# Cse190: Blockchain Security

Deian Stefan, Spring 2025

## Introduction

Adopted from CSE 291 (Savage, Stefan) and CS251 (Boneh)

# First, a bit about us…

- Deian Stefan (he/him)
  - PL + Sec; building principled and practical secure systems
  - Have blockchain startup
  - OHs: Monday 6:30pm in CS 3126

- Naomi Smith (she/her)
  - Verification + Sec; more impact on browser security than all of us
  - Born cypherpunk
  - OHs:

- Enze "Alex" Lui (he/him)
  - Sec + measurements; does it all
  - Blockchain bona fides – studying crypto bridge fraud

# Second… why are we teaching this course?

?

# Course objectives

- Learn how things work
  - Important blockchains (e.g., Bitcoin, Ethereum, Solana – most others derivative)
    - What are the core assumptions and objectives
  - The ecosystem they operate in (e.g., exchanges, mixes, bridges, mining pools)
- Learn how they get abused
  - Theft, fraud, money-laundering
    - Technical issues, social engineering, lack of regulator oversight
  - Market manipulation (e.g., frontrunning, wash trading)
  - How these things work, why they work, when they work(ed)
- Understand efforts to manage risk
  - Crypto tracing, regulatory and law enforcement efforts
- Identify the interesting open questions in blockchain security

# Readings and Discussion (10%)

- This is a *reading* and *discussion* class
- We'll be reading/listening to:
  - Academic papers
  - Anonymous white papers
  - Blogs and industry hand-waves
  - Guest speakers
- This will be a **discussion-oriented class**
  - Lecture will cover fundamentals, but you should come to class having read the material
  - We need people to engage with material – ask & respond to questions, **interrupt**, challenge us and each other, etc
  - You will get from this class (and every other class) what you put into it
- Everything will be at: https://cseweb.ucsd.edu/~dstefan/cse190-spring25/
- And class slack: #cse190-sp25-blockchain

# Group Projects (40%)

**Goal:** Get a real feel for working with blockchains

- Groups of at most 3

Project 1: Bitcoin transactions (10%)

Project 2: Payment dapp (15%)

Project 3: DEX (15%)

Expectations: You write the code, you can answer any questions about the code.

# Exams (50%)

- Midterm: 20%
- Final: 30%
  - Resurrection final ⟹ `midterm = final > 0 ? max(final, midterm) : midterm`
- What to expect on exam?
  - What's covered in the reading and lecture
  - Goal: Forcing function for really understanding the material
  - No open laptop/book, but you can bring 2-page cheatsheet

# Let's talk about LLMs

# Quick check in

- What are you hoping to get from this course?

- How much do you know about blockchains/crypto?
  - Have some idea what a blockchain is?
  - Could roughly explain how Bitcoin mining works and what its for?
  - Could explain the difference between a cryptocurrency and an NFT?
  - Have heard of Ethereum?
  - Know what the EVM is and can program in Solidity?
  - Understand how Proof of Stake works?
  - Can explain the difference between a bridge and an exchange?

# Some history on how we got here

- Two predominant forms of consumer payment in the early 20th century
  - Cash and coinage – minted by government (in US authority from Article I, Section 8)
  - Checks – three party promissory note (from payers account at regulated bank to payee)
  - Cash largely anonymous, checks… not so much

- In 1950 Diners Club introduces charge card; then Amex (1958), Bank of America (1966 – becomes Visa), Interbank (1966 – becomes Mastercard)
  - On-demand consumer credit offered on behalf of consumer
    - Funded based on fees on transactions (a couple percent) and interest on overdue repayment
  - Today, credit cards (and debit, closer to check) dominate consumer payments
  - Hugely centralized in practice
- In 1983 David Chaum proposes anonymous eCash guaranteed via crypto
  - Used online blind signatures with 3rd party; later did offline version with Moni Naor
  - Founded DigiCash (Nicholas Negroponte was chairman) to offer anonymous cash payments
    - Never took off, bankrupt in 1998

# Some history on how we got here

- 1979 – Merkle comes up with the idea of a Merkle hash tree
  - Every non-leaf labelled with cryptographic hash of its children; easy to show in log time that a given leaf is part of data structure from the root
- 1992 Bayer, Haber & Stornetta & Bayer – how to use Merkle trees to "time-stamp" documents cryptographically
  - In use since 1995 by Surety Inc – arguably first "blockchain"
- 1993 Moni Naor and Cynthia Dwork invent "proof of work"
  - Cryptgraphic evidence that a certain amount of work has been done; originally proposed as a defense against spam
  - 1997, Adam Back proposes hashcash PoW algorithm using SHA-1 hashes with certain number of zeros
  - 2004, Hal Finey extends to "reusable proof of work" for digital tokens (i.e., uses trusted server to track "ownership" to avoid double spending)
- Lots of effort in 90s to try to develop low-transaction cost ecash (particularly on cypherpunks mailing list) as mechanism to pay for Web (in lieu of ads)
- In late 90s early 2000s, lots of work in research community on peer-to-peer protocols for distributed storage

lentless attacks on news coverage that he does not like, and has long expressed hostility toward traditional press freedoms. He has vowed to "open up" the nation's libel laws, even though those statutes are in fact state, not federal, laws.

NOTICES & LOST AND FOUND (5100-5102)

Universal Registry Entries:
Zone 2–
ITKb/LUUVC2trMOSeFFeb
DUB53nuP08bnm13ui0+X2INbMb
569vU57v44EIBcecE/hAZQ==
Zone 3–
IVQVu/spL6/oB/5VsIV/jK9CGW
ba39iMRIUO2EakjFWDMliKLBK
paQ1KPjRqa9vzM+dn6A==
These base64-encoded values represent the combi... digital records f... tween 20180808... www.surety.com

pc
ati... already complica... with the preside... Trump has foug... Gahn as much a... top aides, White... have said, both... fited significantl... nership.

Mr. McGahn ... of Mr. Trump's ... plishments — s... courts and cu... regulations — ... champion of c... process.

But the two ... one — the W...

The first blockchain

# Bitcoin

- Oct 31, 2008, Satoshi Nakamura (pseudonym) releases white paper
  - Roughly describes how to combine ideas of PoW, Haber/Merkle attestation, and a distributed peer-to-peer gossip protocol to create Bitcoin
  - Initial implementation released to public in January 2009
- After slow start, interest explodes
  - Today (April 1, 2024), a single Bitcoin exchanges with the USD for over $83k, the total market cap is 1.65T USD and an estimated trading volume of $29B (in last day)
  - Massive venture capital investment
  - There are now roughly 10K+ "active" cryptocurrencies
    - Some (starting with Ethereum) embedded Turing-complete computation (so-called "smart contracts")
  - Blockchains also start to be used to represent ownership in unique (non-fungible) digital objects (i.e., NFTs)

# What is a blockchain?

Abstract answer: Technology that provides coordination between many parties, with no single trusted party

2009

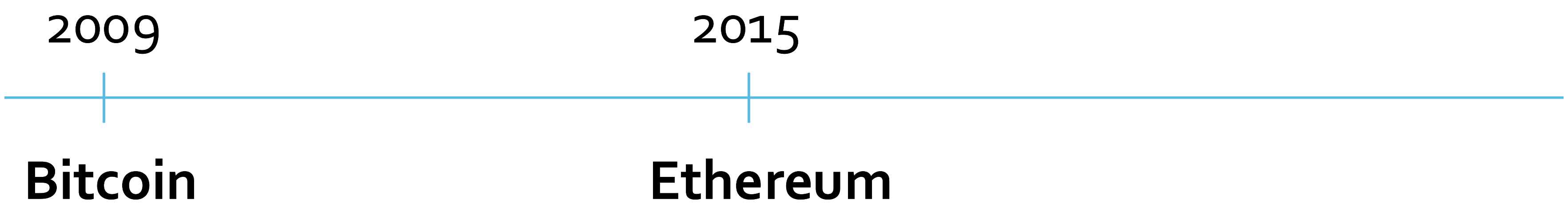
**Bitcoin**

A practical **public append-only data structure**, secured by replication and financial incentives

A fixed supply asset (BTC). Digital payments, and more.

# What is a blockchain?

Abstract answer: Technology that provides coordination between many parties, with no single trusted party



2009 2015

**Bitcoin** **Ethereum**

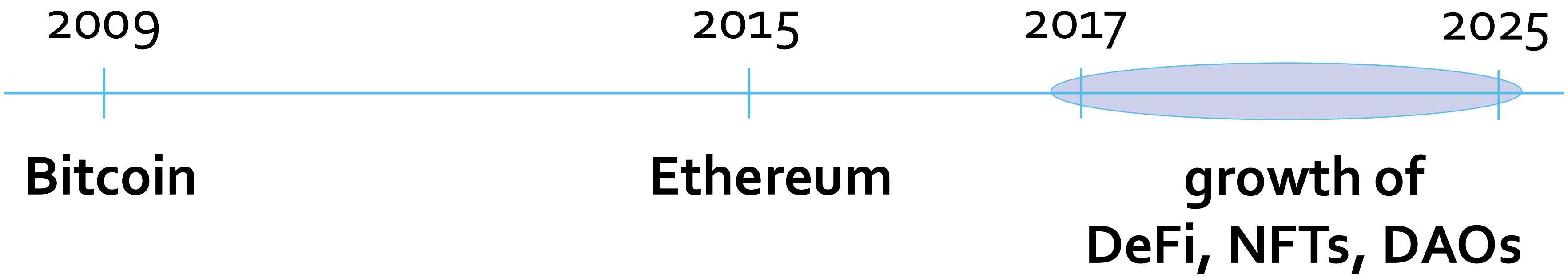
**Blockchain computer**: a fully programmable environment

⟹ public programs that manage digital and financial assets

Composability: applications running on chain can call each other

# What is a blockchain?

Abstract answer: Technology that provides coordination between many parties, with no single trusted party



2009 2015 2017 2025

**Bitcoin**

**Ethereum**

**growth of**
**DeFi, NFTs, DAOs**

**DeFi**: financial instruments managed by public programs

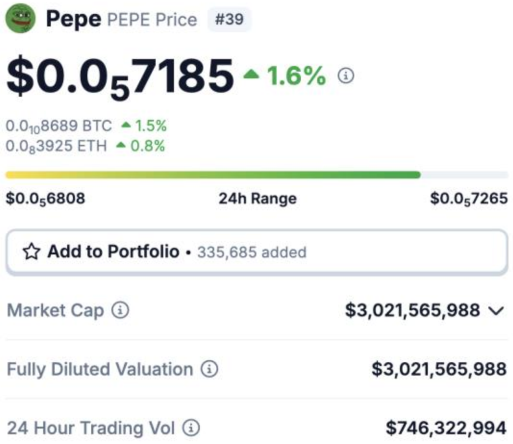
⟹ stablecoins, lending, exchanges, ....

Asset management (**NFTs**): art, game assets, domain names.

Decentralized organizations (**DAOs**): decentralized governance

# Why?

- Libertarian interests
  - Replacement for money without government oversight
    - Medium of exchange, store of value, unit of account
  - Free from regulation and anonymous (even from govt)
- Speculative interests
  - Who knows why crypto is valuable, but it's going to the moon!  HODL!



Pepe PEPE Price #39

$\$0.0_{5}7185$ ▲1.6%

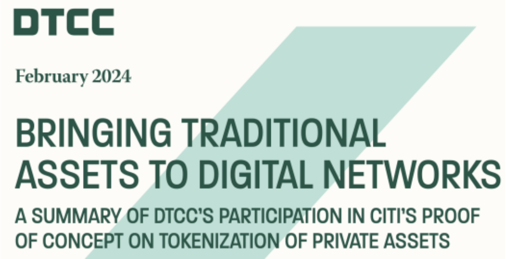
$0.0_{10}8689$ BTC ▲1.5%
$0.0_{8}3925$ ETH ▲0.8%

| $\$0.0_{5}6808$ | 24h Range | $\$0.0_{5}7265$ |
|---|---|---|

☆ Add to Portfolio • 335,685 added

| | |
|---|---|
| Market Cap | $3,021,565,988 |
| Fully Diluted Valuation | $3,021,565,988 |
| 24 Hour Trading Vol | $746,322,994 |

- Reaction against high transaction costs and slow innovation in Western (particularly US) financial system
  - e.g., no real-time settlement
- Resisting inflation/capital controls in certain countries
  - i.e., Global South



DTCC

February 2024

BRINGING TRADITIONAL ASSETS TO DIGITAL NETWORKS

A SUMMARY OF DTCC'S PARTICIPATION IN CITI'S PROOF OF CONCEPT ON TOKENIZATION OF PRIVATE ASSETS

- Raw techno-optimism?  Others?

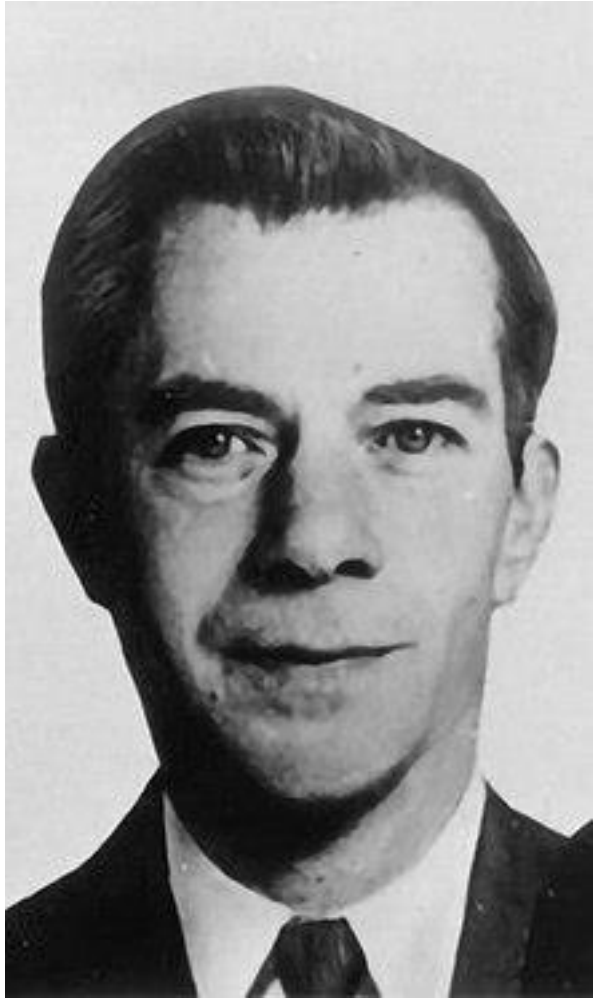
# Properties of blockchains that people seem to want

- **Safety** – both that records are immutable, but also that transactions cannot be manipulated to modify outcomes (e.g., your money goes away, your orders go to someone else, etc.)
  - Related: decentralized trust (otherwise, use a database)
- **Decentralization** – that no small number of parties can control the blockchain
- **Accountability** – if fraud, you can pursue legal challenges against counterparty (note, hardcore libertarians don't want this)
- **Efficiency/fairness** – low cost of use and no favorites among users
- **Usability** – easy to use and understand what you're doing and its consequences

- Crypto has been mostly terrible at all of these so far…

When asked why he robbed banks, Willie Sutton is said to have replied, "*Because that's where the money is*."[*]

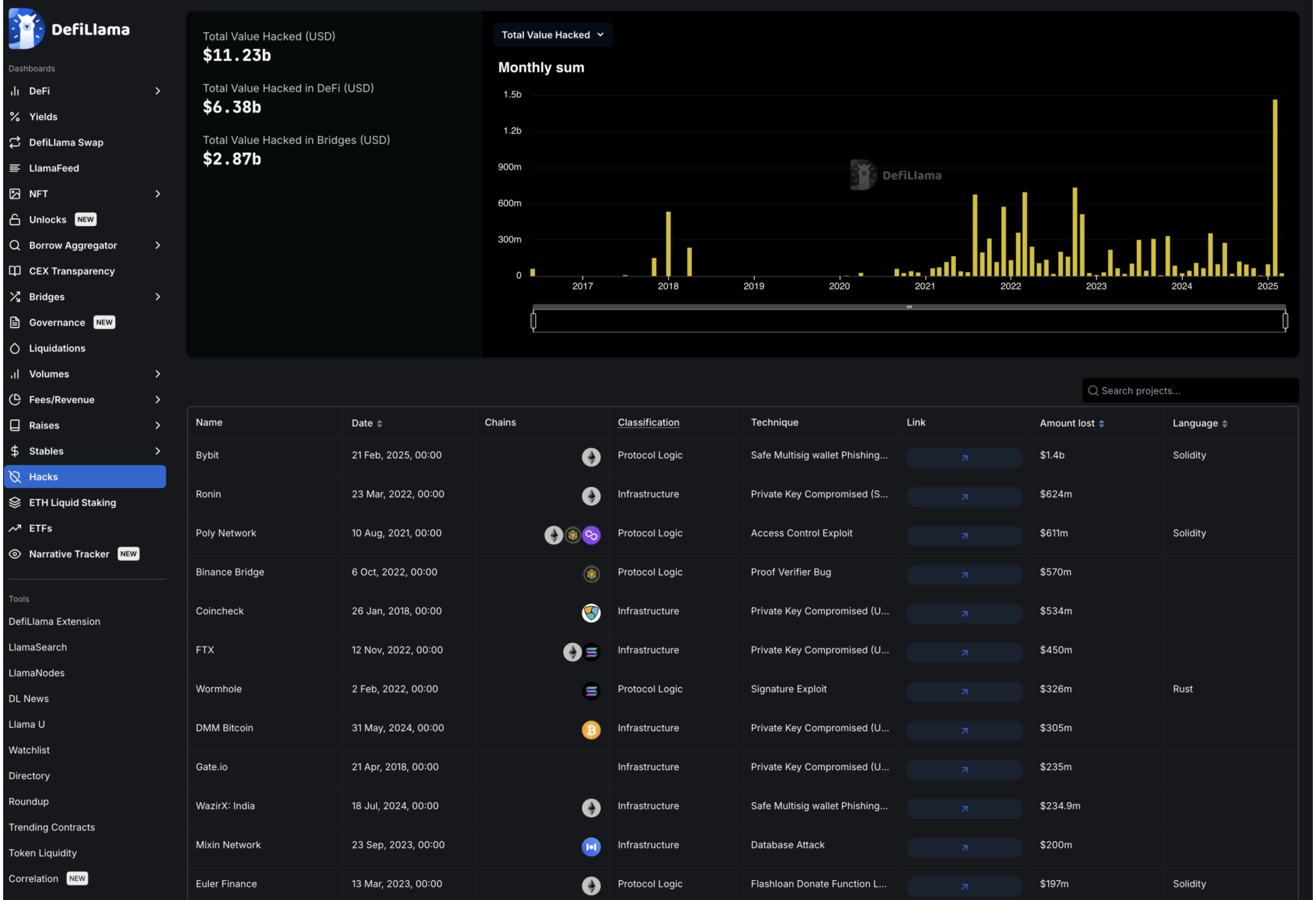
But today the money is on a blockchain…



[*] This story is widely repeated, but is apocryphal, and ironically morphed into "Sutton's Law" which is used to teach doctors to start diagnosis with the most obvious possibility.

# Largest physical bank robbery in US history

- 1997 Dunbar Armored facility in Los Angeles
  - Total Ocean’s 11 operation; insider, timed to avoid video; attacked when vault was open, high-denomination non-sequential bills; pre-planned alibi, etc
  - Waited 6mos to launder funds via front companies and real estate
- Stole 18.9M
- All perpetrators eventually caught and convicted, but only a third of the money recovered (~$14M unaccounted for)
- All bank customers made whole (i.e., losses borne by bank and insurer)

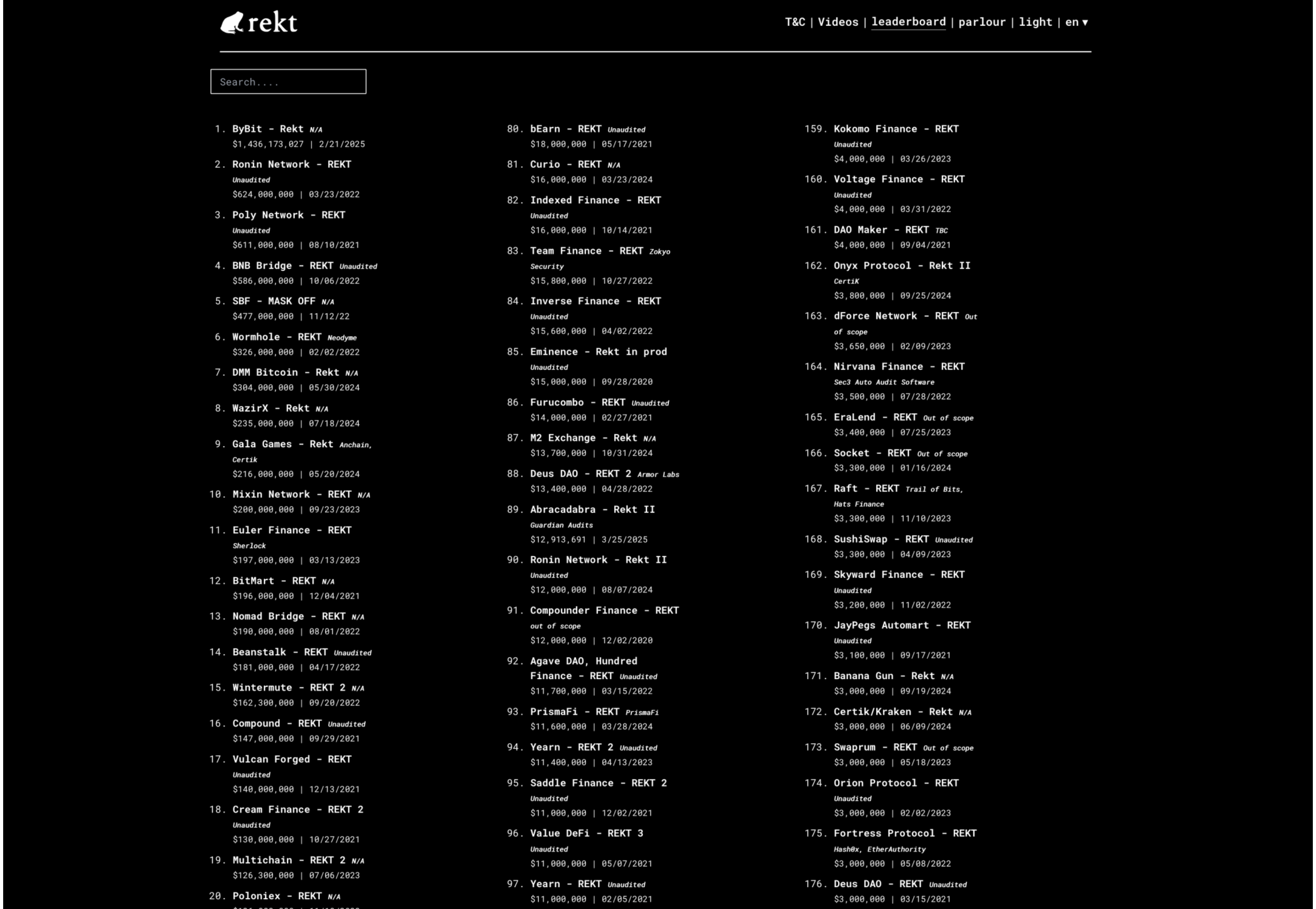


Total Value Hacked (USD)
**$11.23b**

Total Value Hacked in DeFi (USD)
**$6.38b**

Total Value Hacked in Bridges (USD)
**$2.87b**

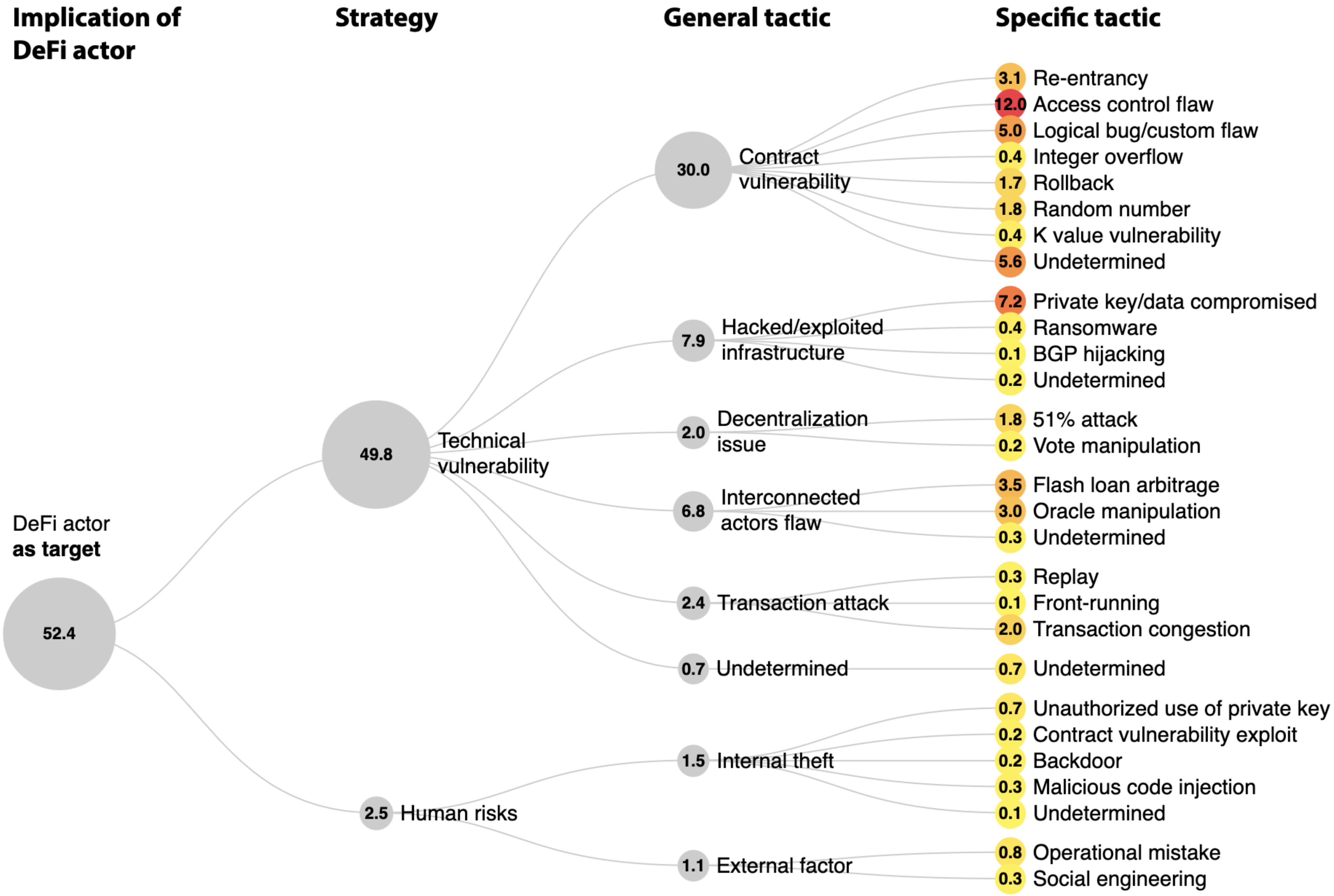
| Name | Date | Chains | Classification | Technique | Link | Amount lost | Language |
|---|---|---|---|---|---|---|---|
| Bybit | 21 Feb, 2025, 00:00 | | Protocol Logic | Safe Multisig wallet Phishing... | ↗ | $1.4b | Solidity |
| Ronin | 23 Mar, 2022, 00:00 | | Infrastructure | Private Key Compromised (S... | ↗ | $624m | |
| Poly Network | 10 Aug, 2021, 00:00 | | Protocol Logic | Access Control Exploit | ↗ | $611m | Solidity |
| Binance Bridge | 6 Oct, 2022, 00:00 | | Protocol Logic | Proof Verifier Bug | ↗ | $570m | |
| Coincheck | 26 Jan, 2018, 00:00 | | Infrastructure | Private Key Compromised (U... | ↗ | $534m | |
| FTX | 12 Nov, 2022, 00:00 | | Infrastructure | Private Key Compromised (U... | ↗ | $450m | |
| Wormhole | 2 Feb, 2022, 00:00 | | Protocol Logic | Signature Exploit | ↗ | $326m | Rust |
| DMM Bitcoin | 31 May, 2024, 00:00 | | Infrastructure | Private Key Compromised (U... | ↗ | $305m | |
| Gate.io | 21 Apr, 2018, 00:00 | | Infrastructure | Private Key Compromised (U... | ↗ | $235m | |
| WazirX: India | 18 Jul, 2024, 00:00 | | Infrastructure | Safe Multisig wallet Phishing... | ↗ | $234.9m | |
| Mixin Network | 23 Sep, 2023, 00:00 | | Infrastructure | Database Attack | ↗ | $200m | |
| Euler Finance | 13 Mar, 2023, 00:00 | | Protocol Logic | Flashloan Donate Function L... | ↗ | $197m | Solidity |



1. **ByBit - Rekt** *N/A*
   $1,436,173,027 | 2/21/2025
2. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
3. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
4. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
5. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
6. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
7. **DMM Bitcoin - Rekt** *N/A*
   $304,000,000 | 05/30/2024
8. **WazirX - Rekt** *N/A*
   $235,000,000 | 07/18/2024
9. **Gala Games - Rekt** *Anchain, Certik*
   $216,000,000 | 05/20/2024
10. **Mixin Network - REKT** *N/A*
    $200,000,000 | 09/23/2023
11. **Euler Finance - REKT** *Sherlock*
    $197,000,000 | 03/13/2023
12. **BitMart - REKT** *N/A*
    $196,000,000 | 12/04/2021
13. **Nomad Bridge - REKT** *N/A*
    $190,000,000 | 08/01/2022
14. **Beanstalk - REKT** *Unaudited*
    $181,000,000 | 04/17/2022
15. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022
16. **Compound - REKT** *Unaudited*
    $147,000,000 | 09/29/2021
17. **Vulcan Forged - REKT** *Unaudited*
    $140,000,000 | 12/13/2021
18. **Cream Finance - REKT 2** *Unaudited*
    $130,000,000 | 10/27/2021
19. **Multichain - REKT 2** *N/A*
    $126,300,000 | 07/06/2023
20. **Poloniex - REKT** *N/A*

80. **bEarn - REKT** *Unaudited*
    $18,000,000 | 05/17/2021
81. **Curio - REKT** *N/A*
    $16,000,000 | 03/23/2024
82. **Indexed Finance - REKT** *Unaudited*
    $16,000,000 | 10/14/2021
83. **Team Finance - REKT** *Zokyo Security*
    $15,800,000 | 10/27/2022
84. **Inverse Finance - REKT** *Unaudited*
    $15,600,000 | 04/02/2022
85. **Eminence - Rekt in prod** *Unaudited*
    $15,000,000 | 09/28/2020
86. **Furucombo - REKT** *Unaudited*
    $14,000,000 | 02/27/2021
87. **M2 Exchange - Rekt** *N/A*
    $13,700,000 | 10/31/2024
88. **Deus DAO - REKT 2** *Armor Labs*
    $13,400,000 | 04/28/2022
89. **Abracadabra - Rekt II** *Guardian Audits*
    $12,913,691 | 3/25/2025
90. **Ronin Network - Rekt II** *Unaudited*
    $12,000,000 | 08/07/2024
91. **Compounder Finance - REKT** *out of scope*
    $12,000,000 | 12/02/2020
92. **Agave DAO, Hundred Finance - REKT** *Unaudited*
    $11,700,000 | 03/15/2022
93. **PrismaFi - REKT** *PrismaFi*
    $11,600,000 | 03/28/2024
94. **Yearn - REKT 2** *Unaudited*
    $11,400,000 | 04/13/2023
95. **Saddle Finance - REKT 2** *Unaudited*
    $11,000,000 | 12/02/2021
96. **Value DeFi - REKT 3** *Unaudited*
    $11,000,000 | 05/07/2021
97. **Yearn - REKT** *Unaudited*
    $11,000,000 | 02/05/2021

159. **Kokomo Finance - REKT** *Unaudited*
     $4,000,000 | 03/26/2023
160. **Voltage Finance - REKT** *Unaudited*
     $4,000,000 | 03/31/2022
161. **DAO Maker - REKT** *TBC*
     $4,000,000 | 09/04/2021
162. **Onyx Protocol - Rekt II** *CertiK*
     $3,800,000 | 09/25/2024
163. **dForce Network - REKT** *Out of scope*
     $3,650,000 | 02/09/2023
164. **Nirvana Finance - REKT** *Sec3 Auto Audit Software*
     $3,500,000 | 07/28/2022
165. **EraLend - REKT** *Out of scope*
     $3,400,000 | 07/25/2023
166. **Socket - REKT** *Out of scope*
     $3,300,000 | 01/16/2024
167. **Raft - REKT** *Trail of Bits, Hats Finance*
     $3,300,000 | 11/10/2023
168. **SushiSwap - REKT** *Unaudited*
     $3,300,000 | 04/09/2023
169. **Skyward Finance - REKT** *Unaudited*
     $3,200,000 | 11/02/2022
170. **JayPegs Automart - REKT** *Unaudited*
     $3,100,000 | 09/17/2021
171. **Banana Gun - Rekt** *N/A*
     $3,000,000 | 09/19/2024
172. **Certik/Kraken - Rekt** *N/A*
     $3,000,000 | 06/09/2024
173. **Swaprum - REKT** *Out of scope*
     $3,000,000 | 05/18/2023
174. **Orion Protocol - REKT** *Unaudited*
     $3,000,000 | 02/02/2023
175. **Fortress Protocol - REKT** *Hash0x, EtherAuthority*
     $3,000,000 | 05/08/2022
176. **Deus DAO - REKT** *Unaudited*
     $3,000,000 | 03/15/2021



**Implication of DeFi actor** | **Strategy** | **General tactic** | **Specific tactic**

- 52.4 DeFi actor **as target**
  - 49.8 Technical vulnerability
    - 30.0 Contract vulnerability
      - 3.1 Re-entrancy
      - 12.0 Access control flaw
      - 5.0 Logical bug/custom flaw
      - 0.4 Integer overflow
      - 1.7 Rollback
      - 1.8 Random number
      - 0.4 K value vulnerability
      - 5.6 Undetermined
    - 7.9 Hacked/exploited infrastructure
      - 7.2 Private key/data compromised
      - 0.4 Ransomware
      - 0.1 BGP hijacking
      - 0.2 Undetermined
    - 2.0 Decentralization issue
      - 1.8 51% attack
      - 0.2 Vote manipulation
    - 6.8 Interconnected actors flaw
      - 3.5 Flash loan arbitrage
      - 3.0 Oracle manipulation
      - 0.3 Undetermined
    - 2.4 Transaction attack
      - 0.3 Replay
      - 0.1 Front-running
      - 2.0 Transaction congestion
    - 0.7 Undetermined
      - 0.7 Undetermined
  - 2.5 Human risks
    - 1.5 Internal theft
      - 0.7 Unauthorized use of private key
      - 0.2 Contract vulnerability exploit
      - 0.2 Backdoor
      - 0.3 Malicious code injection
      - 0.1 Undetermined
    - 1.1 External factor
      - 0.8 Operational mistake
      - 0.3 Social engineering

https://arxiv.org/pdf/2310.04356.pdf

# Some ways cryptocurrencies get abused

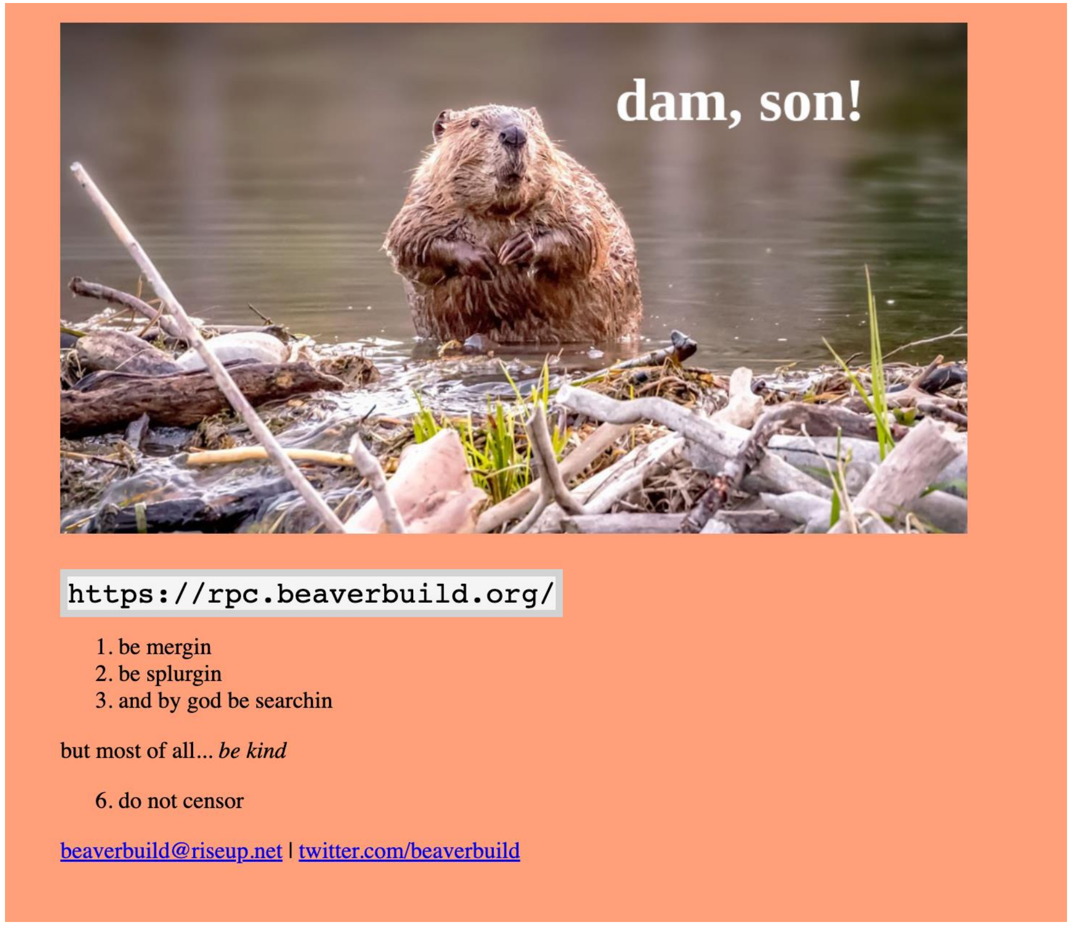
- Theft
  - Private keys
    - Stolen from end system (unhosted wallet), stolen from exchange (hosted wallet), guessed passphrase (brain wallets)
    - Private keys allow transfers; no ability to reverse such a transfer
  - Defraud automated transaction
    - X pays Y in units of Z; if transaction protocol can be fooled/confused money may get transferred event without keys being stolen (e.g., bridge scams or bugs in smart contracts)
    - Alternatively, if hosted wallet (e.g., Coinbase) compromise site authentication (e.g., via SIM swapping) and transfer out money. Same for new kinds of unhosted wallets (e.g., Privy users SIM swapped)
    - Or, just backdoor UI supply chain for Ledger, Safe, etc. to confuse user into signing arbitrary payloads
- Fraudulent representations
  - Convince investors to invest in new crypto endeavor (ICO); take money; abandon new coin (aka rug pull)
  - High yield investment scams (Ponzi and otherwise; promise high yield); may involve impersonation
  - Misrepresent whether investment assets are kept liquid or used for investment (e.g., FTX)
  - Pump and dump; fraudulent activity to make crypto coin X look hot (e.g., wash trades); attacker sells into artificially inflated market
  - Sale of “fake” NFTs etc to unsuspecting parties

# Some ways cryptocurrencies get abused

- Manipulating transaction execution
  - Transaction ordering (e.g., front running)
  - Arbitrage games via manipulating price oracles
  - Manipulating consensus protocol
  - Manipulating DeFi protocol (e.g., flash loans and AMMs)
- Cryptojacking
  - Malware/Websites that use your compute power to mine crypto for third parties
- Use in illegal activity
  - Widely used for victim to criminal payment (e.g., ransomware, pig butchering, blackmail)
  - Widely use for criminal-to-criminal payment (fee for service)
  - Used for some illicit transactions (e.g., drugs)
  - Money laundering vehicle for non-crypto assets

# It's the wild west out there… seriously

50% of all Ethereum blocks are constructed by this guy



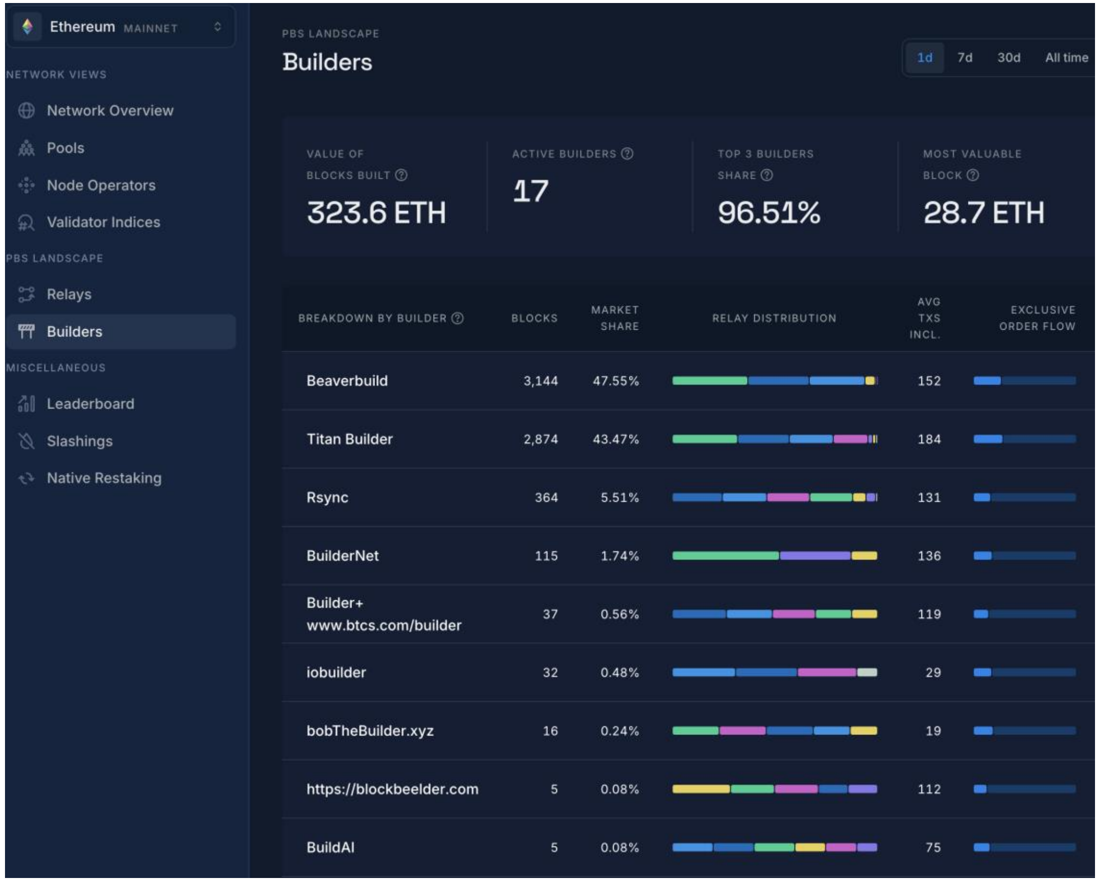
```
https://rpc.beaverbuild.org/
```

1. be mergin
2. be splurgin
3. and by god be searchin

but most of all... *be kind*

6. do not censor

beaverbuild@riseup.net | twitter.com/beaverbuild



PBS LANDSCAPE

## Builders

| VALUE OF BLOCKS BUILT | ACTIVE BUILDERS | TOP 3 BUILDERS SHARE | MOST VALUABLE BLOCK |
|---|---|---|---|
| 323.6 ETH | 17 | 96.51% | 28.7 ETH |

| BREAKDOWN BY BUILDER | BLOCKS | MARKET SHARE | RELAY DISTRIBUTION | AVG TXS INCL. | EXCLUSIVE ORDER FLOW |
|---|---|---|---|---|---|
| Beaverbuild | 3,144 | 47.55% | | 152 | |
| Titan Builder | 2,874 | 43.47% | | 184 | |
| Rsync | 364 | 5.51% | | 131 | |
| BuilderNet | 115 | 1.74% | | 136 | |
| Builder+ www.btcs.com/builder | 37 | 0.56% | | 119 | |
| iobuilder | 32 | 0.48% | | 29 | |
| bobTheBuilder.xyz | 16 | 0.24% | | 19 | |
| https://blockbeelder.com | 5 | 0.08% | | 112 | |
| BuildAI | 5 | 0.08% | | 75 | |

# Tentative syllabus

- Bitcoin
- Ethereum and EVM
- DeFi
- MEV
- Mixers
- Bridges

# For next time

- Intro to cryptography
- Read Bitcoin: A Peer-to-Peer Electronic Cash System, by Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf), and some of the sections from site
- Start looking around for who you might like to be in a group with
- Think about what crypto questions/interests you have (related to security/abuse) and bring them! Syllabus is still open!