OKX Web3

Security White Paper

August 2025

Abstract

This white paper presents an in-depth overview of the security framework that underpins OKX's Web3 ecosystem, including the wallet, decentralized exchange (DEX), marketplace and related applications.

1 Introduction

The advance of Web3 technologies has ushered in a new era of financial innovation, characterized by decentralized finance (DeFi) platforms that offer open, permissionless access to financial services. Unlike traditional finance (TradFi), which relies on centralized institutions and intermediaries, DeFi operates through smart contracts on blockchain networks, eliminating the need for trusted third parties.

This paradigm shift enables greater financial sovereignty and inclusivity but also introduces unique challenges, including increased exposure to illicit activities and systematic risks. The permissionless and pseudonymous nature of DeFi necessitates novel approaches to security and risk management that extend beyond the frameworks established by Web2 or centralized financial systems.

OKX Web3 functions primarily as a technology service provider, offering tools and infrastructure to facilitate user interaction with decentralized networks. In this capacity, OKX Web3 does not engage in custodial activities or financial services. Recognizing the critical importance of security and compliance in the evolving DeFi landscape, OKX Web3 is committed to adopting proactive measures to safeguard users and uphold the integrity of the ecosystem. Our defense strategy is built on four core pillars:

- **OKX Internal Blocklist Program (On-chain risk intelligence and risk analytics)**
- **Address Screening & Blocking**

  Leveraging intelligence and data feeds from:

  ELLIPTIC   BLOCKSEC   Etherscan   SLOWMIST

- **Smart contract and application security**
  - Transaction simulation and verification, token security and URL screening by Blockaid
  - Domain abuse takedowns and brand protection by:

  Doppel   netcraft

- **Incident Response & Enforcement**

  Real-time detection, escalation, and mitigation mechanisms.

This white paper details how OKX Web3 addresses key risk vectors and enforces robust protections at both infrastructure and application layers.

2 OKX Internal Blocklist Program

The OKX Internal Blocklist Program is a multi-layered defense framework designed to proactively detect, classify, and block high-risk blockchain entities and transactions before they can cause harm to users or the ecosystem. It combines **real-time monitoring, behavioral clustering**, and **threat intelligence enrichment** to deliver fast and accurate risk signals across multiple chains and protocols.

1. Illicit Asset Transaction Monitoring

The **Asset Transfer Monitoring Service (ATMS)** tracks the movement of illicit funds and automatically clusters related wallet addresses controlled by bad actors as they attempt to move assets. The system ingests real-time transaction data from 10+ public blockchains, including EVM-compatible and non-EVM chains. It monitors cross-chain bridges, DEX interactions, and token transfers across protocols. Using behavior-based heuristics, ATMS flags suspicious patterns such as:

- **Rapid, multi-hop transfers between mixers and DEXs**
- **Transaction patterns consistent with stolen funds laundering**
- **Sudden asset flows from high-risk or sanctioned sources**

  When anomalies are detected, ATMS automatically generates alerts that trigger:

  - Automated response workflows
  - Manual compliance and security reviews for deeper investigation

This approach enables **early detection and disruption** of illicit fund movements before they can be obfuscated or integrated into legitimate markets.

2. On-Chain Labeling & Entity Mapping

OKX Web3 maintains a proprietary labeling engine that clusters wallet addresses based on behavioral heuristics and on-chain indicators. These clusters are designed to identify relationships between addresses even when controlled by pseudonymous actors and enable proactive risk detection.

Key clustering methods include:

Common Spending: Detecting addresses that participate together in the same transaction, indicating potential shared ownership or coordination.

Key Reuse: Identifying addresses that sign transactions with the same private key.

Transaction Graph Analysis: Tracking repeated interactions, temporal transaction proximity, and circular flows of funds between addresses.

Funding Origin Tracing: Linking addresses based on shared funding sources (e.g., mixers, CEX withdrawal wallets, phishing proceeds).

Once clustered, these address groups are enriched with multiple layers of metadata.

Risk Labels: Categorized into high-risk classes, such as:

- Sanctioned entities
- Mixers
- Phishing operators

Source Data: Intelligence is derived from:

- **Internal blacklists & incident response databases**
- **OSINT (Open Source Intelligence)**
- **External vendor partnerships & blockchain analytics platforms**

These enriched labels directly power our Address Screening & Blocking, and are also used in forensic investigation support. By combining behavioral clustering with external intelligence and proprietary labeling, our system can surface emergent threats and link them to known patterns of abuse, often before they are publicly disclosed.

3 Address Screening & Blocking

To proactively prevent illicit activities, OKX implements real-time wallet address screening across all Web3 interfaces. The program integrates sanctions compliance, entity-level risk scoring, and exploit fund interception.

1. Sanctions Compliance

Wallets interacting with OKX Web3 are checked against:

- OFAC Specially Designated Nationals (SDN) List
- EU, UN, and FATF-aligned sanctions databases
- Custom internal blacklists

2. Entity-Focused Risk Scoring

Clusters associated with illicit activities such as ransomware, terrorist financing, scam rings, or darknet markets are assigned elevated risk scores. These scores drive:

- Risk-based feature restrictions
- Escalation triggers for compliance reviews

3. Security Exploit & Stolen Funds Blocking

Wallets identified as holding or receiving proceeds from security exploits such as DeFi protocol hacks, private key leaks, or unauthorized smart contract interactions are immediately flagged through real-time intelligence feeds and internal alerts.

Key mechanisms include:

- Continuous monitoring of public disclosures (OSINT, social media, etc) and on-chain anomalies
- Integration of threat reports from security partners and whitehat networks
- Tagging of exploiter-controlled wallets based on initial hack transaction traces and laundering patterns

4. Elliptic Integration

OKX Web3 integrates with Elliptic, a leading blockchain analytics provider, to enhance on-chain address screening and threat detection. Through Elliptic's API, OKX ingests real-time risk intelligence across a broad set of categories, including:

- Sanctions exposure (e.g., OFAC, EU, UN lists)
- Terrorist financing links
- Stolen or hacked funds
- Exposure to darknet marketplaces and ransomware actors
- Child exploitation and human trafficking financing
- Fraud, Ponzi schemes, and phishing clusters

Elliptic's platform provides both ownership risk (direct control by sanctioned or criminal entities) and counterparty risk (transactional exposure to illicit actors). The API returns a risk score and associated typology that informs OKX's policy engine. Depending on severity and context, outcomes can include:

- Wallet connection denial
- Feature access restrictions
- Enhanced due diligence or manual review

Elliptic's global data coverage, sourced from millions of blockchain and off-chain signals, helps OKX Web3 maintain industry-leading standards in risk prevention and regulatory alignment.

5. Etherscan, SlowMist, and Chainlabs Label Contributions

In addition to deep integration with commercial analytics engines, OKX Web3 leverages on-chain intelligence from Etherscan, SlowMist, and Chainlabs to amplify the breadth and accuracy of its screening system.
These partners contributed foundational seed labels critical for bootstrapping OKX's proprietary address clustering and entity attribution engine. Contributions include:

- Known scam and phishing addresses
- Associations with DeFi exploits, hacks, and rug pulls
- Ties to malware infrastructure and attack campaigns
- Cross-referenced tags linking wallet behavior to known threat actors

OKX ingests and normalizes such intelligence to improve clustering fidelity and expand detection coverage. In practice, these tags are used to:

- Enrich behavioral labeling models

- Identify previously unknown addresses linked to high-risk entities
- Flag suspicious interaction patterns in wallet or API traffic

For example, Etherscan's Pro API provides fast, structured labeling at scale. This enhances OKX's ability to screen wallet connections at runtime, before any transaction is initiated. Combined with labels from SlowMist's threat intel and Chainlabs' attacker attribution work, these data layers ensure high-confidence detection with minimal false positives.

6. Automated Policy Enforcement

High-risk addresses are subject to automated, protocol-level restrictions that prevent them from:

- **Initiating transactions** via the OKX Web3 Wallet
- **Accessing specific DApp features,** such as the OKX Web3 DEX service

These enforcement rules are **natively embedded** within wallet interfaces, API endpoints, and smart contract logic, ensuring that risk-based flags are applied **consistently and in real time** across all user touchpoints.

4 Smart contract and application security

At OKX Web3, smart contract and application security is enforced through a structured framework that emphasizes code-level risk assessment and targeted enforcement actions. Our goal is to safeguard users from malicious or unsafe interactions without compromising the openness of the decentralized ecosystem.

We apply risk-based controls solely based on known technical indicators such as vulnerability patterns, malicious behaviors, or exploit-linked signatures as well as verified legal and regulatory requests (e.g., law enforcement takedown orders or seizure notices). This ensures a measured, transparent, and minimally invasive approach to risk management.

We do not make subjective judgments about protocols or developers, nor do we restrict access based on speculation. Instead, contract-level enforcement is activated only when grounded in clear evidence from multiple sources, including prior exploit history, behavioral similarity to known attack vectors, or external legal authority. Every enforcement decision is reviewed for potential user impact, and wherever possible, flagged actions are accompanied by transparent user warnings instead of hard blocks.

1. Signature Risk Awareness ("KYS")

KYS (Know Your Signature) helps users analyze the risks associated with their signature and provides real-time warnings to enhance their understanding of transactions they are about to sign.

We proactively alert users and internally flag transactions in the following high-risk scenarios:

- Transactions that modify account permissions
- Transactions that may lead to financial loss
- Token approvals granted to suspicious addresses
- Transactions with clear detrimental outcomes
- Transactions involving sanctioned entities

To date, KYS has flagged **over 80 million** high-risk transactions, safeguarding users from potential threats.

2. Token Risk Tagging

Tokens flagged as:

- Rugs/scams
- Honeypots
- Socially engineered traps

Are clearly labeled and auto-hidden in user interfaces unless manually revealed.

3. Seed Phrase Protection

To safeguard recovery phrases:

- Users must complete a security education module before backing up
- Copy/paste functions are split (partial text revealed with manual input) to prevent clipboard hijacks
- Seed phrase phishing simulations are used during onboarding

4. Approval Management

Users are regularly prompted to review wallet token approvals. A risk engine flags:

- Approvals to known scam contracts
- Unused or long-standing approvals
- Infinite approval permissions

One-click revocation is integrated into the wallet interface.

5. Project integration due diligence

New DApps or protocols integrated with OKX DEX undergo a structured vetting process to mitigate security and financial risks to users. This screening includes:

- Smart Contract Audit Status:

  Verification of recent third-party audits, review of audit scope and findings, and follow-up on remediations. Preference is given to projects with audits from reputable firms and transparent disclosures.

- Project Liquidity and Market Risk:

Evaluation of token liquidity on decentralized and centralized markets, including concentration of token holdings, potential for price manipulation, and susceptibility to rug pulls. Projects with low or opaque liquidity are flagged.

- **Code Similarity to Known Malicious Actors:**
  Static and behavioral code analysis is used to detect overlap with previously identified scam or exploit contracts. Heuristics cover opcode patterns, proxy logic, and fallback behaviors.

Projects that present unresolved risks are either blocked from listing or sandboxed in isolated environments where user exposure is minimized, pending further review. Only projects that pass due diligence are made accessible through the OKX Web3 platform.

6. Domain abuse and brand protection

While brand protection may not traditionally fall under the umbrella of technical application security, it is a critical component of defending users against scams and impersonation attacks in the DeFi space. As the OKX Web3 ecosystem expands, so too does the threat surface from malicious actors seeking to exploit our brand to deceive users and steal funds.
Fraudsters commonly employ tactics such as:

- Impersonation websites mimicking OKX Web3's wallet, DEX, or other services
- Fake social media accounts posing as official OKX support or team members
- Phishing schemes conducted through deceptive domains or advertisements
- "Social engineering" scams that trick users into signing malicious transactions or sending funds to fraudulent addresses

To address such threats, OKX Web3 has partnered with two specialized brand protection vendors:

- **Doppel**
  Doppel continuously monitors the internet for fraudulent use of the OKX Web3 brand, including fake domains, phishing pages, scam ads, and lookalike URLs. Their detection engine leverages machine learning to identify impersonation attempts and spoofed interfaces. Doppel also facilitates rapid takedown processes by coordinating with registrars and hosting providers.
- **Netcraft**
  Netcraft provides deep visibility into global domain infrastructure abuse, including phishing kits, typo-squatting domains, and cloned wallet interfaces. Their anti-fraud network enables real-time blocking and takedown of high-risk pages before users are exposed. Netcraft's intelligence further enhances our internal phishing detection models.

By integrating these domain abuse protection tools into our overall security posture, OKX Web3 proactively prevents brand misuse and ensures a safer environment for our users.

5 Incident Response & Enforcement

1. Real-Time Enforcement

Active defenses include:

- **Blacklist Blocking:** Prevents interaction with flagged wallets
- **Transaction Velocity Limits:** Flags high-frequency or suspiciously large batch activities
- **Geo-Fencing:** Restricts or disables access based on regulatory jurisdiction

When a threat is detected:

- A cross-functional escalation protocol is immediately triggered.
- The Risk Control team conducts an investigation, halts suspicious activity, and coordinates with legal and compliance functions.
- For confirmed API-based exploit attempts, the account is suspended without delay. This includes all KYB (Know Your Business) API clients, where all API activities are suspended and permissions revoked.
- Law enforcement is engaged when appropriate, based on severity and jurisdiction.
- All enforcement actions are recorded in tamper-proof audit logs to support forensic traceability and compliance review.

2. Security Collaborations

OKX Web3 collaborates closely with the broader security ecosystem, including:

- **Whitehat researchers** and **bug bounty platforms**, to identify vulnerabilities and surface real-world attack vectors.
- **BlockSec, SlowMist, CertiK**, and other leading security and forensic vendors, to enhance detection accuracy, shorten response times, and support attribution of advanced threat actors.

These partnerships enable continuous refinement of our defenses and help us stay ahead of the evolving threat landscape in Web3.

6 Roadmap & Continuous Improvement

To maintain leadership in Web3 security, OKX Web3 is committed to ongoing investment in its risk control framework. Key areas of development include:

- **Expanded Labeling Coverage:**
  Broaden our on-chain labeling capabilities by integrating more third-party intelligence providers and sourcing from a wider range of threat data. This will enhance detection accuracy and entity attribution across more chains and protocols.
- **Regulatory/Law Enforcement Cooperation:**
  Build out workflows and channels to support case documentation, escalation, and potential reporting to regulators or law enforcement.
- **Training & Certification:**
  Upskill internal teams through continuous training programs focused on DeFi risk analysis, security

engineering, smart contract auditing, and Web3 compliance. This includes role-specific certifications and simulation-based drills.

- **Threat Intel Alliances:**
  Expand partnerships with industry alliances and intelligence-sharing communities. Collaborating on threat indicators, best practices, and incident response will help strengthen our collective defense posture and foster trust within the Web3 ecosystem.
- **Device Intelligence & Behavioral Monitoring Enhancements:**
  Advance our capabilities in detecting anomalous access and abuse by enhancing device fingerprinting, IP risk scoring, and behavioral pattern analysis. This includes:
  - Cross-device tracking to identify multi-account collusion or bot activity
  - Risk-based authentication using IP reputation, location mismatches, and behavioral biometrics

7 Conclusion

OKX Web3 is committed to making decentralized finance safer, more transparent, and more compliant. Through a multi-layered approach spanning technical audits, behavioral intelligence, jurisdictional enforcement, and user education, we aim to set a new industry benchmark in Web3 security. As the ecosystem matures, we will continue to adapt and expand our defenses, protect user assets, and reinforce the integrity of the decentralized financial stack.