coingecko

2026 State of Crypto Security Report

Sponsored by

Toobit

Content

Introduction	2
Crypto Hacks & Breakdown by Attack Vector	3
Top Crypto Attack Vectors Comparison	4
Smart Contract Exploits	5
Oracle & Price Manipulation	6
Supply Chain & Infrastructure Exploits	7
Social Engineering & Private Key Compromise	8
Crypto Security Audits	9
On-Chain Insurance Protocols	10
CEX Insurance Funds	11
On-Chain Security Measures	12
CEX Security Measures	13
Summary Conclusion	14

Zhong

Head of Research

Win Win

Research Analyst

coingecko Research

© 2026 CoinGecko

Introduction

As the crypto space continues to mature, both centralized and decentralized platform have remained on the forefront of providing the highest level of security to safeguard user assets as well as protect users from the plethora of attack vectors that exist today. Unfortunately, despite the numerous improvements in security measures and risk mitigation protocols, the industry has continued to suffer escalating losses due to hacks and exploits, with over $2.5B stolen in 2025 alone.

Across these incidents, the attack vectors vary between centralized and decentralized infrastructure. On the CEX side, private key exposure remains the single largest point of failure, while on-chain protocols are more vulnerable to smart contract errors that can be manipulated to undermine their integrity. However, these vectors are just the tip of the iceberg as more recent exploits have shown that hackers are quickly adapting their methods of gaining unauthorized access by utilizing fake user interfaces for multi-sig signing and malicious integrations.

Although the tactics employed by malicious actors have constantly evolved, it's worth noting that the relevant actors have also transformed dramatically; while older exploits tend to be executed by smaller teams of rogue individuals, organized crypto cartels and syndicates, included state-sponsored hackers from North Korea, are now largely responsible for most of the hacks that occurred in the past year. Combined with more sophisticated usage of mixers, bridges and staggered withdrawals to cover their tracks, this new generation of hackers have notoriously become difficult to trace.

With that said, this report seeks to examine the current level of state of crypto security in 2026, highlighting and providing deeper insight on the different kinds of hacks that today's platforms constantly face. **Additionally, we will also take a closer look at the effectiveness of smart contract auditing, the necessity of crypto insurance protocols and the various security features utilized by CEXes such as Toobit to protect users at all times.**

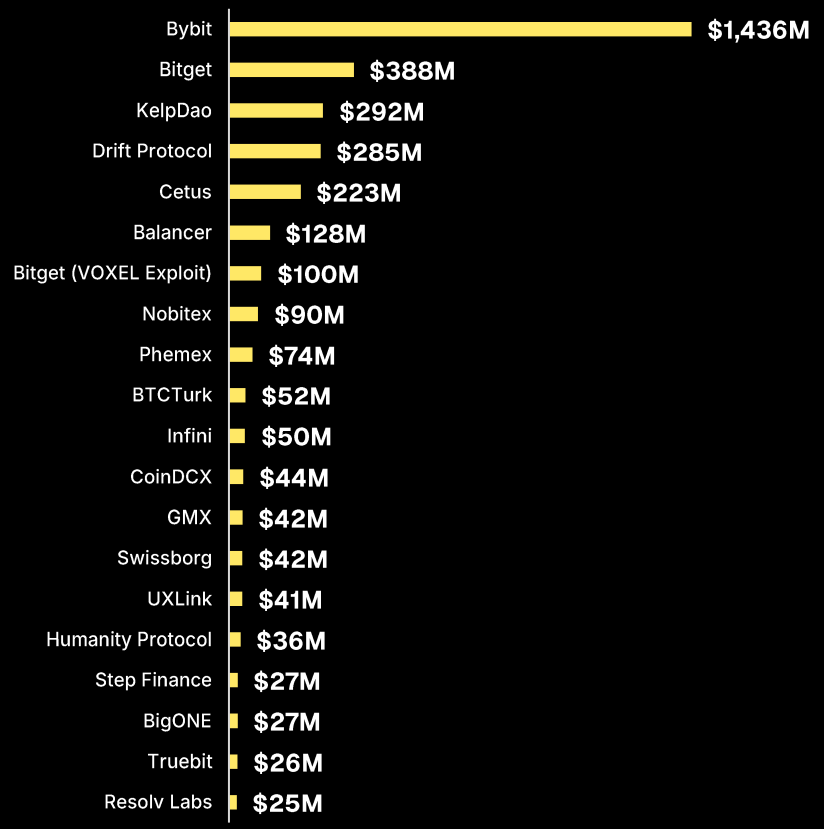
© 2026 CoinGecko

coingecko Research

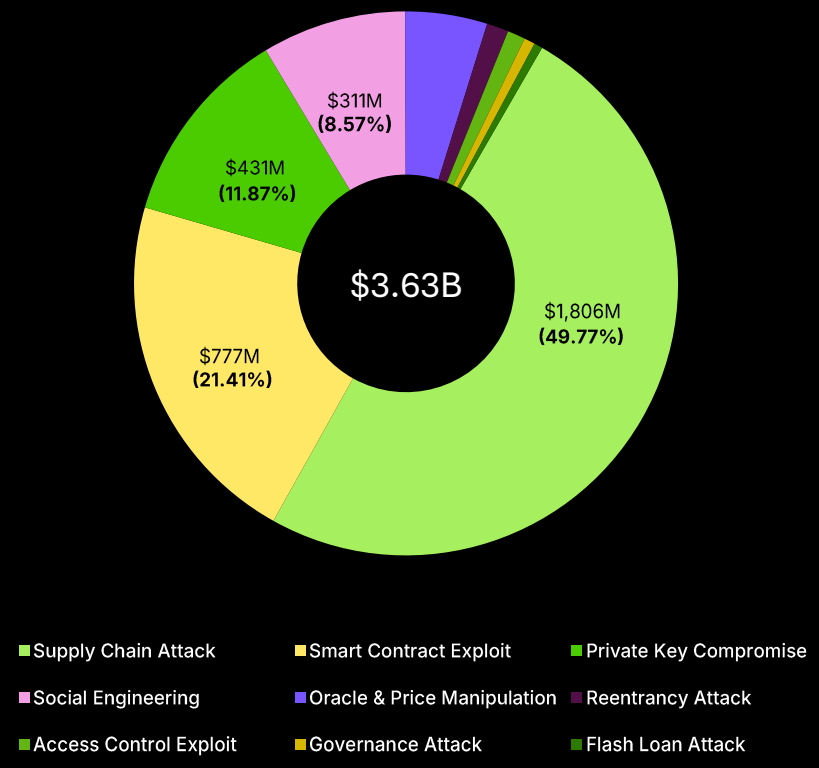
Crypto Hacks & Breakdown by Attack Vector

Since the start of 2025, crypto platforms have lost over $3.63B, largely due to supply-chain attacks, smart contract exploits and stolen private keys.

Top 20 Largest Crypto Exploits (2025-2026)



Crypto Exploit Breakdown by Attack Vector* (2025-2026)



In recent years, the frequency of crypto-specific exploits have exploded like never before. Over the past 19 months, crypto platforms lost $3.63B worth of funds across 245 incidents. Of the total amount, more than 72.5% was stolen in the top 10 largest attacks since 2025.

Across both CEXes and DEXes, supply chain or infrastructure attacks have resulted in the most damage thus far, with over $1.8B lost to these types of attacks such as the Bybit and KelpDAO hacks.

Different platforms are more vulnerable to specific exploits. For CEXes, compromised private keys to exchange wallets were the most common point of failure, while dApps lost $546M to smart contract exploits.

However, both types of platforms still succumbed to market and oracle manipulation caused by errors from internal mechanisms, such as Binance and Hyperliquid.

Source: DeFiLlama & supplemented by credible news coverage

*Includes 245 recorded crypto exploits that occurred from January 2025 to September 2026

© 2026 CoinGecko

coingecko Research

Top Crypto Attack Vectors Comparison

Vector	Mechanism	Number of Hacks (2025-2026)	Notable Hacks	Main Targets
Smart Contract Exploit	The attacker finds and exploits a bug or logic flaw in a smart contract's code to drain funds directly	135	Cetus Protocol : $223M Balancer: $128M	Decentralized protocols, cross-chain bridges and CeDeFi applications
Oracle & Price Manipulation	The attacker distorts a price feed to trick a protocol into mispricing collateral or triggering false liquidations	22	Bitget (VOXEL exploit): $100M Hyperliquid: $12M	On-chain price oracles , low liquidity orderbooks and trading pools, lending protocols, perpetuals and yield vaults
Supply Chain Attack	The attacker breaches a vendor, dependency, or cross-chain bridge integration rather than the target directly, exploiting insufficient verification between systems	9	Bybit: $1.44B KelpDAO: $292M	RPC nodes, multi-signing interfaces, extensions, third-party dependencies and software development kits (SDKs)
Private Key Compromise	The attacker gains control of a wallet's private keys, giving them access to transfer or withdraw funds from user accounts	33	Nobitex: $90M Phemex:$73.5M	Particularly CEXes, but private keys of DEX wallets and important individuals can also be targeted
Social Engineering	The attacker impersonates a trusted party via fake sites or malware to extract sensitive information or execute malicious acts such as listing fake tokens or signing fraudulent transactions.	5	Drift*: $285M Ionic: $6.94M	Core team members, protocol signers, developers and insiders

© 2026 CoinGecko

Source: CoinGecko

* Drift has rebranded to Velocity after the exploit

Smart Contract Exploits

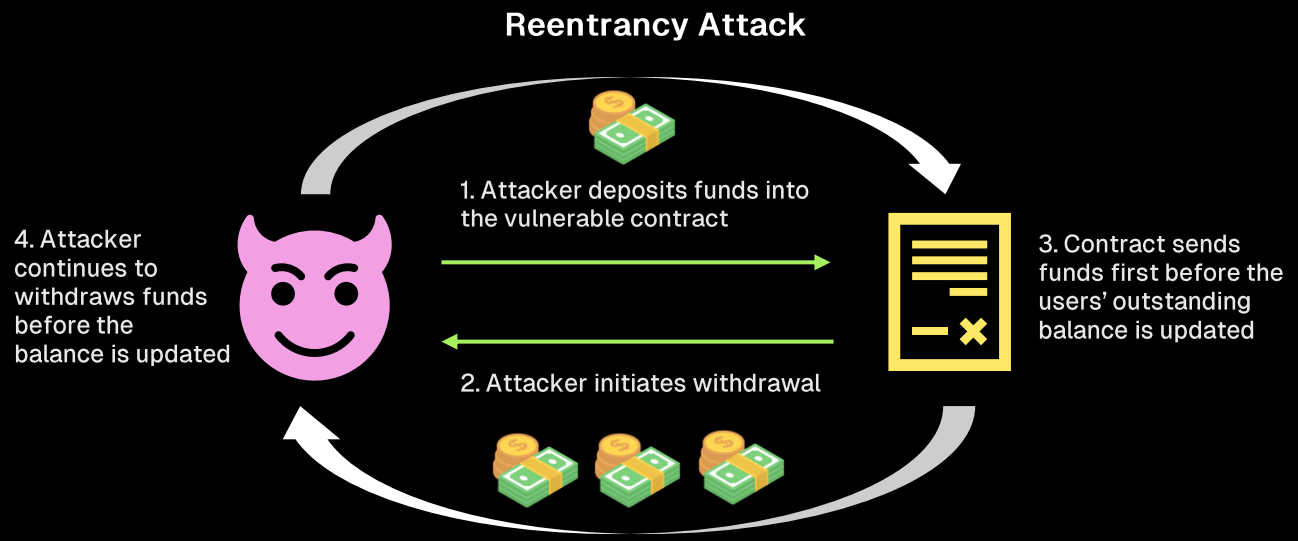
Code flaws in smart contracts allow malicious actors to circumvent the intended logic of a protocol, allowing them to set new parameters or transfer funds without authorization.

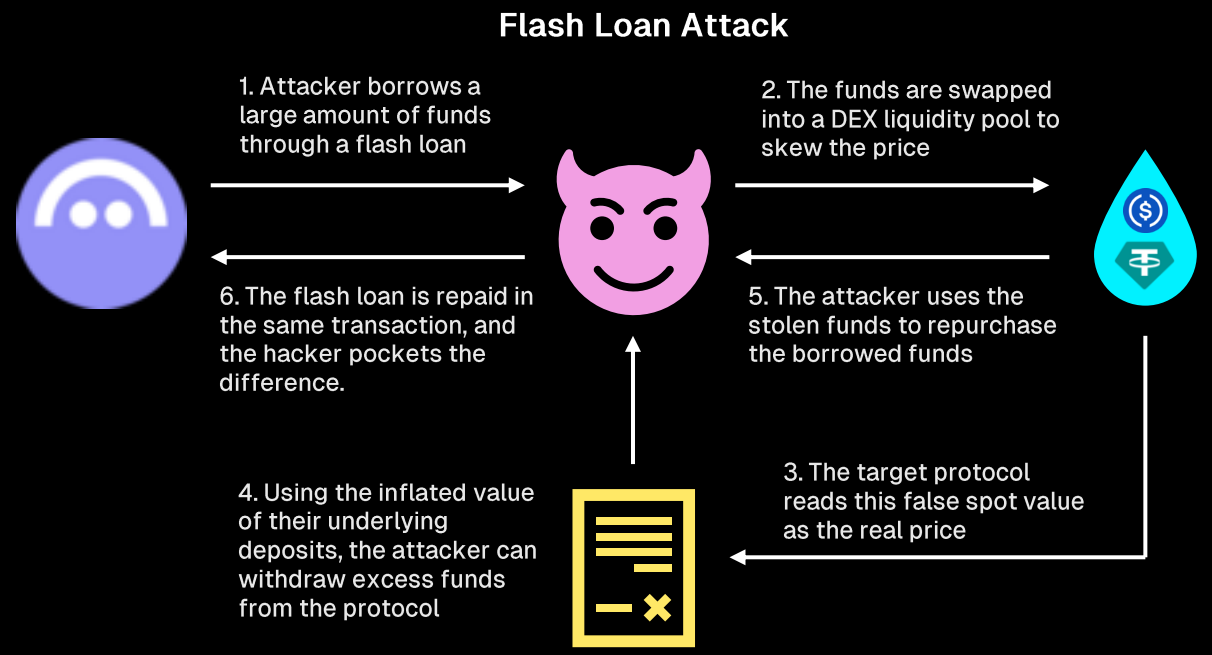
While smart contracts are normally coded to perform specific functions as intended, the immutability of these contracts also means that hackers can leverage on flaws in the contract's logic, such as rounding and accounting errors, to trigger unintended actions.

The most common smart contract exploits include reentrancy and flash loan attacks, where over $54M have been stolen through both types of exploits since the start of 2025.

While flash loans themselves are an integral feature of lending protocols, it is often used to drain vault contracts, manipulate prices (*see Slide 6*) or raise funds to commit a larger exploit. Additionally, both reentrancy and flash loan exploits typically occur in a single transaction, leaving little to no time for victims to intervene.

However, it's worth noting that decentralized protocols are not the only targets of smart contract exploits; CEXes are also exposed through misconfigured wallet contracts and vulnerable CeDeFi integrations.





Source: CoinGecko

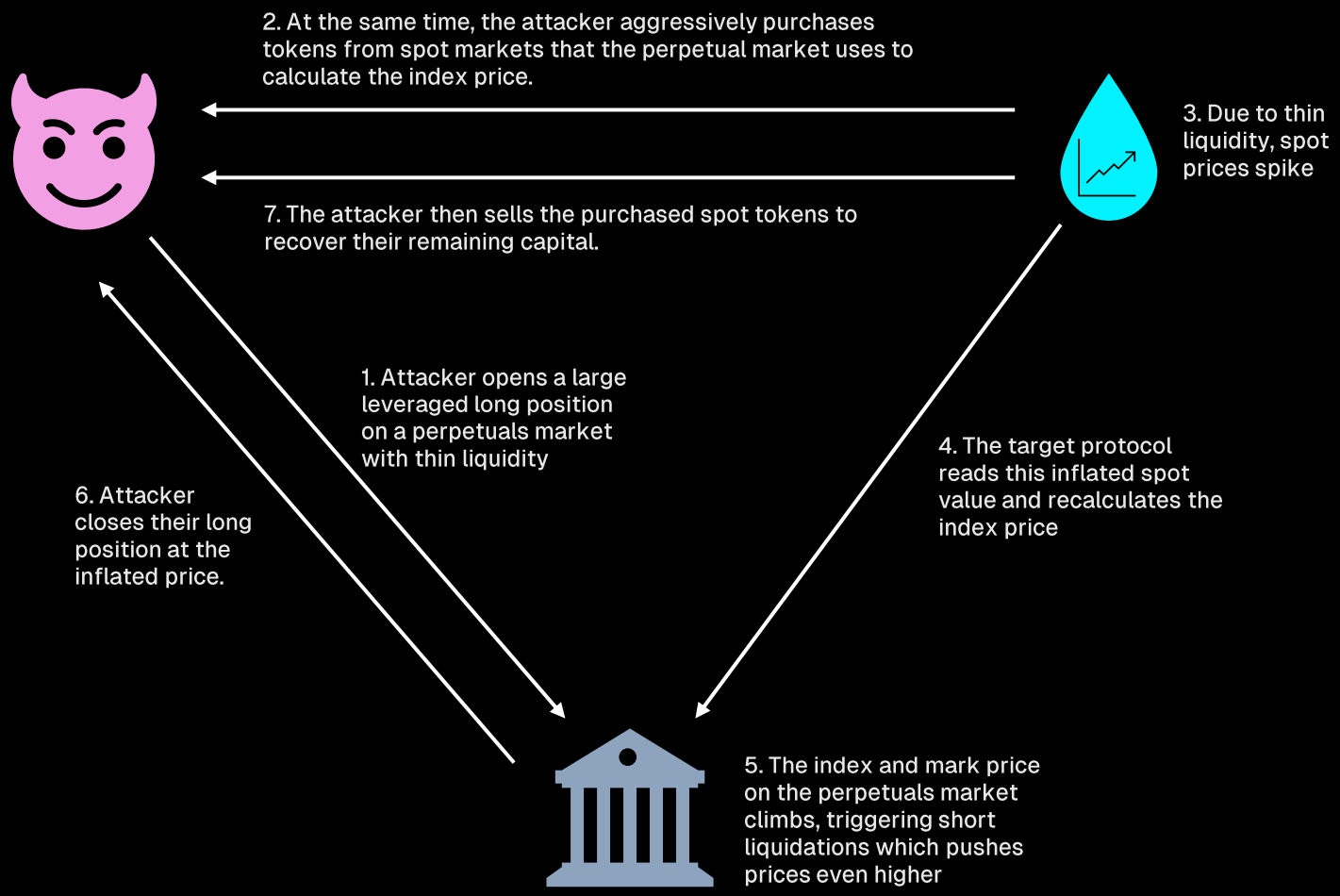
© 2026 CoinGecko

coingecko Research

Oracle & Price Manipulation

While decentralized protocols are more susceptible to oracle attacks, prices on CEX perpetual markets can also be manipulated through vulnerable external sources.

Price Manipulation on CEX Perpetuals



A crypto oracle is a data feed that sources, verifies, and transits external data to on-chain smart contracts or centralized platforms. However, it's important to note that the oracle is not the data source itself but merely retrieves and verifies the data. This allows malicious actors to manipulate the data to trick weak oracle feeds.

When token prices moves weak oracle setups on DEXes or lending protocols that rely on only one oracle will interpret it as the correct data, leading to inflated collateral values or miscalculated liquidations.

While CEXes don't generally use oracles, the perpetuals market utilizes external spot prices to determine index price for less liquid tokens, which opens additional vectors for hackers to exploit. Besides that, centralized platforms tend to feature more complex methods in price manipulation through coordinated pump-and-dump schemes and automated market-making bots.

A newer variant of this type of exploit has also affected prediction markets such as Polymarket, where the relevant oracles were influenced through governance votes or physical tampering, causing the wager markets to settle wrongly.

Source: CoinGecko

© 2026 CoinGecko

coingecko Research

Supply Chain & Infrastructure Exploits

Instead of a direct attack, exploiters often find alternative points of entry through various firmware and integrations that crypto platforms rely on.

Breakdown of the 2025 Bybit Hack

Lazarus Group hackers gain access to a developer's workstation/environment for the Safe multi-sig wallet

After two weeks of unauthorized access and reconnaissance, hackers inject malicious JavaScript code into the Safe multi-sig user interface

Two days later, Bybit operators initiate routine ETH transfer from cold to warm wallets

Signers are shown legitimate transaction details in the Safe user-interface, while hiding the malicious transaction

All the required signers unknowingly approve the transaction, allowing the attacker to gain control of the multisig wallet

Hackers steal over $1.4B in ETH and ETH derivatives to other wallets and exchanges

Source: NCC Group

A supply chain attack is where attackers target weak infrastructure or dependencies that a protocol relies on, rather than the actual protocol itself. This includes different tech-specific components such as compromised packages, scripts or developer environments.

In the crypto space, hackers have become more prolific in targeting crypto-specific elements within platforms such as multi-sig wallets and RPC nodes.

For example, the most recent attack against Bitget in September 2026 resulted in over $388M in losses as hackers were able to exploit a vulnerability in the platform's wallet infrastructure to execute fraudulent transfers. However, the platform was able to utilize its Protection Fund to make users whole.

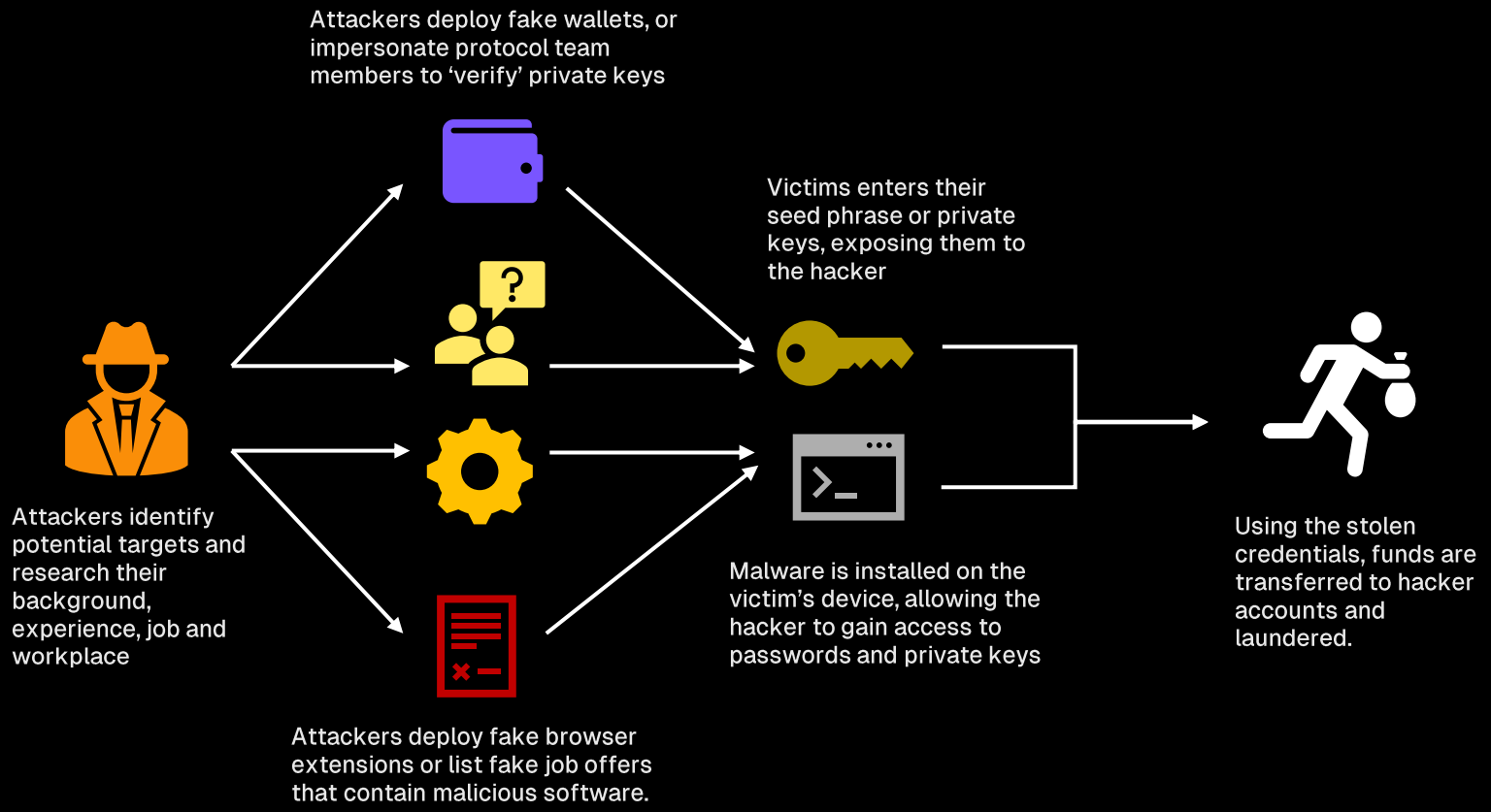
However, protocols should also be responsible for configuring their existing setup to mitigate risks against potential attacks. In both the Bybit and KelpDAO exploits, the lack of additional verification or failsafes for transaction validation was the key point of failure that enabled hackers to drain funds.

© 2026 CoinGecko

coingecko Research

Social Engineering & Private Key Compromise

Social engineering is one of the most common crypto attack vectors but also the most difficult to defend against, often targeting a protocol's core personnel to acquire sensitive information



Among all other crypto hacks, social engineering is still one of the most crucial entry points for hackers, often serving as the gateway for subsequent supply chain and access control exploits.

Unlike other security breaches, which can often be solved with upgrades and hotfixes, both social engineering and private key compromises target the human aspect, which can take place over a very long duration and requires constant vigilance.

Attackers can utilize various methods to gain access to insider credentials and private keys such as sending targeted spear-phishing links and malware to high-ranking protocol employees or even masquerading as other known team members.

In recent times, these tactics have become even more sophisticated, evolving from single target to complex multi-prong attacks to gain a victim's trust. These strategies aim to bolster the hacker's legitimacy and urgency in obtaining access to sensitive information, forcing the victim to panic and give in before performing additional verification checks.

Source: CoinGecko

© 2026 CoinGecko

Crypto Security Audits

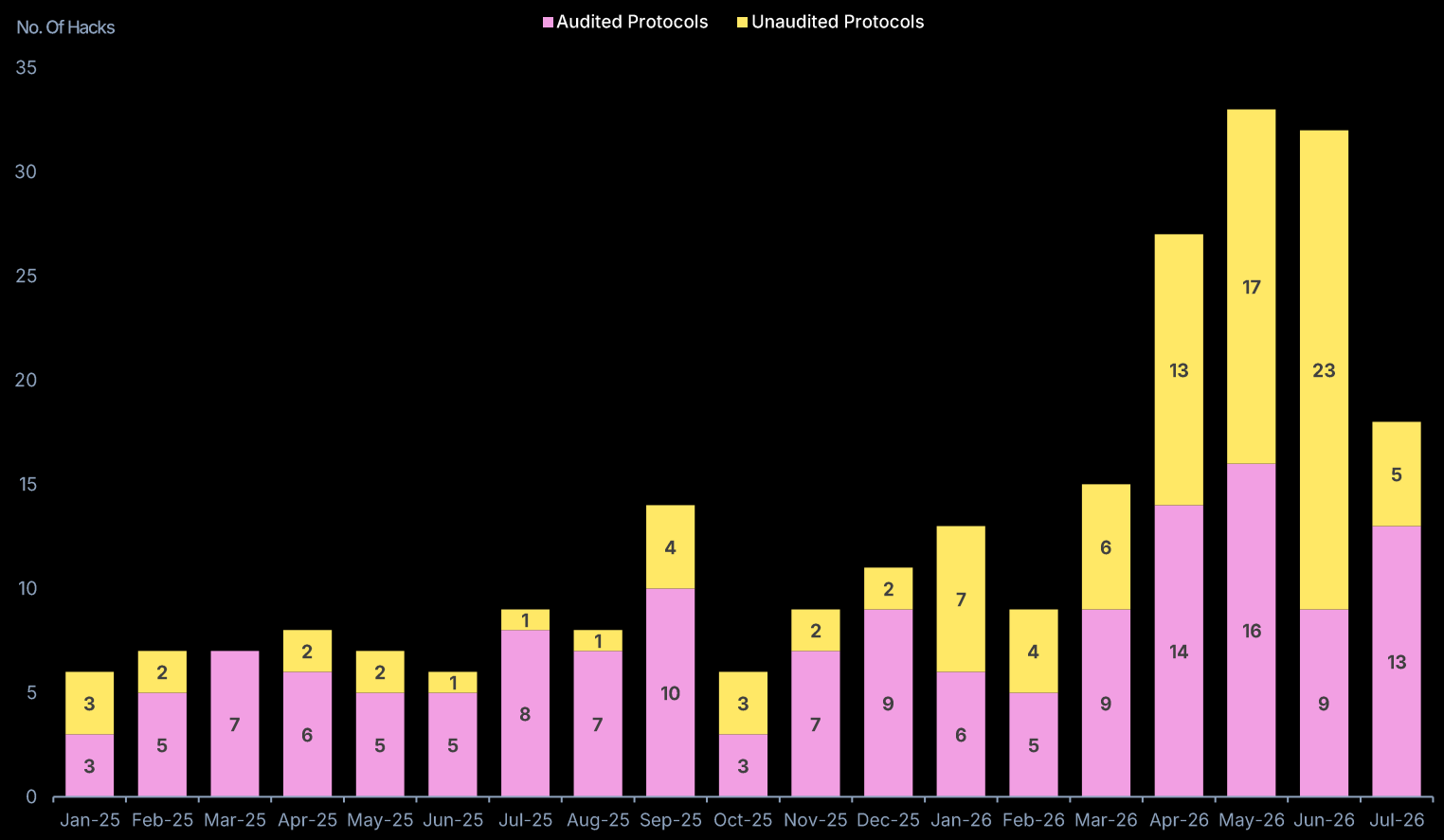
Approximately 60% of exploited crypto platforms had completed independent security audits, but most attacks are well beyond the conventional audit scope.

Of the 245 recorded incidents since the start of 2025, 147 of the affected protocols had been audited prior to their respective attacks, making up over 88.44% of the total funds stolen in the past 19 months.

Most of the exploits on audited protocols target components beyond the scope of standard smart contract audits, newly introduced code that was not part of the original audit, or abusing features that work as intended (governance attacks). Notably, just under 11.0% of the audited protocols suffered in-scope attacks, losing $396.0M in the process.

While CEXes don't generally complete the same types of audits as their decentralized counterparts, they are often required to undergo strict compliance checks, financial audits and provide Proof-of-Reserve attestations to maintain user safety. However, this does not guarantee immunity to other exploits such as social engineering and private key compromise.

Audited vs Unaudited Protocol Exploits (Jan 2025 – Jul 2026)*



Source: DeFiLlama, and other verifiable sources.

*Some unaudited protocols may have completed audits in private.

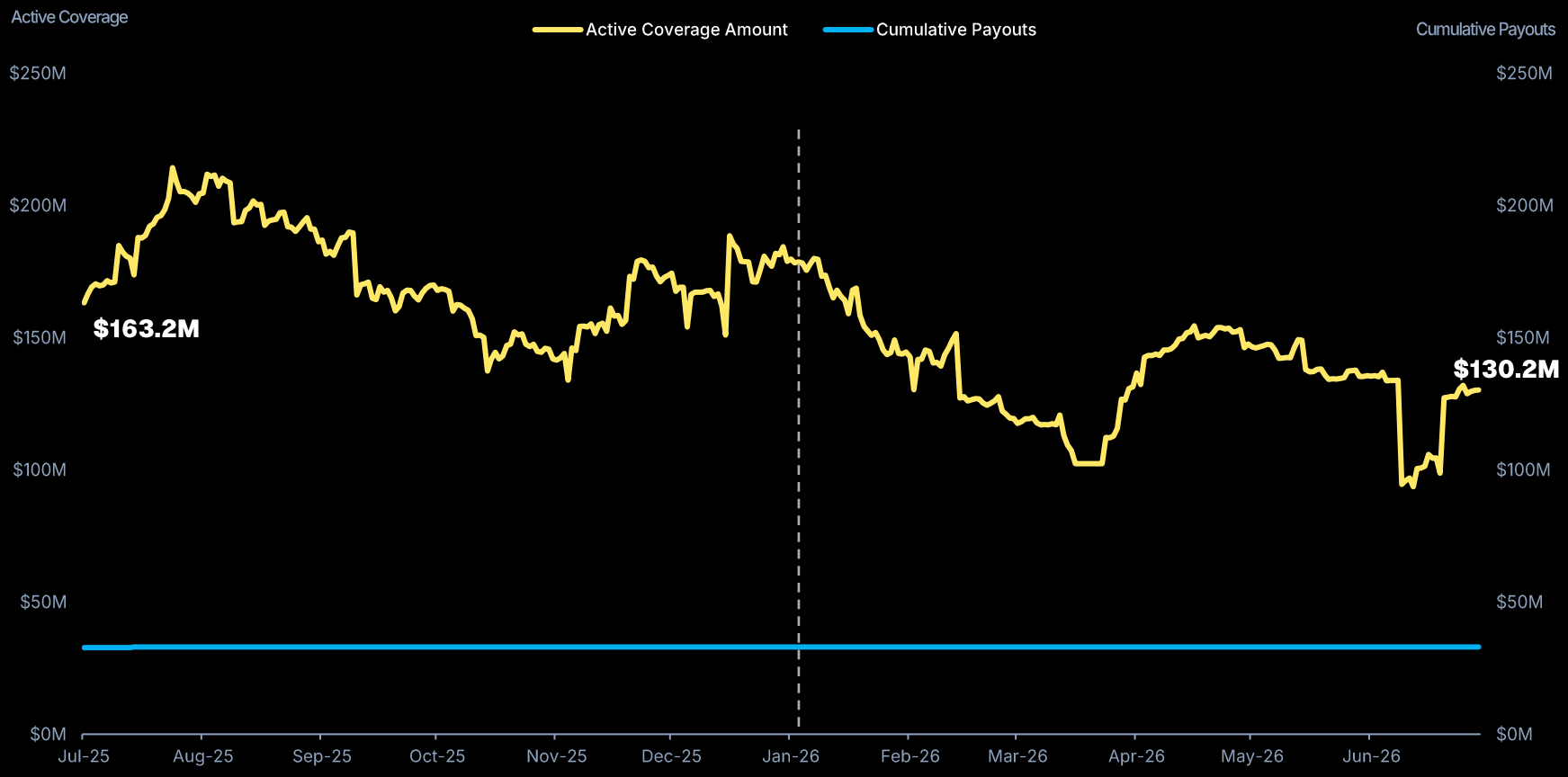
© 2026 CoinGecko

coingecko Research

On-Chain Insurance Protocols

Crypto insurance platforms offer monetary protection against smart contract failures and de-pegging events but carry the same hurdles for claimants as their traditional counterparts.

Active Coverage on Top 9 On-Chain Insurance Protocols vs Cumulative Payouts (Jul 2025 – Jul 2026)*



Despite the rise in exploits, active coverage on the top crypto insurance protocols have steadily decreased by -20.2% from $163.2M to $130.2M, while cumulative payouts have largely remained stagnant at $33.0M.

This is likely due to already-heightened risk levels with the crypto space, which has discouraged users from providing capital as well as purchasing premiums at elevated prices.

Furthermore, the scope of crypto-based protection can be extremely restrictive, limiting claims to only verified smart contract exploits or infrastructure failures. Users may be unable to receive a payout if the exploit stems from human error, compromised private keys or general market volatility.

As such, the demand for on-chain cover has never truly entered the limelight; as of August 2026, 5 of the 9 on-chain insurance protocols have gone inactive or pivoted to other segments.

Source: OpenCover

*Includes Nexus Mutual, Chainproof, Sherlock, LunosDAO, Unslashed Finance, InsureDAO, Risk Harbor, Neptune Mutual & Ease.

© 2026 CoinGecko

coingecko Research

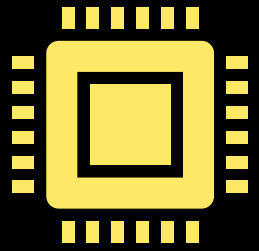
CEX Protection Funds

Platform	Mechanism	Assets Held	Total Fund Value*
Toobit Shield Fund	• Launched by Toobit in October 2025 with as a $50M dedicated reserve pool protect users from platform-related losses. • Protection is standard for all users with regardless of account size and volume. • Users can monitor Shield Fund assets in real-time across 4 dedicated wallets.	BTC ETH USDT USDC	~$41.2M
Binance Secure Asset Fund for Users (SAFU)	• Originally established in July 2018 to protect user assets from exploits on Binance's internal mechanisms or security protocols. • A portion of trading fees are allocated to the fund and stored in a secure dedicated cold wallet. • The reserve will be replenished backed to $1B should the total value of the fund falls below $800M due to Bitcoin's price movements.	BTC	~$1.25B
MEXC Guardian Fund	• Launched in June 2025 to boost platform safety and user trust. • The Guardian funds covers incidents such as platform security breaches and technical issues. • All related fund addresses are published publicly and can be monitored on-chain.	USDT	~$101.6M
Bitget Protection Fund	• Originally deployed in August 2022 with $200M of funds consisting of 6000 BTC and $80M USDT. • In the aftermath of FTX's collapse, Bitget has increased the minimum fund threshold to $300M. • Currently holds ~3,067 BTC as a large portion of the funds were used to reimburse users after the exploit on September 24.	BTC	~$255.5M
BingX Shield Fund	• Launched in June 2025 as a permanent, fully self-funded reserve covering platform-side incidents. • Reserve wallets are published on the Shield Fund page for on-chain verification and regular external audits.	BTC ETH USDT	~$133.7M
WEEX Protection Fund	• Fully backed by WEEX and kept strictly segregated from operational funds, so eligible losses are covered directly rather than through external processes. • Wallet addresses are published for on-chain verification.	BTC	~$83.4M

Data as of 29th September 2026
© 2026 CoinGecko

On-Chain Security Measures

Decentralized protocol utilize a multi-layered approach to ensure that are all potential vectors – from the smart contract level to the human aspect – are well protected.



Smart Contract Protection

- Running multiple independents audits, ensuring that new code changes are within scope.
- Implementing extensive timelocks on key smart contract functions, allowing ample time for watchers to raise the alarm and respond.
- Formal verification of smart contract logic to ensure they work as intended.
- Constant bug bounty programs that are meaningful to incentivize participation instead of exploitation.
- Ensure that dependent smart contract tooling is up-to-date.

Protocol-Level Protection

- For lending platforms, markets are isolated with sufficient supply and borrowing caps to mitigate risks of bad debt.
- Using multiple weighted oracles to derive mark and index prices help perpetual DEXes to mitigate price manipulation.
- Implementation of withdrawal delays for abnormally large fund transfers.
- Constant automated on-chain monitoring to detect anomalous calls and trigger the appropriate defense mechanisms.
- Setting up an insurance fund to mitigate shortfalls and reimburse users post-attack.

Access Control

- Funds are stored in multisignature wallets, with access limited to dedicated hardware.
- Delegated control between core team members, and no individual person can deploy protocol upgrades.
- Encrypt sensitive data and enable redundant authentication measures for additional verification.
- Setting up a separate Security Council with access to implement emergency measures should all core member are compromised.

© 2026 CoinGecko

coingecko Research

CEX Security Measures

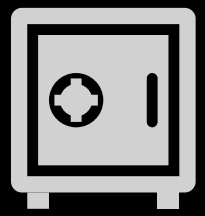
CEXes such as Toobit incorporate multiple features to mitigate security risks such as isolated wallets, the Shield Fund and real-time monitoring to safeguard user assets against vulnerabilities.

User Account Security

- Two-factor verification with the option to add more verification methods.
- Standard know-your-customer (KYC) checks to tie identities to account access or trace stolen funds.
- Anti-phishing verification tools on Toobit help users confirm genuine links and channels.
- Withdrawal whitelisting prevents users from sending funds to non-approved addresses.
- Withdrawal delay for newly added addresses, providing time for users to be alerted.

Platform Security

- Verified security frameworks which are ISO and SOC2-certified.
- Constant audits and penetration testing on by multiple firms.
- Multi-layered infrastructure and private key protection with encryption and DDoS mitigation.
- Multi-cloud infrastructure for resilience and low-latency uptime.
- AI-powered on-chain monitoring which happens in real time, allowing Toobit to detect anomalous transfers.
- Toobit Shield Fund, which holds ~$38M, helps to reimburse users in the event of exploits.



Proof-of-Reserves

- Proprietary Bee-Safe defense system where over 90% of users assets are stored in cold wallets.
- User assets are backed 1:1 with real-time verification available.
- Proof-of-Reserves reports are published regularly and currently exceed 100% for BTC, ETH, USDC & USDT.

© 2026 CoinGecko

Summary Conclusion

- Despite the numerous security improvements that have been made in recent years, crypto platforms are still highly susceptible to hacks and exploits, losing over $3.63B across 245 separate incidents since 2025.
- The top attack vectors across both centralized and decentralized protocols include smart contract exploits, oracle & price manipulation, as well as private key compromises, with a cumulative total of 190 recorded attacks since 2025.
- Smart contract exploits enable hackers to take advantage of code flaws into opportunities to freeze or steel funds. Common methods include reentrancy attacks that repeatedly drains funds before a contract's state is updated or utilizing legitimate tools such as flash loans to drain significant vault balances in a single transaction.
- Although crypto oracles are crucial for bringing external data on-chain, the data itself can be falsified to manipulate lending, perpetual and prediction markets in the attacker's favor.
- Supply-chain attacks target a platform's infrastructure instead of the platform itself, relying on vulnerable dependencies and software as entry points, which can affect multiple platforms that utilize the same services.
- The human element in crypto is often the most under-looked attack vector but also the most dangerous, as malicious actors are have begun to use more varied and sophisticated social engineering techniques to convince victims to compromise their sensitive data and private keys.
- Smart contract audits are a key part of maintaining protocol security before deployment, but they are not completely fool-proof as narrow scopes and undocumented code changes could become potential points of attack; centralized platforms conduct their own strict set of compliance checks, ensuring their capability to offer the highest level of user protection.
- While on-chain insurance protocols could act as a safety net against potential hacks, the product has failed to gain real traction as a mainstream risk mitigation tool due to hefty premiums and restrictive terms.
- To further safeguard user assets against future vulnerabilities, CEXes such as Toobit have established their own protection funds as an additional safety net to provide seamless compensation against potential losses.
- To minimize potential attack vectors, decentralized protocols tend to complete extensive third-party audits, implement restrictions on unauthorized decisions and fund transfers, as well as diversify its exposure across external tools, wallets and team members.
- Similarly, centralized platforms layer user account controls, professionally certified infrastructure with regular audits, and reserve attestations to boost security and user confidence. Toobit's Bee-Safe framework utilizes these mechanisms in combination with cold storage custody, its robust Shield Fund and real-time AI monitoring to safeguard user assets.

© 2026 CoinGecko

Toobit

Toobit is the award-winning global cryptocurrency exchange serving over 4 million active traders. Established in 2022, the exchange features over 1,000 trading pairs and 500x leverage on major cryptoassets, alongside guaranteed zero-slippage copy trading.

Non-mandatory KYC

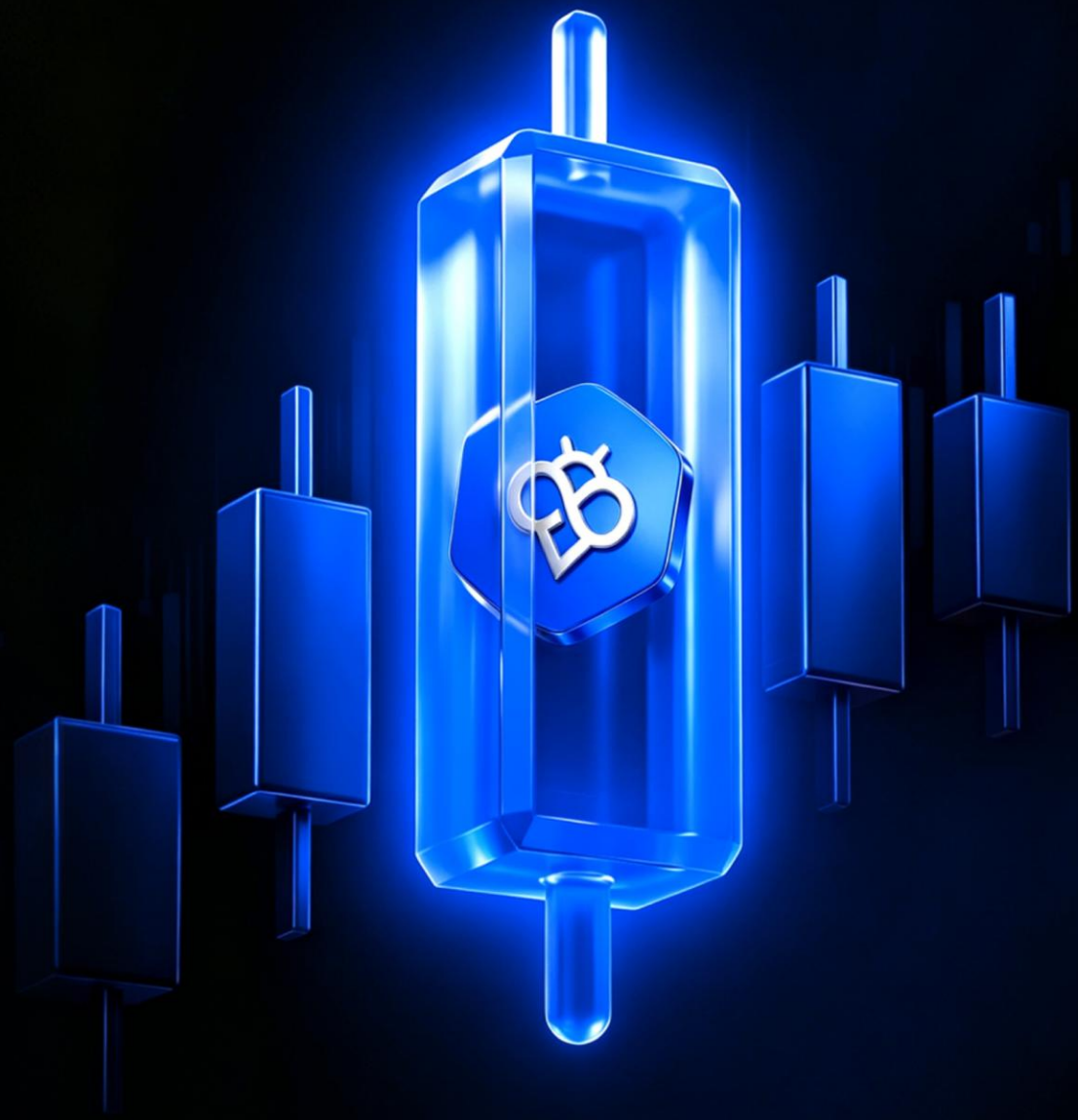
200+ TradFi pairs

ISO 27001-certified, audited by Hacken

$40M Shield Fund, 1:1+ Proof of Reserves

Better crypto trading starts here

www.toobit.com



coingecko Research

That's it.

We hope you enjoyed reading.

Follow us on:

2026 State of Crypto Security Report
© 2026 CoinGecko

coingecko

Disclaimer

All content provided herein our website, hyperlinked sites, associated applications, forums, blogs, social media accounts and other platforms (“Site”) is for your general information only, procured from third party sources. We make no warranties of any kind in relation to our content, including but not limited to accuracy and updatedness. No part of the content that we provide constitutes financial advice, legal advice or any other form of advice meant for your specific reliance for any purpose. Any use or reliance on our content is solely at your own risk and discretion. You should conduct your own research, review, analyse and verify our content before relying on them. Trading is a highly risky activity that can lead to major losses, please therefore consult your financial advisor before making any decision. No content on our Site is meant to be a solicitation or offer.