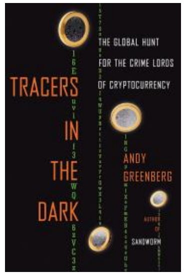
Cse291-J: Blockchain Security

Deian Stefan and Stefan Savage, Spring 2024

Introduction

First, a bit about us…

- Stefan Savage
  - Empirical security, trying to measure/infer how things work
  - Largely deconstructive (how things work now)
  - Blockchain bona fides – helped with early crypto tracing work
  - Old



- Deian Stefan
  - PL + Sec; building principled and practical secure systems
  - Largely constructive (how things should work)
  - Blockchain bona fides – has blockchain startup and Stanford Ph.D.
  - Young

cubist™

- Enze "Alex" Lui
  - Does it all
  - Blockchain bona fides – studying crypto bridge fraud
  - Timeless

Second… why are we teaching this course?

?

Course objectives

- Learn how things work
  - Important blockchains (e.g., Bitcoin and Ethereum – 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

- 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 (more on this in a sec)
- This will be a **discussion-oriented class**
  - This is particularly important because Deian and I barely know what we're talking about
  - We need people to engage with material – ask & respond to questions, **interrupt**, challenge us and each other, etc
  - You will get from this class what you put into it
- Everything will be at: https://cseweb.ucsd.edu/~dstefan/cse291-spring24/

Invited speakers (so far)

- David Anderson, Professor, CMU
  - Crazy crypto was Dave's side hustle during the early post-Bitcoin era
  - This will be the first time he tells the crazy stories from the trenches

- Nicolas Christin, Professor, CMU
  - Nicholas co-directs the Secure Blockchain Initiative at CMU and has published widely on empirical analyses of cryptocurrency risks and abuse

- Eun Young Choi, Deputy Assistant Attorney General, National Security Division, DoJ
  - EYC was previously the first director of the National Cryptocurrency Enforcement Team (NCT) and before that ran DoJ's ransomware efforts

Group project

- Group original research project on some aspect of Blockchain abuse
  - ~3 people per group
- We're still figuring this one out, but one of the really nice things about Blockchains is that all the data is public, so lots of room for interesting data analysis projects
  - Examples:
    - Analysis of various smart contract attacks
    - Where does money from various thefts "go"? (and how does value change by the time its extracted)
    - How much crypto does the US Govt actually control?
    - "Dark crypto" moves (huge amounts of crypto was mined and never put into circulation… some it has suddenly started moving)
    - Is Ethereum (say) actually decentralized? Is DVT anything more than BS?
    - Analyze security of popular wallets (Metamask and Phantom), bridges (LayerZero), DEXes (dYdX), etc.
- Alex is going to use his magic to help each group refine their project ideas

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?

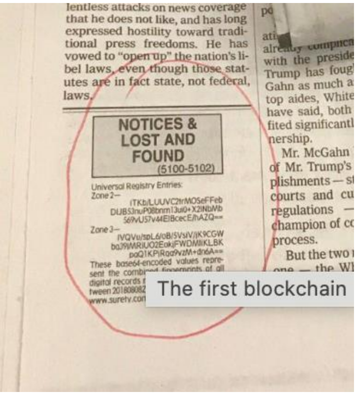
Ok, first some history

- 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

More history

- 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)

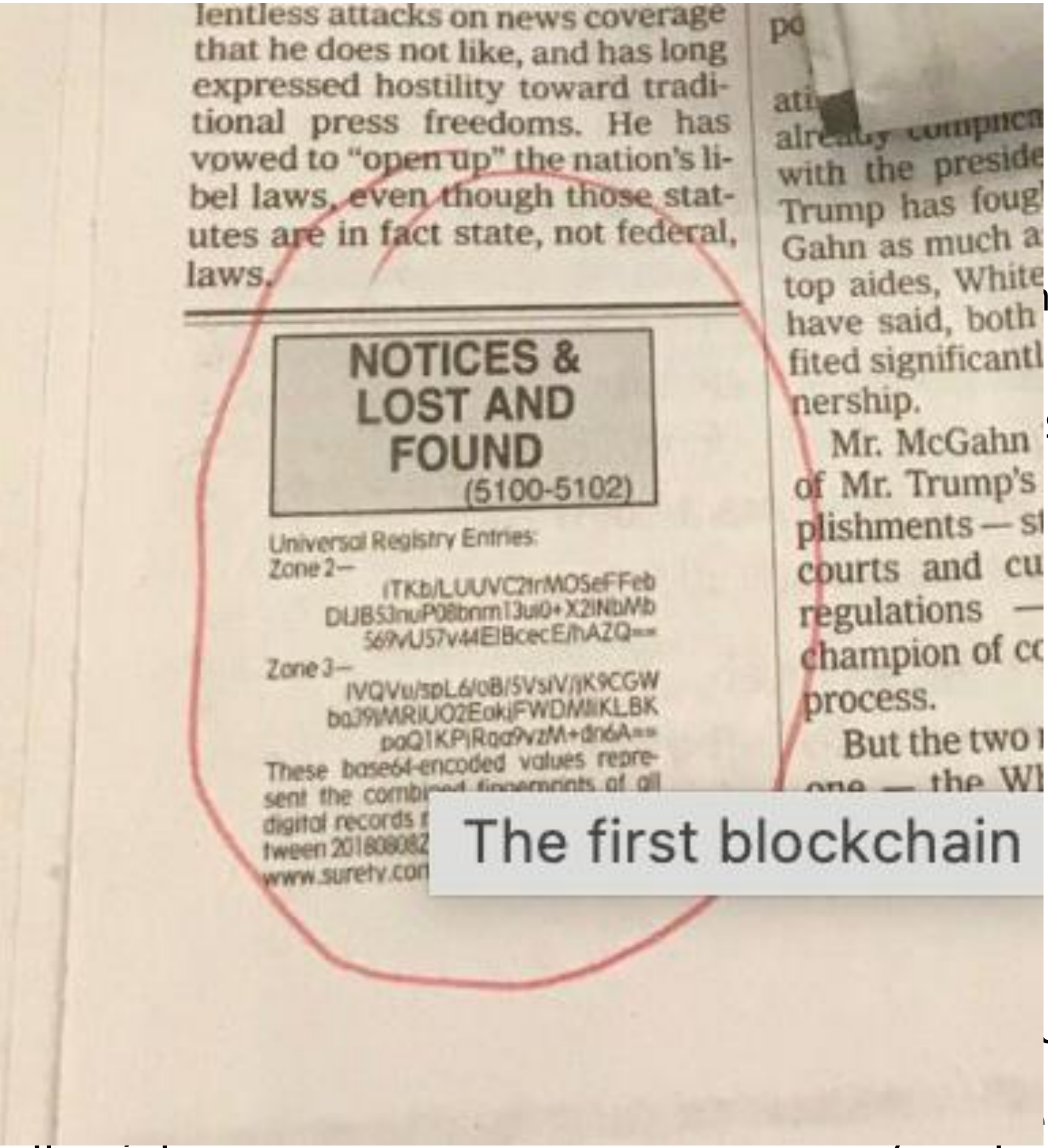
Universal Registry Entries:
Zone 2—
ITKb/LUUVC2lrMOSeFFeb
DUB53nuP08bnm13ui0+X2INbMb
569vUS7v44ElBcecE/hAZQ==
Zone 3—
IVQVu/spL6/oB/5VsIV/jK9CGW
ba39jMRiUO2EokjFWDMIlKLBK
poQ1KPjRqa9vzM+dn6A==
These base64-encoded values represent the combi
digital records
tween 2018082
www.surety.con

po
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

More histor

- 1979 – Merkle cc
  - Every non-leaf la ıow in log time
    that a given leaf
- 1992 Bayer, Hab s to "time-
  stamp" documer
  - In use since 1995
- 1993 Moni Naor
  - Cryptgraphic evi
    originally propos
  - 1997, Adam Bac with certain
    number of zeros
  - 2004, Hal Finey
    (i.e., uses truste
- Lots of effort in (particularly
  on cypherpunks ı of ads)
- In late 90s early er-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/spL6/0B/5VsIV/jK9CGW
ba39WRIUO2EokjFWDMIKLBK
paQ1KPjRqa9vzM+dn6A==
These base64-encoded values represent the combined fingerprints of all digital records tween 20180802
www.surety.com

po
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

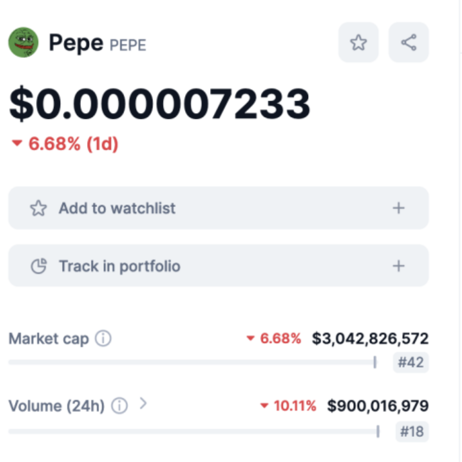
The first blockchain

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 $69k, the total market cap is 1.34T USD and an estimated trading volume of $34B
  - Massive venture capital investment (e.g., ~$2B just in the 4th quarter of 2023)
  - There are now roughly 9000 “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)

Underlying attraction of cryptocurrencies

- 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 its going to the moon! HODL!



Pepe PEPE

$0.000007233

▾ 6.68% (1d)

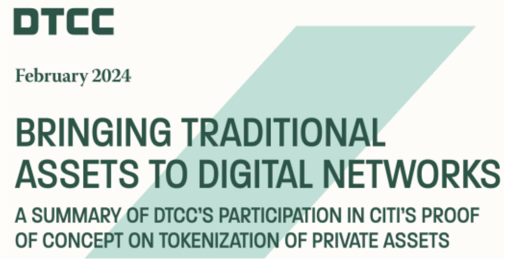
☆ Add to watchlist +

Track in portfolio +

Market cap ⓘ ▾ 6.68% $3,042,826,572 #42

Volume (24h) ⓘ > ▾ 10.11% $900,016,979 #18

- Reaction against high transaction costs and slow innovation in Western (particularly US) financial system
  - e.g., no real-time settlement



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

- Resisting inflation/capital controls in certain countries
  - i.e., Global South
- Raw techno-optimism? Others?

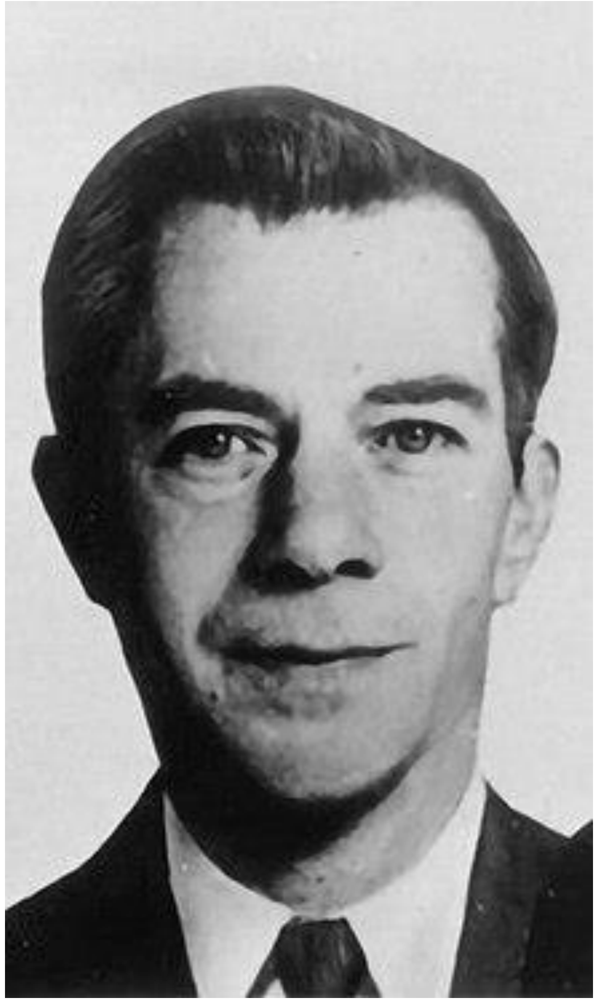
Properties of blockchains that people seem to want

- **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…

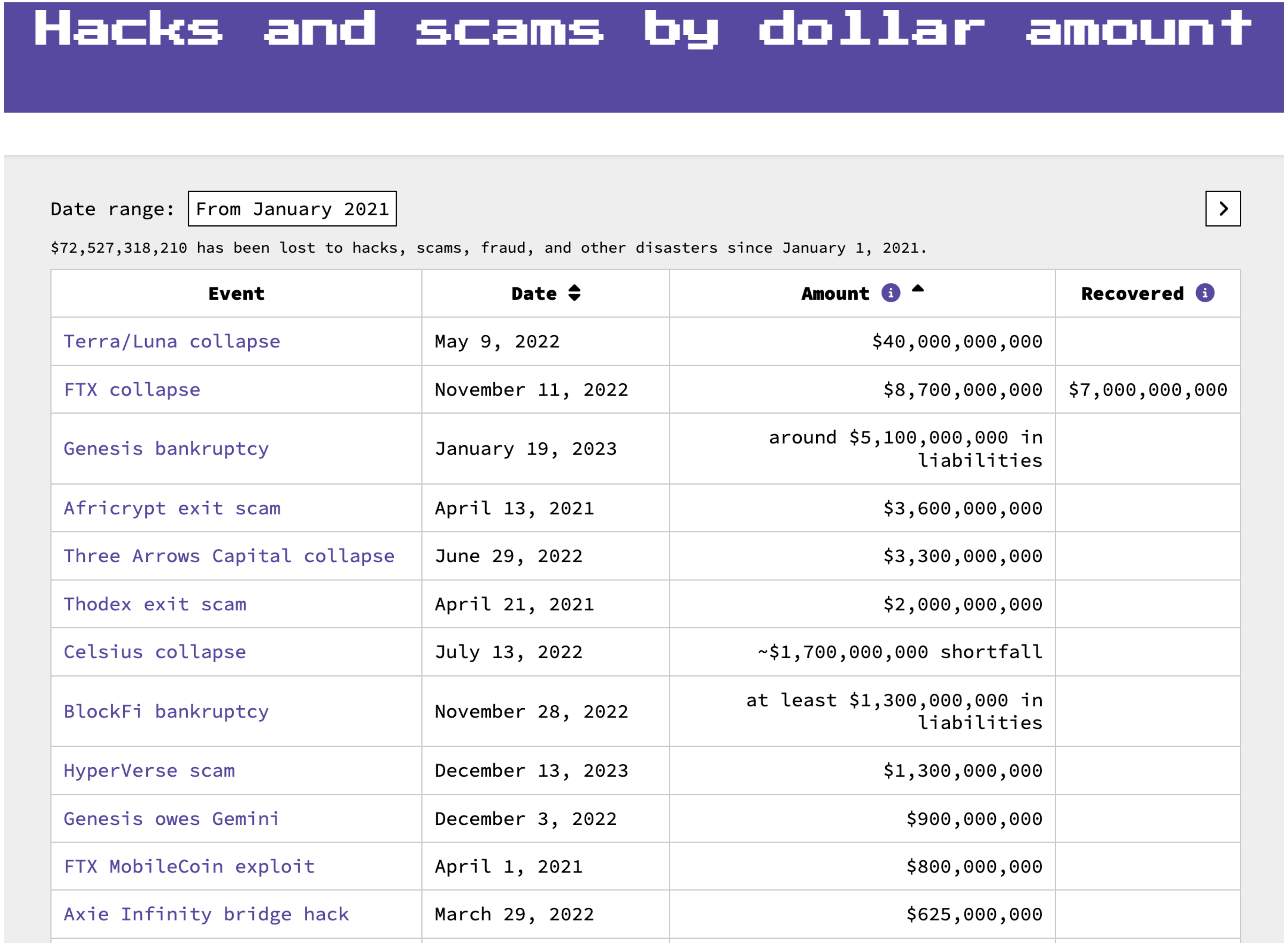


[*]This story is widely repeated, but is apocryphal, and ironically morphed into "Sutton's Law" which is used to teach doctors to start diagnosis with the most obvious possibility.

Robbed two banks in Chula Vista in 2021. Caught and convicted. Sentenced to 48 months in prison. How much did he get away with?

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)

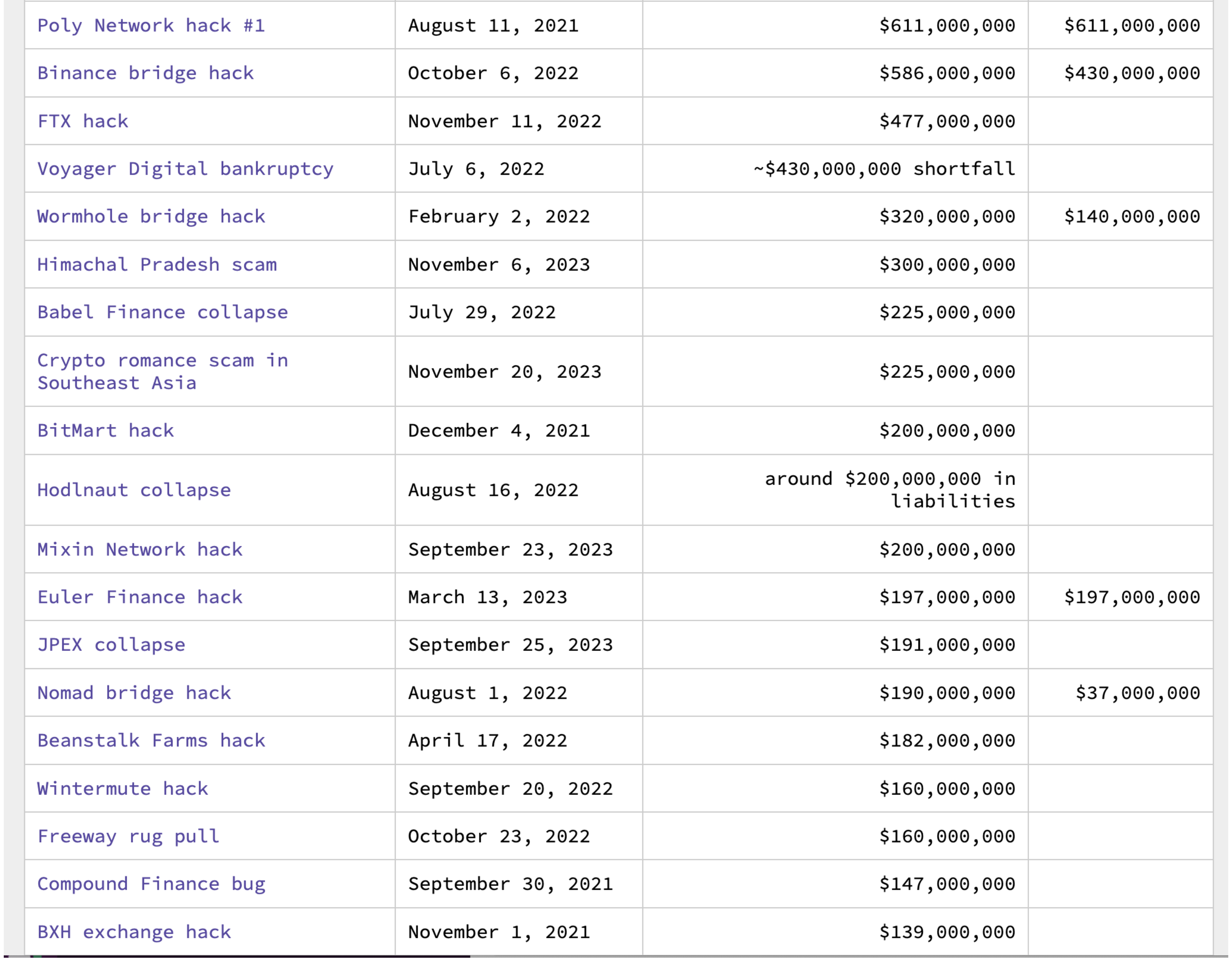


Hacks and scams by dollar amount

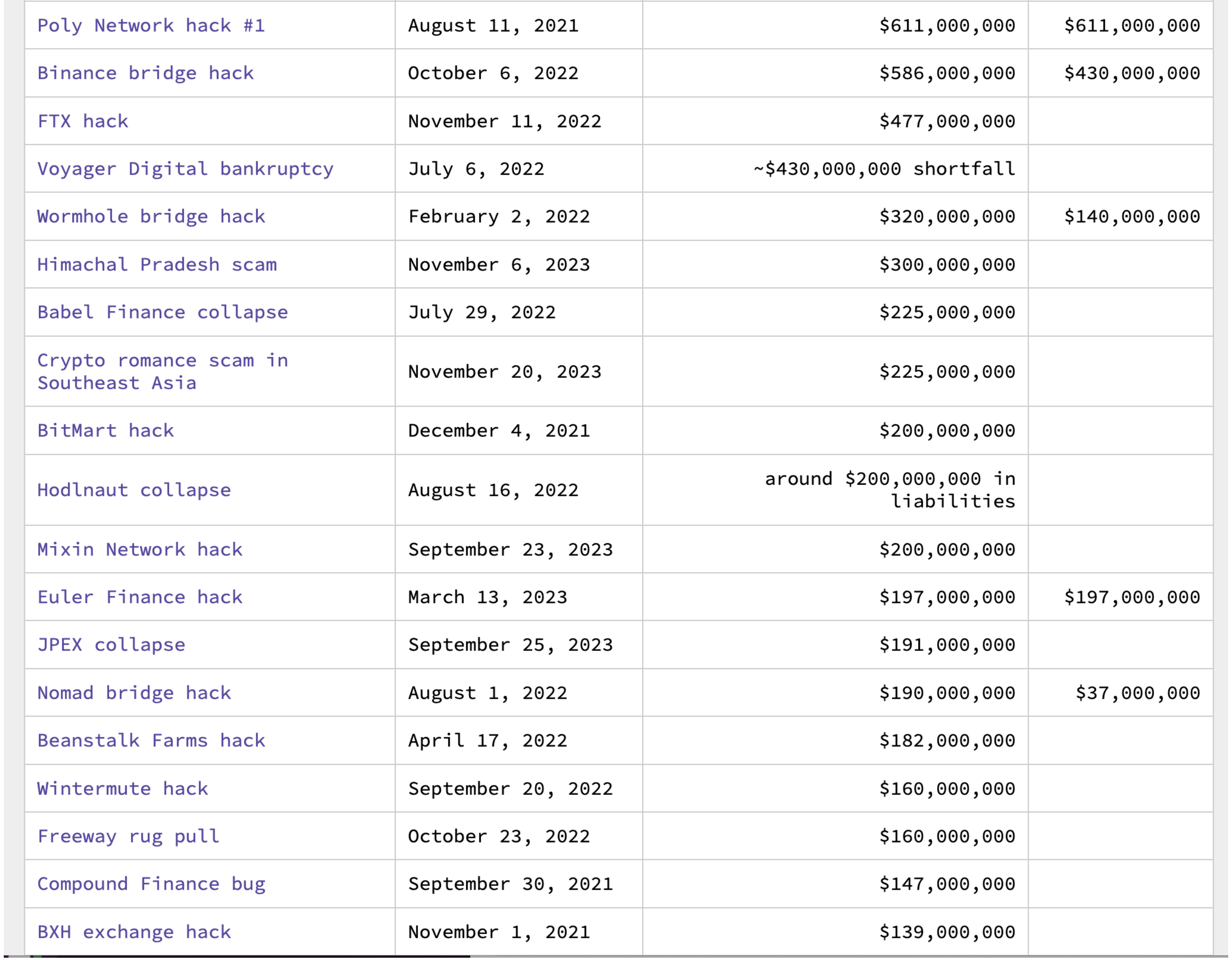
Date range: From January 2021 >

$72,527,318,210 has been lost to hacks, scams, fraud, and other disasters since January 1, 2021.

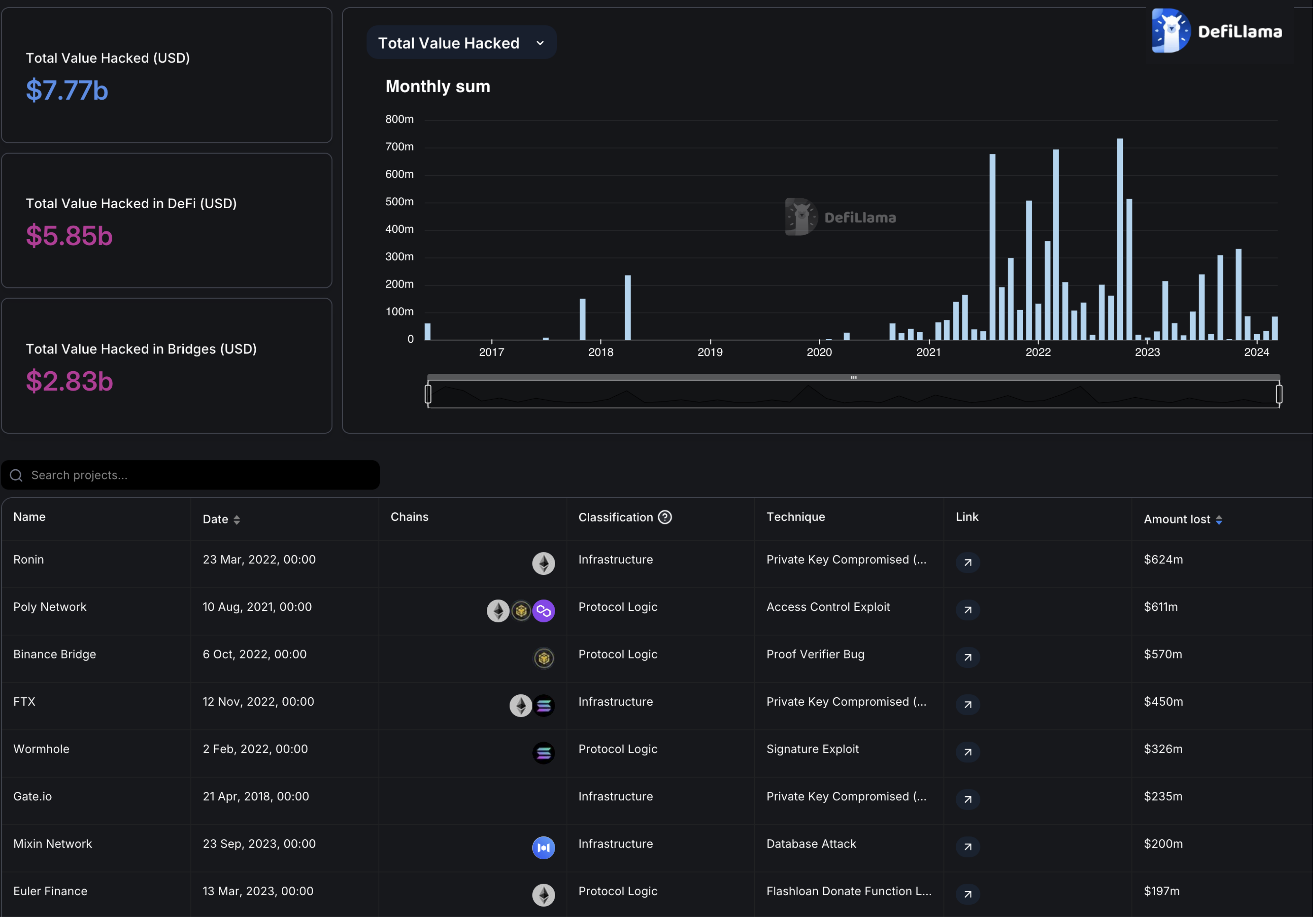
Event	Date ⇕	Amount ⓘ ▲	Recovered ⓘ
Terra/Luna collapse	May 9, 2022	$40,000,000,000	
FTX collapse	November 11, 2022	$8,700,000,000	$7,000,000,000
Genesis bankruptcy	January 19, 2023	around $5,100,000,000 in liabilities	
Africrypt exit scam	April 13, 2021	$3,600,000,000	
Three Arrows Capital collapse	June 29, 2022	$3,300,000,000	
Thodex exit scam	April 21, 2021	$2,000,000,000	
Celsius collapse	July 13, 2022	~$1,700,000,000 shortfall	
BlockFi bankruptcy	November 28, 2022	at least $1,300,000,000 in liabilities	
HyperVerse scam	December 13, 2023	$1,300,000,000	
Genesis owes Gemini	December 3, 2022	$900,000,000	
FTX MobileCoin exploit	April 1, 2021	$800,000,000	
Axie Infinity bridge hack	March 29, 2022	$625,000,000	



Poly Network hack #1	August 11, 2021	$611,000,000	$611,000,000
Binance bridge hack	October 6, 2022	$586,000,000	$430,000,000
FTX hack	November 11, 2022	$477,000,000	
Voyager Digital bankruptcy	July 6, 2022	~$430,000,000 shortfall	
Wormhole bridge hack	February 2, 2022	$320,000,000	$140,000,000
Himachal Pradesh scam	November 6, 2023	$300,000,000	
Babel Finance collapse	July 29, 2022	$225,000,000	
Crypto romance scam in Southeast Asia	November 20, 2023	$225,000,000	
BitMart hack	December 4, 2021	$200,000,000	
Hodlnaut collapse	August 16, 2022	around $200,000,000 in liabilities	
Mixin Network hack	September 23, 2023	$200,000,000	
Euler Finance hack	March 13, 2023	$197,000,000	$197,000,000
JPEX collapse	September 25, 2023	$191,000,000	
Nomad bridge hack	August 1, 2022	$190,000,000	$37,000,000
Beanstalk Farms hack	April 17, 2022	$182,000,000	
Wintermute hack	September 20, 2022	$160,000,000	
Freeway rug pull	October 23, 2022	$160,000,000	
Compound Finance bug	September 30, 2021	$147,000,000	
BXH exchange hack	November 1, 2021	$139,000,000	



Poly Network hack #1	August 11, 2021	$611,000,000	$611,000,000
Binance bridge hack	October 6, 2022	$586,000,000	$430,000,000
FTX hack	November 11, 2022	$477,000,000	
Voyager Digital bankruptcy	July 6, 2022	~$430,000,000 shortfall	
Wormhole bridge hack	February 2, 2022	$320,000,000	$140,000,000
Himachal Pradesh scam	November 6, 2023	$300,000,000	
Babel Finance collapse	July 29, 2022	$225,000,000	
Crypto romance scam in Southeast Asia	November 20, 2023	$225,000,000	
BitMart hack	December 4, 2021	$200,000,000	
Hodlnaut collapse	August 16, 2022	around $200,000,000 in liabilities	
Mixin Network hack	September 23, 2023	$200,000,000	
Euler Finance hack	March 13, 2023	$197,000,000	$197,000,000
JPEX collapse	September 25, 2023	$191,000,000	
Nomad bridge hack	August 1, 2022	$190,000,000	$37,000,000
Beanstalk Farms hack	April 17, 2022	$182,000,000	
Wintermute hack	September 20, 2022	$160,000,000	
Freeway rug pull	October 23, 2022	$160,000,000	
Compound Finance bug	September 30, 2021	$147,000,000	
BXH exchange hack	November 1, 2021	$139,000,000	



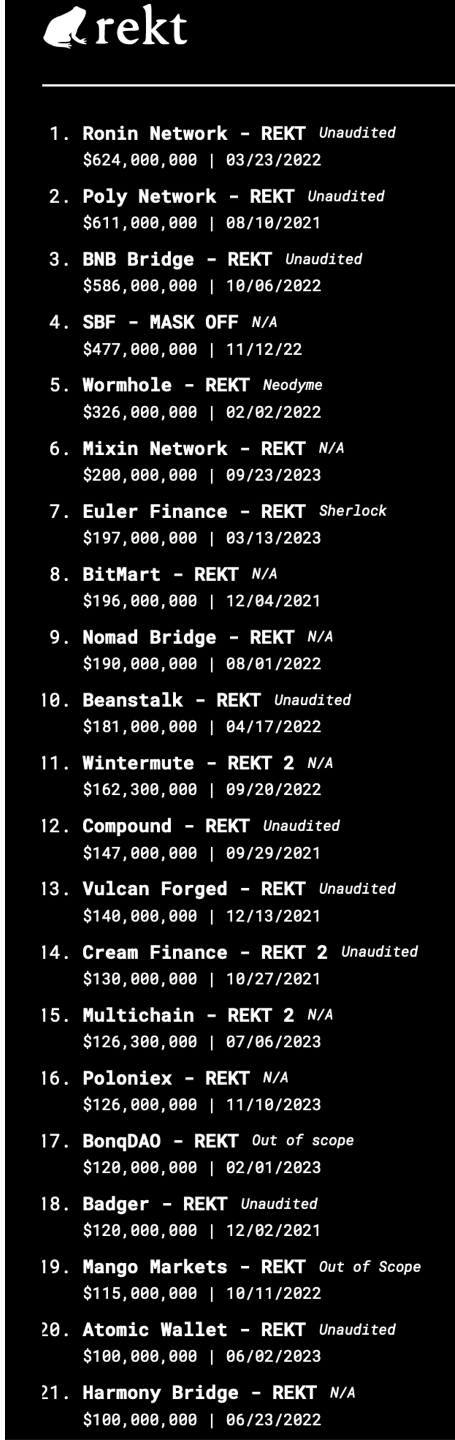
Total Value Hacked (USD)
$7.77b

Total Value Hacked in DeFi (USD)
$5.85b

Total Value Hacked in Bridges (USD)
$2.83b

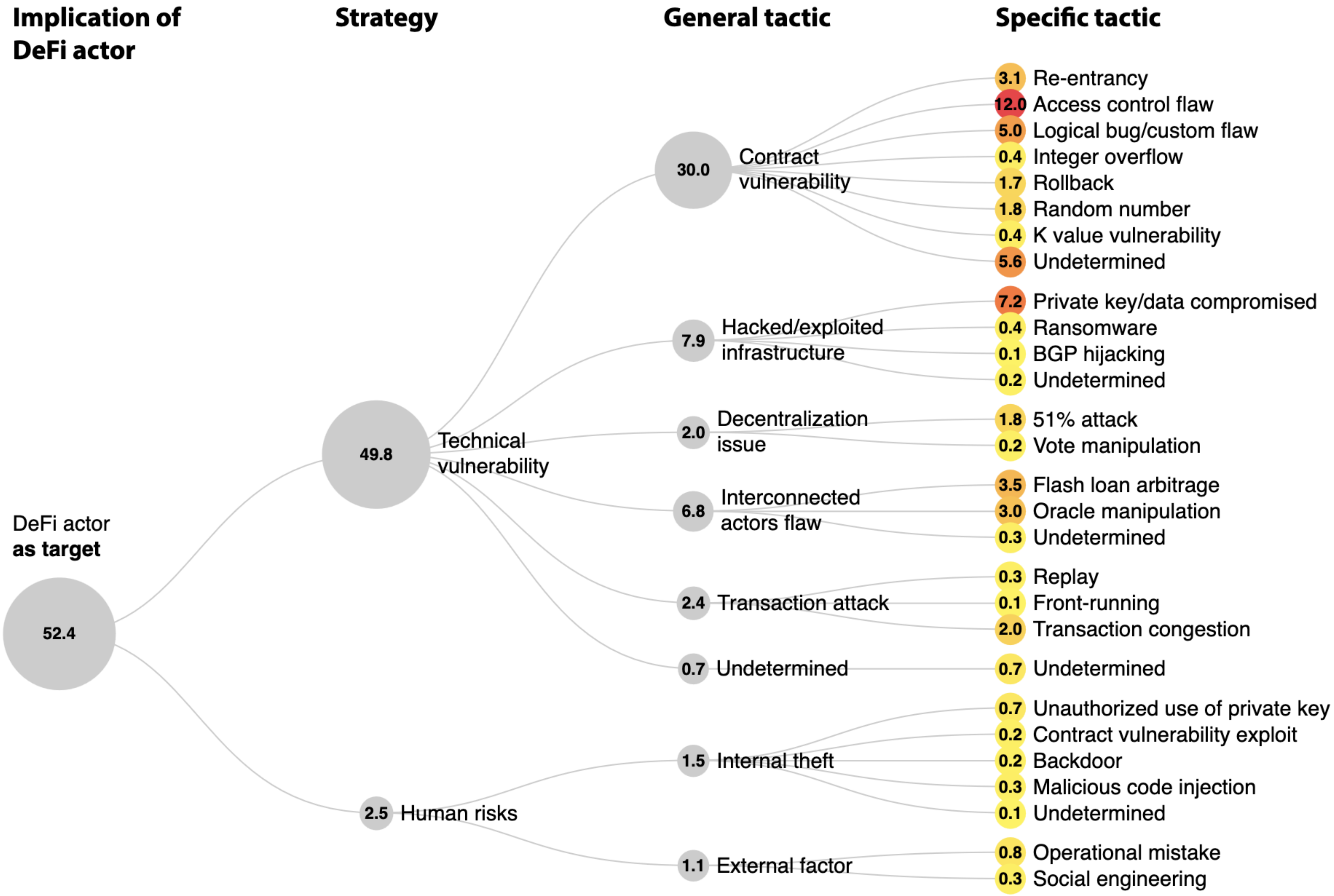
Search projects...

Name	Date	Chains	Classification	Technique	Link	Amount lost
Ronin	23 Mar, 2022, 00:00		Infrastructure	Private Key Compromised (...	↗	$624m
Poly Network	10 Aug, 2021, 00:00		Protocol Logic	Access Control Exploit	↗	$611m
Binance Bridge	6 Oct, 2022, 00:00		Protocol Logic	Proof Verifier Bug	↗	$570m
FTX	12 Nov, 2022, 00:00		Infrastructure	Private Key Compromised (...	↗	$450m
Wormhole	2 Feb, 2022, 00:00		Protocol Logic	Signature Exploit	↗	$326m
Gate.io	21 Apr, 2018, 00:00		Infrastructure	Private Key Compromised (...	↗	$235m
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



rekt

1. **Ronin Network - REKT** *Unaudited*
$624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
$611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
$586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
$477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
$326,000,000 | 02/02/2022
6. **Mixin Network - REKT** *N/A*
$200,000,000 | 09/23/2023
7. **Euler Finance - REKT** *Sherlock*
$197,000,000 | 03/13/2023
8. **BitMart - REKT** *N/A*
$196,000,000 | 12/04/2021
9. **Nomad Bridge - REKT** *N/A*
$190,000,000 | 08/01/2022
10. **Beanstalk - REKT** *Unaudited*
$181,000,000 | 04/17/2022
11. **Wintermute - REKT 2** *N/A*
$162,300,000 | 09/20/2022
12. **Compound - REKT** *Unaudited*
$147,000,000 | 09/29/2021
13. **Vulcan Forged - REKT** *Unaudited*
$140,000,000 | 12/13/2021
14. **Cream Finance - REKT 2** *Unaudited*
$130,000,000 | 10/27/2021
15. **Multichain - REKT 2** *N/A*
$126,300,000 | 07/06/2023
16. **Poloniex - REKT** *N/A*
$126,000,000 | 11/10/2023
17. **BonqDAO - REKT** *Out of scope*
$120,000,000 | 02/01/2023
18. **Badger - REKT** *Unaudited*
$120,000,000 | 12/02/2021
19. **Mango Markets - REKT** *Out of Scope*
$115,000,000 | 10/11/2022
20. **Atomic Wallet - REKT** *Unaudited*
$100,000,000 | 06/02/2023
21. **Harmony Bridge - REKT** *N/A*
$100,000,000 | 06/23/2022


Implication of DeFi actor
Strategy
General tactic
Specific tactic
DeFi actor **as target**
52.4
49.8
Technical vulnerability
2.5
Human risks
30.0
Contract vulnerability
7.9
Hacked/exploited infrastructure
2.0
Decentralization issue
6.8
Interconnected actors flaw
2.4
Transaction attack
0.7
Undetermined
1.5
Internal theft
1.1
External factor
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
7.2
Private key/data compromised
0.4
Ransomware
0.1
BGP hijacking
0.2
Undetermined
1.8
51% attack
0.2
Vote manipulation
3.5
Flash loan arbitrage
3.0
Oracle manipulation
0.3
Undetermined
0.3
Replay
0.1
Front-running
2.0
Transaction congestion
0.7
Undetermined
0.7
Unauthorized use of private key
0.2
Contract vulnerability exploit
0.2
Backdoor
0.3
Malicious code injection
0.1
Undetermined
0.8
Operational mistake
0.3
Social engineering

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)

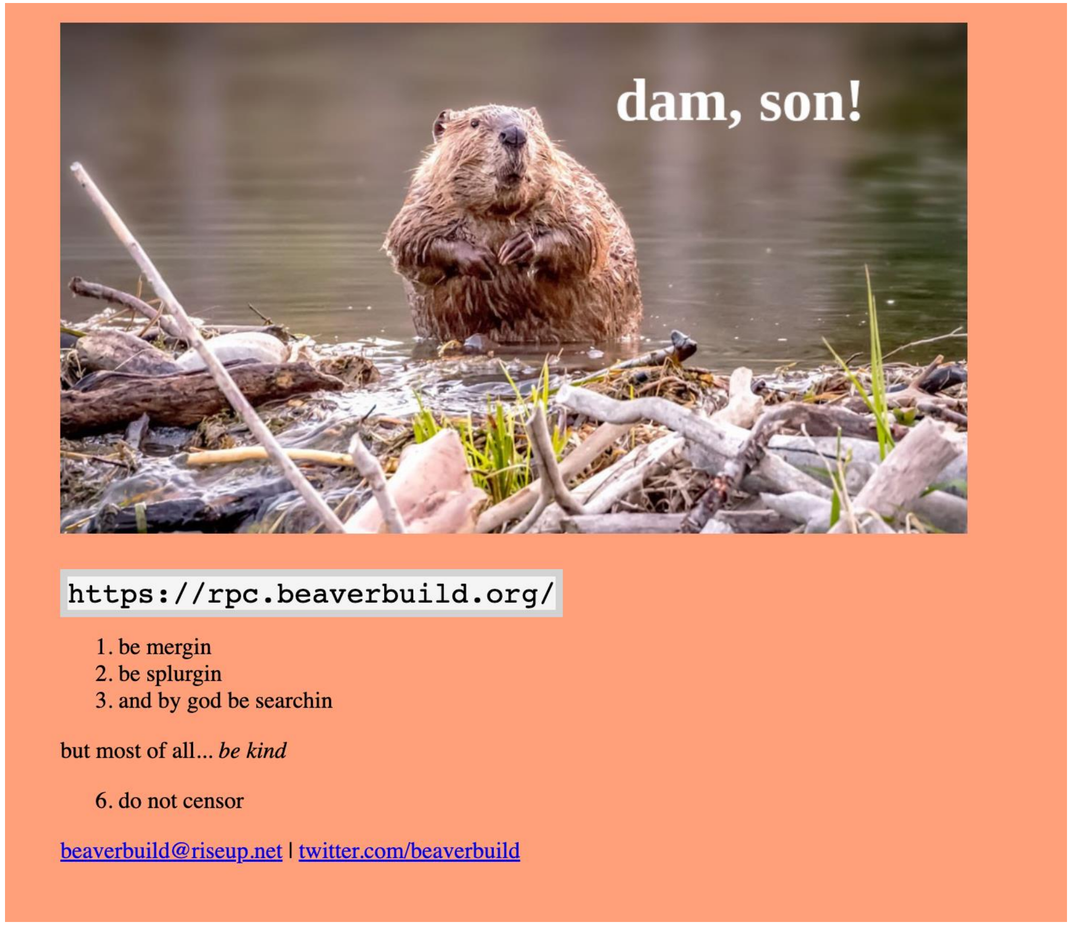
- Fraudulent representations
  - Convince investors to invest in new crypto endeavor (ICO); take money; abandon new coin (aka rug pull)
  - High yield investment scams (Ponzi and otherwise; promise high yield); may involve impersonation
  - Misrepresent whether investment assets are kept liquid or used 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 (e.g., Binance)

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

It’s the wild west out there… seriously

- Texas is the largest source of Bitcoin mining on the planet (repurposed aluminum smelting plants)
- 2.5% of whole grid’s peak load; another 40% trying to come online
  get paid if they mine or not (demand response; biggest battery in Texas)

For next time

- 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
  [the syllabus is still wide open]