SOLIDUS LABS

The 2022 Rug Pull Report

Everything you need to know about crypto and DeFi scams

December 2022
Solidus Labs Report Series
www.soliduslabs.com

What's Inside The 2022 Rug Pull Report

- Why the vast majority of rug pulls have evaded detection under traditional approaches to scam identification
- The seven types of scam tokens, how they steal from users, and how many investors they've harmed
- How token smart contract screeners can help regulators, blockchain platforms, and crypto companies combat money laundering

Contents

What is a rug pull? 3

The rug pull epidemic in numbers 4

Hard rug pulls 6

- Honeypots 7
- Hidden mints 9
- Fake ownership renunciations 9
- Hidden balance modifiers 9
- Hidden transfers 9
- Hidden fee modifiers 10
- Hidden max transaction amount modifiers 10

Soft rug pulls 11

HALO Threat Intelligence: Solidus' Web3 AML Solution 13

First things first: What is a rug pull?

A rug pull is when a scammer develops a crypto token, deploys it on a blockchain, convinces users to buy it, and then liquidates his or her holdings without warning, leaving investors in the lurch.

There are two main types of rug pulls — hard and soft.

In a **hard rug pull**, also known as a token scam, the scammer *programs* their token to steal from investors. They may write scripts that make it impossible for others to sell the token (honeypots), that allow them to mint unlimited new ones (hidden mints), or that charge sell fees as high as 100% (hidden fee modifiers). There are seven main types of hard rug pulls.

In a **soft rug pull**, also known as an exit scam, the scammer *promotes* their token to steal from investors. They may publish misleading marketing websites and roadmaps, announce fake partnerships, or use bots to manufacture trading activity.

The rug pulls that steal the most cryptocurrency the fastest tend to be both 'hard' and 'soft.' The Squid Game token, for example, was a honeypot with its own marketing website, whitepaper, and promotional video. Within days of its release, it had netted its creators more than $3 million.

... And why have most gone undetected?

Because for one thing, in most rug pulls, the theft occurs exclusively on-chain. The scam is encoded in the token's smart contract, the token is traded on a decentralized exchange, and the scammer's illicit profits are denominated in crypto, not fiat currency.

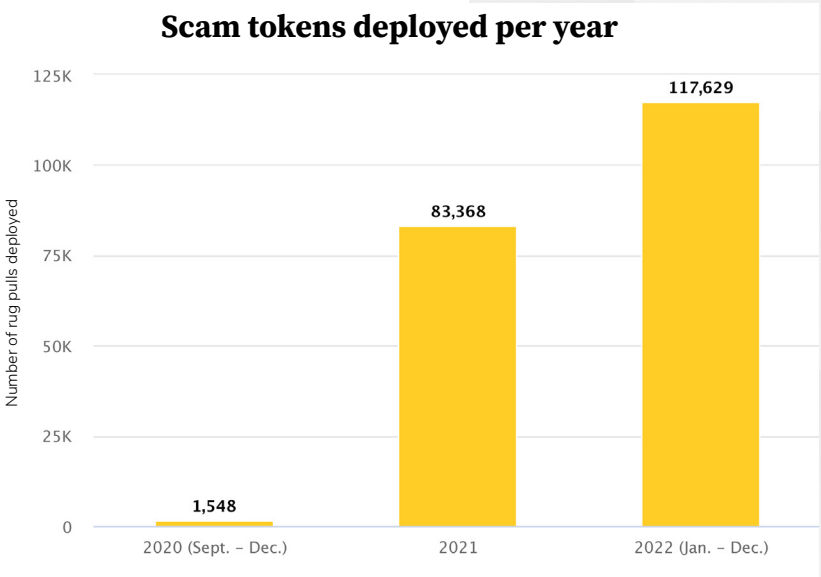
For another, while token scammers may sometimes amplify their malicious tokens' reach with fraudulent marketing, attracting investors by using bots to spam social media or execute wash trades, they can do many of these actions without even registering a web domain.

By scanning the source code of every new cryptocurrency deployed on an EVM blockchain since 2020 — amounting to 1.8 million tokens and 12 chains to date — Solidus' Web3 AML solution has become the first and only comprehensive rug pull detection tool.

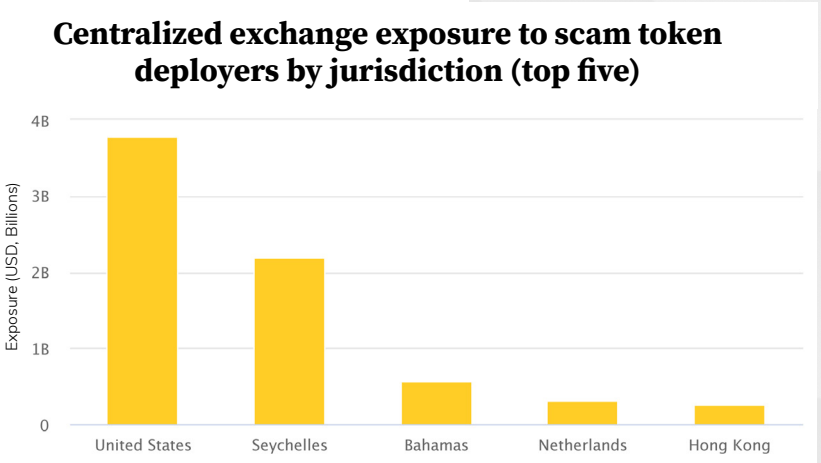
The Rug Pull Epidemic in Numbers

Rug pulls are one of the most common scams in crypto, but until now, regulators and crypto companies have not had access to forensic or compliance tools that properly identify, let alone address, the massive scale of the problem. Prior industry research spotted only 24 rug pulls in all of 2021, while Comparitech's rug pull tracker, which relies on public sources like industry news and court filings, has tallied just 262 so far in 2022.

In reality, the rug pull epidemic is larger by several orders of magnitude. Data from Threat Intelligence, Solidus Labs' new smart contract scanning tool, reveals that **fraudsters deployed over 200,000 scam tokens from September 2020 to December 1st, 2022.**



Many of the scammers behind these tokens use crypto-to-fiat exchanges to both seed their scams and launder their proceeds. **These fraudsters — benefiting from the fact that more than 99% of their malicious tokens have evaded detection under traditional approaches to scam identification – deposited and withdrew a combined $11 billion worth of ETH to/from 153 different CeFi exchanges during the time period we studied.** The five jurisdictions that oversee CeFi exchanges with the most exposure collectively are the United States, Seychelles, the Bahamas, the Netherlands and Hong Kong.

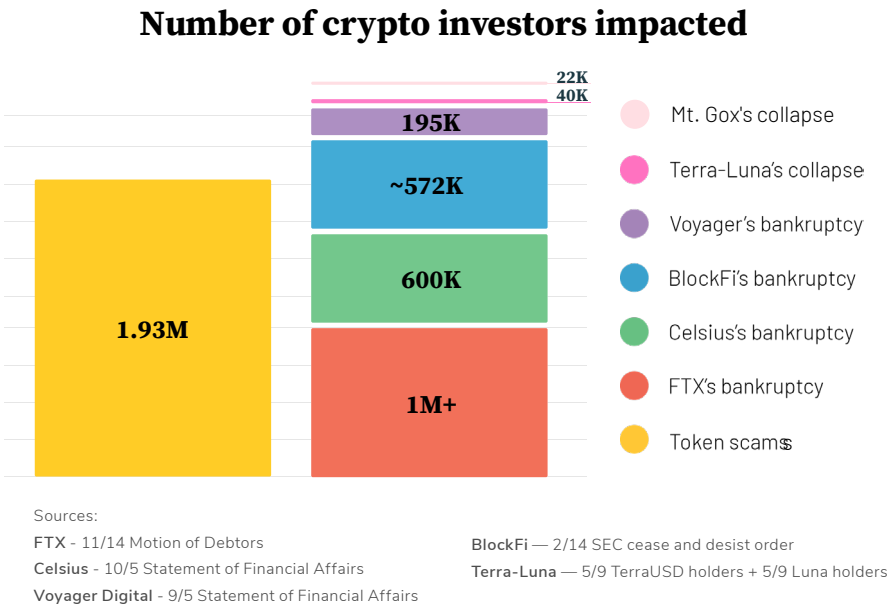


ETH price at time of conversion: $1286.29
Exposure is calculated by summing the amount of ETH that has been deposited to/withdrawn from an exchange that is also tied either directly or indirectly to a known rug pull deployer.

In total, five of these centralized crypto exchanges have more than $1 billion worth of exposure to scam token deployers. 17 of these exchanges have more than $100 million. Ninety-three exchanges have at least $1 million worth of exposure to scam token deployers.

In other words, almost every major crypto exchange is impacted. These exchanges are required to prevent money laundering under the regulatory regimes in every jurisdiction in which they operate. Further, they face additional regulatory requirements in many jurisdictions regarding investor protection and market abuse prevention.

We have also identified a staggering number of rug pull victims. **Almost two million investors have lost funds to rug pull tokens. This is comparable to the number of investors facing unsecured losses in multiple of crypto's biggest collapses.**

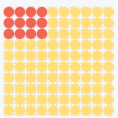


While the number of impacted investors in some of the listed incidents are estimates – FTX and BlockFi have yet to publish their exact number of creditors, and it is likely that some of the crypto addresses we have counted as separate users are controlled by the same person – this demonstrates that rug pulls have harmed more investors than any single collapse in crypto to date.

This hidden theft phenomenon reveals significant gaps in consumer protection, anti-money laundering, and crypto market integrity.

In the following sections, we map this epidemic in depth, using original research and case studies to explain how Solidus Labs detects, defines and categorizes rug pulls at scale.

8% of all Ethereum tokens are programmed to execute rug pulls



12% of all BNB Chain tokens are scams (the highest of any blockchain)

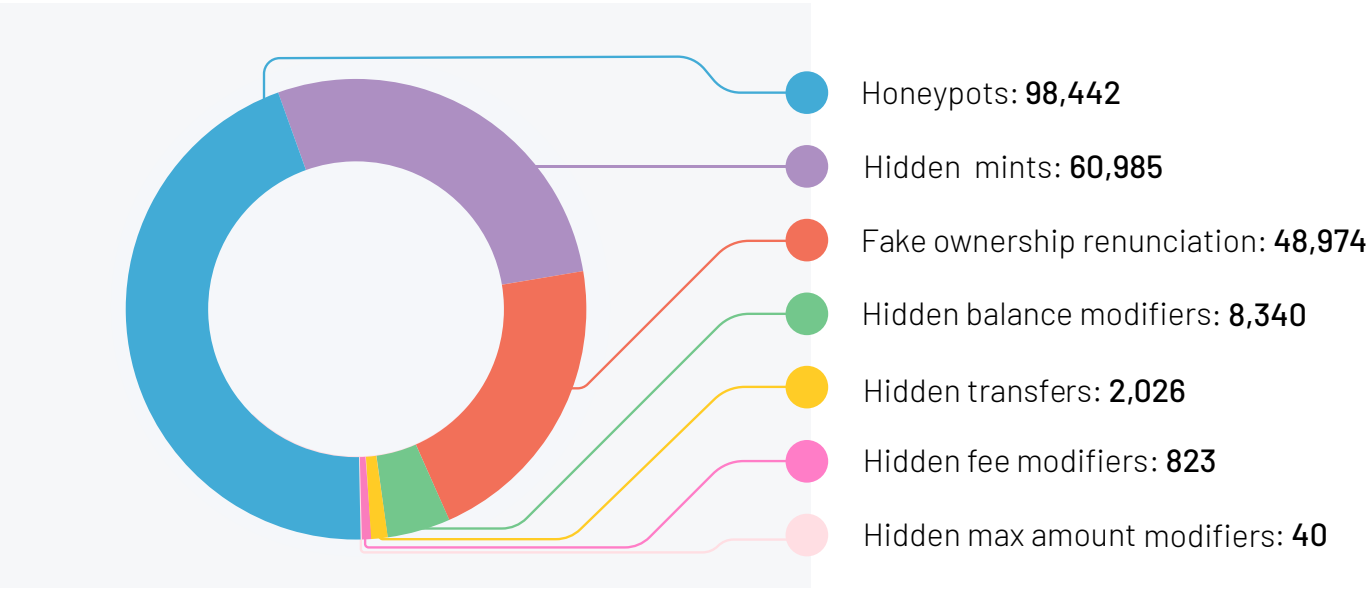
15 new scam tokens are detected every hour

Hard rug pulls

Solidus' Web3 AML solution sorts all hard rug pulls into one or more of the following seven categories:

- **Honeypots**
  prevent buyers from re-selling their tokens.
- **Hidden mints**
  let developers create unlimited new tokens.
- **Fake ownership renunciations**
  let token developers hide the fact that they can call sensitive functions.
- **Hidden balance modifiers**
  let developers edit users' balances.
- **Hidden fee modifiers**
  let developers establish sell fees as high as 100%.
- **Hidden max transaction amount modifiers**
  let developers set maximum transaction values as low as zero.
- **Hidden Transfers**
  let developers to transfer tokens from other holders' addresses to their own.

Scam tokens deployed by exploit type



Honeypots

Scams detected: 98,442

A honeypot prevents the buyers of a token from reselling it. This inability to sell causes the token's price to only increase for as long as the scammer would like, creating the appearance of a "mooning" token and thereby tricking even more users into buying it. This is why honeypots are by far the most popular rug pull — because they allow their deployers to both manipulate their users and the token's price.

The majority of honeypots to date have been implemented in one of four ways: liquidity pool blocks, using external contracts, blocklists, or allowlists.

Liquidity Pool Blocks

Scams detected: 30,323

A liquidity pool (LP) block honeypot prevents users from sending their tokens to this token's liquidity pool smart contract, which is a necessary step in the sale/swap of the token. Only purchases of the token are allowed.

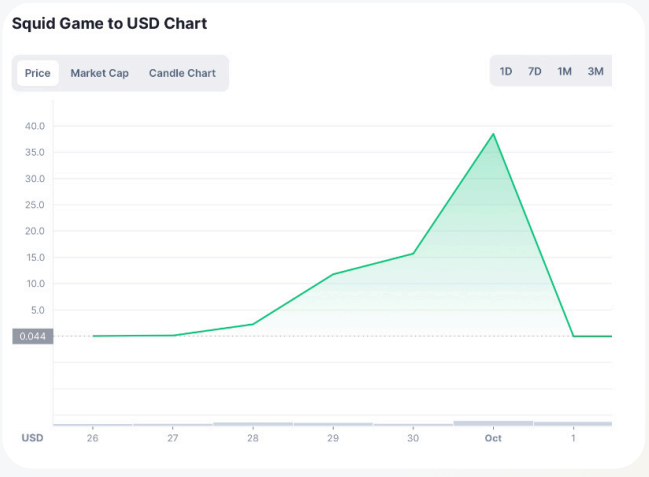
External Contracts

Scams detected: 35,424

In an external contract honeypot, a token's transfer functionality is implemented in a separate contract for which the source code is not public. This private contract blocks token sales and swaps for all addresses except for the deployer's own.

Case study: The Squid Game token

The most famous example of the honeypot exploit is the Squid Game ($SQUID) token. Capitalizing on the popularity of the eponymous Netflix series, SQUID called an external contract in its deployment contract, making it look like a rapidly-growing meme coin to many users. Within days, investors had spent over $3.3 million worth of cryptocurrency buying SQUID, none of which they could then sell. The developers used this opportunity to drain SQUID's liquidity pools and run off with users' funds.



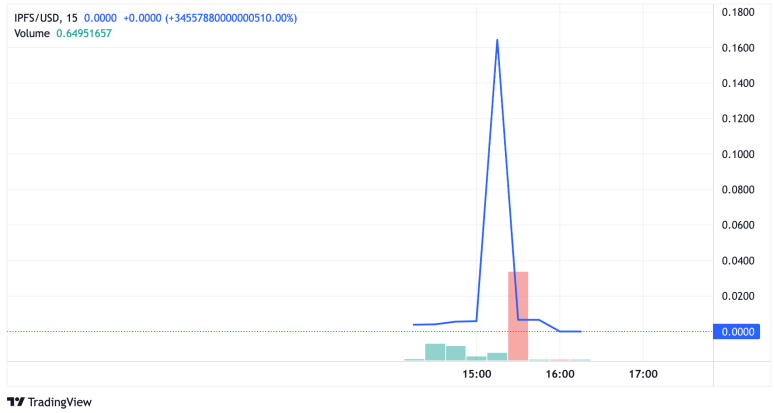
Blocklists/Allowlists

Scams detected: 10,639

A blocklist/allowlist honeypot restricts selling permissions to one or more addresses named by the token's deployer. In the blocklist variant, any user who purchases the token is added to a blocklist either manually or automatically. In the allowlist variant, the token deployer's address typically is the only address granted the ability to sell.

Case study: The InterPlanetary File System impersonation token

The InterPlanetary File System is a peer-to-peer file sharing network that NFT marketplaces like OpenSea use to store NFT metadata. It does not have its own crypto token. But in October 2020, scammers took it upon themselves to create one. This impersonation token ($IPFS) had blocklist capabilities, requiring users to secure the scammer's approval before completing any transfer beyond their initial purchase. Rather than approving these transfers, the scammer simply cashed out their profits — $15,000 of ETH in under two hours — and ran.



Hidden mints

Scams detected: 60,985

A hidden mint allows one or more externally owned accounts (EOAs) – in this context, the personal address(es) of the token's deployers – to mint new tokens using a hidden function within the token's contract. After calling this function, the scammer can dump these extra tokens on the market, devaluing the tokens held by others.

Fake ownership renunciations

Scams detected: 48,974

In a fake ownership renunciation, the scammer deceptively encodes the impression that they have relinquished control of the token contract. In reality, the scammer maintains ownership, and is therefore still able to call sensitive, owner-only functions within the contract, like functions that can pause trading, mint tokens, or set fees.

Hidden balance modifiers

Scams detected: 8,340

A hidden balance modifier allows one or more externally-owned accounts (EOAs), or the token contract itself, to modify token holders' balances. If the EOA sets holder balances to zero, this makes selling impossible, much like a honeypot.

Hidden transfers

Scams detected: 2,026

A hidden transfer allows developers to send tokens from other users' addresses to themselves.

Case study: Grab Chain

The aptly named Grab Chain token (SGC) automatically adds buyer addresses to a custom-made array. Then, after a certain period of time, the scammer calls a public function that is maliciously scripted to transfer all but one token from every buyer's address to the token's marketing wallet, which is controlled by the scammer

Hidden max transaction amount modifiers

Scams detected: 40

Hidden max transaction amount modifiers let developers establish maximum transaction values.

Case study: the SpaceX impersonation token

The impersonation token SpaceX ($FALCON) includes an intentionally misnamed function called burning() that, when called, limits every user's maximum transaction value to zero — except for the rug-puller.

Hidden fee modifiers

Scams detected: 823

Hidden fee modifiers allow token developers to change the fee amounts collected when users buy and/or sell a token. Scammers can make this modification to trick users into unknowingly paying as much or sometimes even more than 100% of the size of their transfers in fees.

Soft Rug Pulls

A soft rug pull, also known as an exit scam, is when a scammer creates a regular crypto token – no malicious smart contract involved – but then promotes that token fraudulently, only to abscond with investors' funds.

Before pulling the rug, exit scammers may:

- Create a misleading marketing website
- Announce partnerships that don't exist
- Assert untrue claims about their development team or backers
- Give themselves token allocations well beyond what they claim to own in public
- Engage in wash trading to artificially inflate the token's volume or price
- Use social media bots to spam positive sentiment about the token on platforms like Twitter, Discord, Reddit, Signal, or Telegram
- When scammers have been caught making false representations like the above, they have been convicted of crimes like money laundering, securities and wire fraud. Atlanta film producer Ryan Felton, for example, pleaded guilty to twelve counts of wire fraud, ten counts of money laundering, and two counts of securities fraud after executing two 2018 rug pulls — FLiK and CoinSpark.

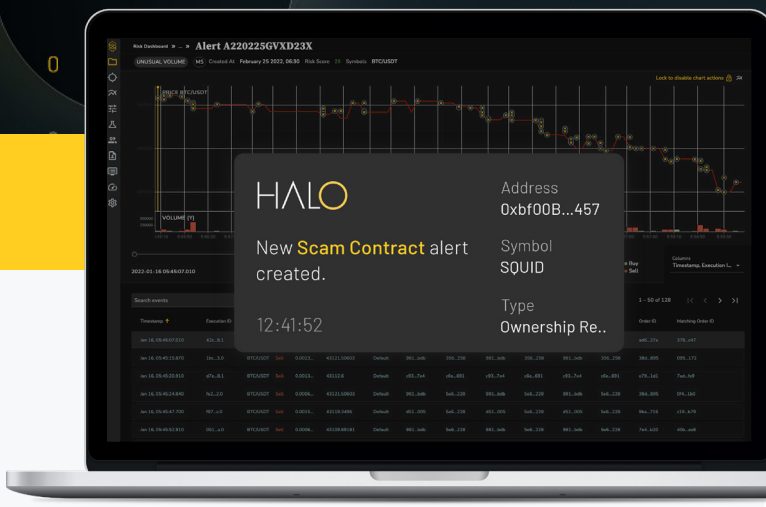
The U.S. Attorney's Office of the Northern District of Georgia's press release announcing the convictions reads:

"Felton falsely represented to investors that a prominent Atlanta rapper and actor was a co-owner of FLiK, the United States military had agreed to distribute the streaming platform to service members, and FLiK was finalizing licensing deals with major film and television studios. In reality, the rapper had no role in the company beyond authorizing a promotional social media post, FLiK had no military contract, and Felton never had discussions with any studio about licensing content. Felton further claimed that he was actively developing the platform and would use all funds raised in the ICO to launch FLiK. After the ICO closed, Felton dumped more than 40 million FLiK coins on trading markets, causing the value of FLiK coins to plummet."

This case shows that U.S. prosecutors are both willing and able to convict the scammers behind soft rug pulls. The same may soon become true of hard rug pulls, too.

HALO | THREAT INTELLIGENCE

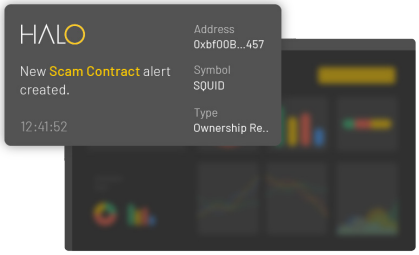
Web3 AML Solution

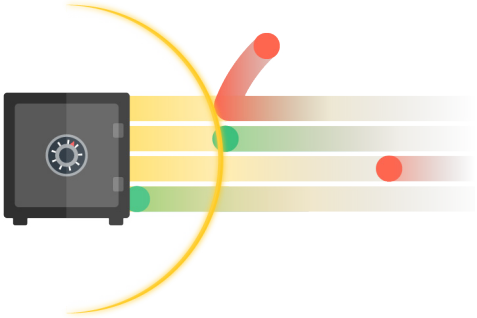


Actively Monitoring 1,888,182 Tokens and 205,704 Scams

Identify Scams at Scale

Continuously scan millions of token contracts using cutting-edge smart contract screening technology, flagging scam vulnerabilities with unprecedented accuracy.





Stop Malicious Actors from Taking Advantage of Your Platform

Deploy a preemptive layer against bad actors violating your platform by empowering your compliance team with real-time Web3 AML alerts.

Safeguard Your Business from Regulatory Enforcement Risk

Protect your organization from avoidable anti-money laundering compliance risks. Future-proof your platform by staying ahead of emerging scam typologies and DeFi threats.

Get in touch to speak with an expert, or learn more:

GET IN TOUCH | SOLIDUSLABS.COM

SOLIDUS LABS

26 Broadway, New York, NY, 10004 United States

soliduslabs.com | @Solidus_Labs | hello@soliduslabs.com