The Top 10 Cryptocurrency Scams and Hacks in 2022

Original: https://www.btcc.com/en-US/academy/research-analysis/the-top-10-cryptocurrency-scams-and-hacks-in-2022

Here we summarized the top 10 cryptocurrency scams and hacks in 2022. Read on to find out how much money the crypto community lost in 2022 — and how to prevent this from happening again.

Despite crypto markets being trapped in a severe bearish recession, scams and hacks in Web3 were on fire for the entirety of 2022. A number of top-tier centralized cryptocurrency heavyweights also collapsed due to poor risk management and insider manipulations.

As the crypto segment approaches New Year, U.Today recaps the most dangerous cryptocurrency scams, their roots, designs and the losses they caused. We have also prepared a short review of the most frequent cryptocurrency scams in social media that target millions of users daily.

Cryptocurrency Scams and Hacks in 2022: Overview

According to numerous cybersec reports, in the first 11 months of 2022, hackers and scammers managed to steal an unprecedented amount of $4.2 billion in cryptocurrency, which is 37% more than in 2021, when key cryptos were 2x-3x more expensive.

- The largest attacks were executed against cross-chain protocols — Axie Infinity's bridge mechanism Ronin and the multi-protocol ecosystem Wormhole.

- The collapses of the Terra LUNA ecosystem, its major DeFi Anchor Protocol (ANC) and the USD-pegged stablecoin TerraUSD (UST) contributed to the Q2-Q4, 2022, phase of the bearish recession.

- The drama around the now-defunct crypto exchange FTX and the associated trading firm Alameda Research was the largest centralized service collapse across 2022.

- Despite the largest hacks being widely discussed in the media, the vast majority of cryptocurrency scams are organized via old methods: fake airdrops, malicious “recovery programs,” scam arbitrage schemes and the like.

- A number of major hacks appeared to be white-hat operations: attackers returned the money stolen in exchange for impressive bug bounties.

- Almost 12% of all BEP-20 tokens and 8% of ERC-20 tokens are fraudulent; 350 new cryptocurrency scams are launched daily.

In this review, we will refer to purposefully launched frauds and projects that were initially legitimate as “cryptocurrency scams,” while “hacks” are third-party attacks on legitimate projects executed without “insider job” events.

Top Cryptocurrency Scams and Collapses of 2022

In 2022, Bitcoin (BTC), Ethereum (ETH) and all major cryptocurrencies lost over 70-80% from their ATH, while in most affected segments — metaverse tokens, GameFi tokens, the Solana (SOL) ecosystem — the median loss exceeds 90%. Some crypto majors failed to survive such a painful drop.

FTX

The collapse of Sam Bankman-Fried’s cryptocurrency exchange FTX and its associated crypto investing firm Alameda Research was the most surprising drama in Web3: SBF and his team attempted to gain enormous control over the industry by signing dozens of partnerships, appearing

on Forbes' covers and so on.

However, the balance sheet of Alameda Research depended heavily on FTX Token (FTT), the native cryptocurrency of FTX. That's why the whole system collapsed when Binance CEO Changpeng "CZ" Zhao started aggressively selling FTT (over $500 million in equivalent was released by CZ).

Just like in all similar cases, investors started mass withdrawing their money from FTX. The platform stopped the withdrawals, SBF stepped down as CEO and filed for bankruptcy. Meanwhile, it became known that he was using investors' and customers' money in his own trading firm, Alameda Research. Due to terrible mismanagement, Alameda Research was well underwater. SBF was arrested and released on bail while the realized losses from the FTX collapse peaked at $9 billion in equivalent.

Terra (LUNA)/Terra USD (UST)

EVM-compatible smart contract platform Terra was among the most overhyped Ethereum killers of 2021. However, the lion's share of its TVL was concentrated on Anchor Protocol, a simple yield farming machine that offered a 19% APY on deposits in Terra USD, Terra's now-defunct USD-pegged stablecoin. In total, more than $20 billion in equivalent was locked in Anchor in Q1, 2022.

However, in early May 2022, someone started aggressively sending UST to pools on the Curve Finance (CRV) DeFi and exchanging the tokens on USD Coin (USDC). UST lost its peg. Terraform Labs and its CEO Do Kwon started injecting liquidity into the UST/LUNA mechanism. However, due to a massive capital run, both LUNA and UST dropped to almost zero values. The Terra blockchain was halted for good.

As covered by U.Today previously, researchers unveiled that it was Terraform Labs that initiated the collapse: massive UST transfers were authorized by Do Kwon. The Terra founder allegedly ran to Serbia and is trying to cash out his Bitcoins there.

Three Arrows Capital

Launched by Su Zhu and Kyle Davies, Columbia University alumni and Credit Suisse veterans, Three Arrows Capital (3AC) was among the most influential crypto hedge funds. It amassed over $20 billion in AUM thanks to being an early investor in Ethereum, Avalanche (AVAX), Solana and others.

However, collapsed LUNA was one of the key elements of the 3AC portfolio. The team invested over $600 million in Terra LUNA: this massive stake was erased in two weeks after the LUNA/UST collapse.

On June 16, 2022, FT announced that 3AC had failed to meet its margin calls due to losses in Terra's Anchor Protocol. The firm was also underwater in its positions in Staked Ether (stETH) in the Lido Finance (LDO) DeFi and in Grayscale Bitcoin Trust (GBTC). In June it failed to repay its loan to crypto giant Voyager. In late July the firm was liquidated by a BVI court while the 3AC management filed for bankruptcy. In total, 20 investors in 3AC lost over $3.5 billion.

Voyager

U.S.-registered creditor Voyager also fell victim to poor risk management: it provided a $650 million unsecured loan to Three Arrows Capital while its net AUM was almost $5.9 billion. The platform boasted 3.5 million customers, 97% of whom invested less than $10,000.

In general, Voyager collapsed due to the fact that its team chose a risky business strategy: it offered loans to multiple trading services and individual cryptocurrency traders. As lenders started withdrawing their money en masse, in early July, Voyager froze customer funds. A few days later, it filed for bankruptcy protection in New York.

As the platform was focused on small-sized retail customers, its collapse was the most painful for cryptocurrency enthusiasts.

Celsius

Celsius was, in fact, the first firm to signal about its problems: in April 2022 the platform announced that it will hold all assets of non-accredited investors in custody: this part of customers was therefore unable to inject new liquidity and get rewards.

In May 2022, scared by the UST and Terra dramas, users started moving money out of the Celsius protocol. On June 12, 2022, Celsius froze the funds of 1.7 million customers (mostly retail investors). Just like Voyager, it filed for bankruptcy in early July.

On July 14, 2022, Celsius' legal advisor Kirkland & Ellis shared that the platform's leaders were informed about a $1.3 billion hole in its balance sheet.

Top Crypto Hack of 2022

As per an analysis of Merkle Science cybersecurity experts, cross-network bridges are particularly vulnerable to exploits due to their technical complexity and highly experimental character.

Bridges between chains are often more susceptible to exploits as they require more interactions and contract approvals than the other protocols. Additionally, bridges are more susceptible to attacks as they are run by unaudited computer codes. Moreover, the identities of validators/nodes, who run the transactions are also unknown.

In 2022, bridges were the primary targets of attacks, while other DeFi mechanisms were also exploited by hackers.

Wormhole

On Feb. 3, 2022, hackers attacked Wormhole, a bridge designed to facilitate seamless value transfer between heterogeneous blockchains. Due to a vulnerability in code, they managed to issue 120,000 Wrapped Ethers (wETH) on the Solana blockchain without putting up the corresponding Ethereum collateral.

The hack could lead to insolvency of any DeFi platform that would be ready to accept 120,000 wETH (printed out of thin air) as a collateral. Fortunately, the worst-case scenario did not happen.

Jump Crypto, the parent company of the Wormhole service, took all the losses: they immediately replenished 120,000 Ethers to the protocol liquidity pools.

Ronin

On March 23, North Korean hackers from Lazarus, an infamous state-backed cyber criminal group, attacked the Ronin network. Ronin is an Ethereum-like sidechain developed specifically for Axie Infinity, a flagship GameFi. Attackers drained Ronin of a whopping $568 million.

Hackers managed to gain control of five out of nine validator signatures for Ronin Bridge. Then they authorized two transactions, 173,600 Ether and 25.5 million USD Coin. Out of this monstrous loot, over $445 million was laundered via the Tornado Cash crypto mixer.

Axie Infinity developer Sky Mavis raised extra funding, ordered another security audit by CertiK and increased the multisig threshold from 5/9 to 8/9.

Beanstalk

On April 16, 2022, Ethereum-based stablecoin project Beanstalk (BEAN) was targeted by a sophisticated flash loan attack. Namely, malefactors managed to get a flash loan on Aave Finance (AAVE) and buy the amount of governance tokens necessary to seize control over the protocol on-chain referendums.

Then the attackers gained the voting supermajority and approved a money transfer to their own account. When $180 million was transferred, they immediately repaid the flash loan; the net profit exceeded $80 million.

Nomad

In August 2022, Nomad, a multi-chain bridge mechanism that moves value between Avalanche, Ethereum, Evmos (EVMOS), Moonbeam (GLMR) and other blockchains, was drained of $190.7 million in crypto. Attackers managed to exploit a vulnerability of the smart contract design: the protocol allowed users to withdraw funds on the target blockchain without checking whether they were equivalent to the initially deployed amount.

Simply put, after the regular upgrade, users were able to deposit 1 ETH on Ethereum and ask for a 100 Ethereum equivalent withdrawal from Avalanche.

The thing is, every tech-savvy Web3 enthusiast had been able to replicate this attack vector and steal funds from Nomad before the patch was released. As such, many Ethereum developers withdrew funds just to send them back to the Nomad team: almost $40 million were sent back.

Wintermute

In September 2022, Wintermute, one of the largest market-making platforms, had its wallets drained for $160 million. Attackers unveiled that some of Wintermute's key wallets were created with Profanity, a generator of "vanity addresses" for the Ethereum network. Such programs can create crypto wallets with human-readable addresses, e.g., 0xJohnDoe1111… and the like.

Due to a vulnerability in Profanity's design, the attackers managed to brute-force the vanity addresses and recover private keys. The attack became possible due to significant compute resources utilized by malefactors.

Do Not Fall into These Long-Running Cryptocurrency Scams

Alongside sophisticated scenarios that include $1 billion flash loans, North Korean hackers and impressive hardware for brute-forcing, very primitive scam campaigns are popping up here and there. Three attack designs are very common in crypto as of 2022:

1. Fake airdrops. To run this cryptocurrency scam, malefactors either organize a YouTube advertising campaign or place their ad on Twitter. Then they announce that an Internet celebrity (Snoop Dogg), a top tech entrepreneur (Vitalik Buterin or Elon Musk) or even politician (Donald Trump) is airdropping cryptocurrency. All who are ready to claim their bonuses should either send an initial deposit (that would allegedly be returned with a 100% profit) or their private keys. Needless to say that both groups will lose their deposits or all money from their wallets.

How to protect yourself: Never send your money to “airdrop organizers” or disclose your private keys or seed phrases.

2. Handmade MEV bots. Maximal extractable value (MEV) is the maximum reward Ethereum network participants can get for their contribution in the process of block validating. Sophisticated techniques allow us to benefit from optimizing MEV. Scammers place video or text manuals on how to build your own “MEV bots” in order to get access to Ethereum wallets and drain funds.

How to protect yourself: Avoid “instant” MEV bots from YouTube manuals.

3. Scammers come to the rescue. As 2022 is definitely a year of hacks, many crypto users are checking whether their favorite blockchains are broken. Scammers are posting fake announcements about this or that project being hacked and launch fake “compensation” programs. All interested in compensation are asked to send their seed phrases to scammers.

How to protect yourself: Only check news about hacks on official media channels of blockchains.

Conclusion

In 2022, most crashes were triggered by the painful plunge of crypto prices, poor risk management and greed of the owners of centralized crypto products. That's why decentralization is a big deal: the crowd wisdom of a DAO would prevent FTX/Celsius/3AC-scale crashes from happening.

In the meantime, on-chain products should pay attention to security audits, updates and private jet management.

Read More:

How to Buy Bitcoin in 2023?

Is Ethereum a Good Buy in 2023?

Bitcoin Futures Trading for Beginners

Pi Network Launch Date: When Will Pi Coin Enter The Market?

Is Pi Network Legit Or Scam: Pi Coin Real Or Fake?

Luna Classic Price Prediction: Will Luna Classic Reach $1?

LUNA Classic Burn: Will LUNC Burn Its Supply?

Shibarium Burn: Will the Burn Remove 111 Trillion SHIB Annually?

Bonk Airdrop: Where to buy Bonk crypto

Gasoline Price Prediction: What Will It Be In Five Years?

NIO Stock Forecast 2025, 2030: Is NIO a Good Stock to Buy?

ADA Cardano Price Prediction 2025, 2030

Ethereum Price Prediction 2025-2030

HBAR Price Prediction 2025, 2030

CRO Crypto Price Prediction 2025: Will CRO Coin Reach $1?

Metamask Airdrop – To Get $MASK Token for Free?

Leverage in Crypto Trading: Something You Need to Know

Best Crypto Leverage Trading Platform for 2023

BTCC Sign up – How to Register an Account on BTCC

BTCC Crypto Futures Trading Guide