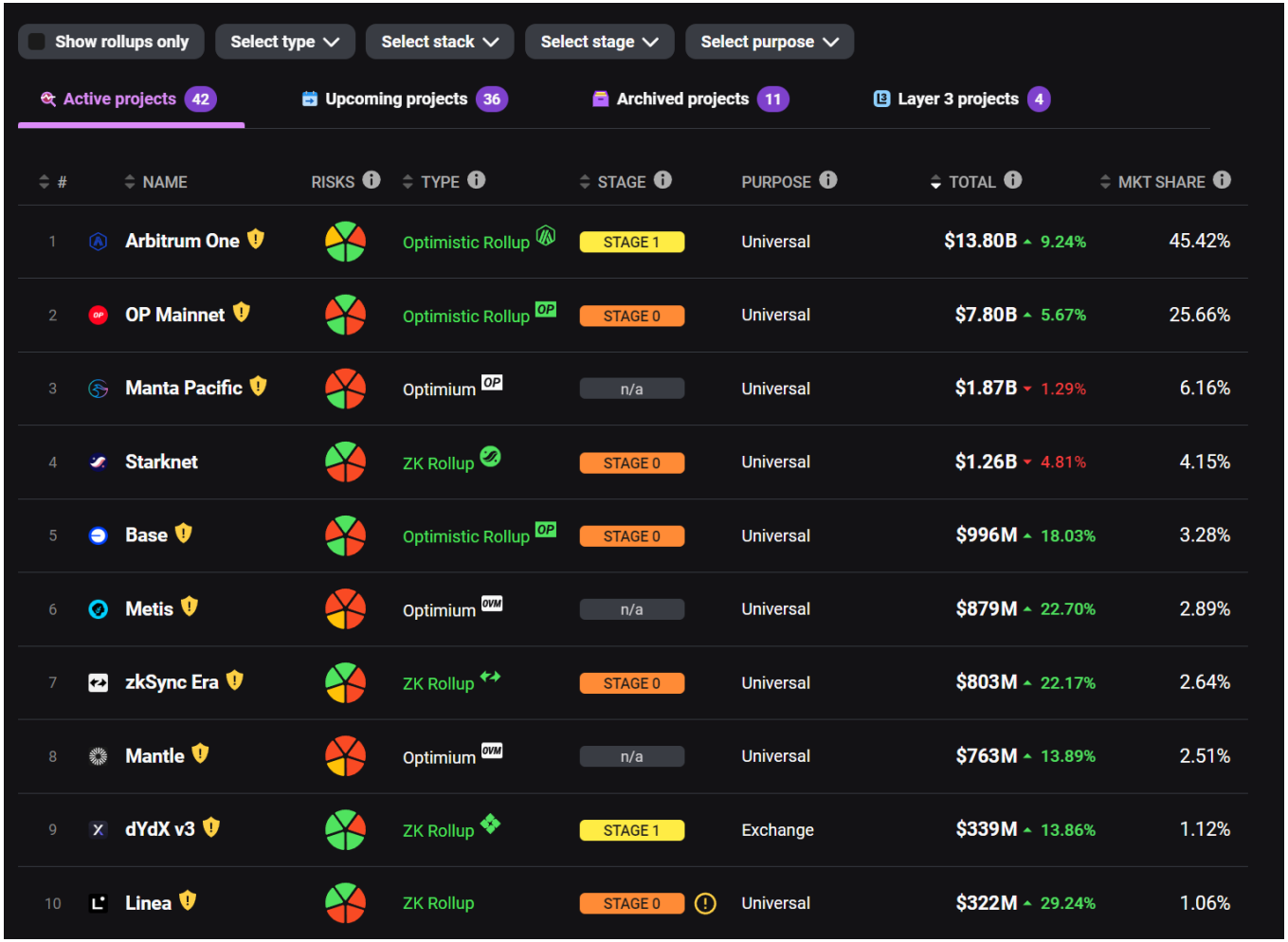
ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- 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



Show rollups only | Select type | Select stack | Select stage | Select purpose

Active projects 42 | Upcoming projects 36 | Archived projects 11 | Layer 3 projects 4

#	NAME	RISKS	TYPE	STAGE	PURPOSE	TOTAL	MKT SHARE
1	Arbitrum One		Optimistic Rollup	STAGE 1	Universal	$13.80B ▲ 9.24%	45.42%
2	OP Mainnet		Optimistic Rollup	STAGE 0	Universal	$7.80B ▲ 5.67%	25.66%
3	Manta Pacific		Optimium	n/a	Universal	$1.87B ▼ 1.29%	6.16%
4	Starknet		ZK Rollup	STAGE 0	Universal	$1.26B ▼ 4.81%	4.15%
5	Base		Optimistic Rollup	STAGE 0	Universal	$996M ▲ 18.03%	3.28%
6	Metis		Optimium	n/a	Universal	$879M ▲ 22.70%	2.89%
7	zkSync Era		ZK Rollup	STAGE 0	Universal	$803M ▲ 22.17%	2.64%
8	Mantle		Optimium	n/a	Universal	$763M ▲ 13.89%	2.51%
9	dYdX v3		ZK Rollup	STAGE 1	Exchange	$339M ▲ 13.86%	1.12%
10	Linea		ZK Rollup	STAGE 0	Universal	$322M ▲ 29.24%	1.06%

Source: L2beat