

Codec Networks

Coding Threats. Decoding Solutions.

BLOCKCHAIN, WEB3 & VIRTUAL DIGITAL ASSETS

Secure Every Key. Prove Every Transaction.

Smart contract audits, wallet and node security, blockchain forensics, managed SOC and compliance support for blockchain, Web3 and virtual digital asset businesses

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

PMLA and FIU-IND, CERT-In, Income-tax Act, IT Act and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



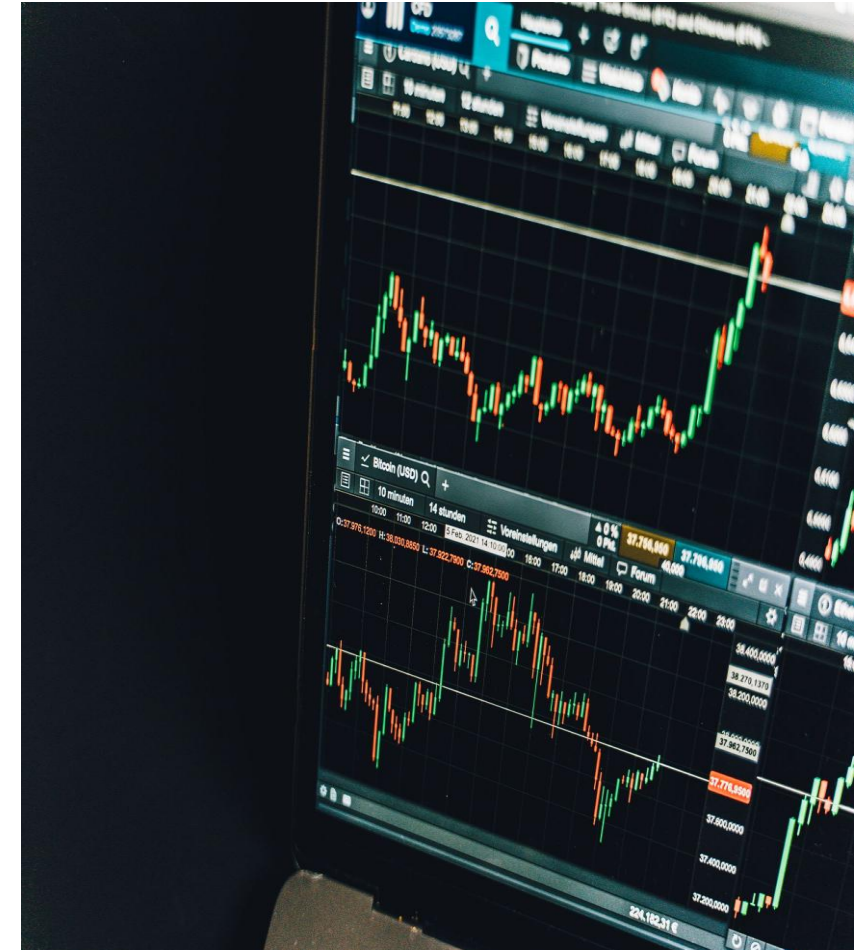
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Digital assets move at internet speed, and so do the thefts

Public figures show the scale of what must be protected

US\$3.4bn+

Stolen in crypto thefts in 2025
(Chainalysis)

US\$2.02bn

Taken by North Korea-linked
hackers in 2025

US\$230m+

Lost in the WazirX hack, July
2024

6 hours

To report cyber incidents to
CERT-In

What this means: Exchanges, brokers, custodians, wallet providers, Web3 and DeFi projects and tokenisation platforms must protect every key and signer, audit every contract and upgrade, monitor every wallet they control, keep KYC and transaction records, pass the CERT-In empanelled audit FIU-IND registration calls for and report incidents within six hours.

Sources: Chainalysis 2026 Crypto Crime Report, WazirX statements (July 2024), CERT-In Directions (2022).

Who we serve across blockchain, Web3 and digital assets



VDA exchanges

Spot, derivatives and INR on-ramps



Brokers and OTC

Institutional and app brokerage



Custodians

Cold storage, MPC, institutional custody



Wallet providers

Custodial and self-custody apps



DeFi protocols

Lending, DEXs, bridges, staking



Web3 projects

dApps, DAOs, developer platforms



Enterprise DLT

Permissioned ledgers, tokenisation



NFT and gaming

Marketplaces, in-game assets

The threats that cost digital asset businesses the most

Six priorities from our 18-threat blockchain, Web3 and VDA assessment



Key and wallet theft

Hot wallets, signers, MPC shares



Signing screen tampering

Multisig interfaces, blind signing



Smart contract exploits

Logic flaws, upgrades, oracles



Bridge and node attacks

Validators, RPCs, relayers



Account takeover

Phished users, stolen API keys



Mules and laundering

Synthetic KYC, mixers, travel rule

Attacks target every step from onboarding to withdrawal

Where Cyber Risk Sits Across the Digital Asset Lifecycle

Every step from onboarding to recovery carries its own attack surface



Digital asset incidents are rarely reversible: once a key signs a malicious transaction, funds move on-chain in minutes and recovery depends on tracing, not reversal.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

PMLA and FIU-IND, CERT-In, Income-tax Act, IT Act and DPDP

The rules shaping VDA and Web3 security

Requirement	Frequency / deadline	Source
Reporting entity status	VDA SPs register with FIU-IND	PMLA notification, 7 Mar 2023
Cyber security audit	Certificate from a CERT-In empanelled auditor	FIU-IND circular, Sep 2025
Customer due diligence	Liveness, geo-tagging, penny-drop checks	FIU-IND Guidelines, Jan 2026
Travel rule	Real-time originator and beneficiary data	FIU-IND Guidelines, Jan 2026
Mixers and unhosted wallets	Monitor, assess risk, do not facilitate mixers	FIU-IND Guidelines, Jan 2026
KYC and transaction records	Kept for five years	CERT-In Directions, 2022
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
Tax and TDS	30% on transfer income; 1% TDS	Finance Act 2022; Income-tax Act
Personal data	Safeguards and breach intimation	DPDP Act 2023; Rules 2025

Key dates on the regulatory timeline

Legal and Regulatory Timeline Shaping VDA and Web3 Security

Tax, anti-money laundering, cyber and data instruments that reach VDA service providers, custodians, Web3 projects and blockchain platforms

● In force ● Upcoming (from Oct 2026)

Mar 2020	● Supreme Court sets aside RBI's 2018 circular restricting banking services to VDA firms
Mar 2022	● Finance Act 2022 defines VDAs in the Income-tax Act and taxes transfer income at 30%
Apr 2022	● CERT-In Directions: 6-hour reporting; VASPs keep KYC and transaction records 5 years
Jul 2022	● 1% TDS on transfers of virtual digital assets takes effect
Nov 2022	● RBI starts the e-rupee wholesale pilot, later followed by a retail pilot
Mar 2023	● PMLA notification makes VDA service providers reporting entities registered with FIU-IND
Sep 2023	● G20 New Delhi Declaration endorses FSB crypto recommendations and the IMF-FSB paper
Dec 2023	● FIU-IND issues notices to nine offshore exchanges and seeks blocking of their URLs
Sep 2024	● MeitY launches the National Blockchain Framework and the Vishvasya blockchain stack
Sep 2025	● FIU-IND ties VDA SP registration to a cyber security audit by a CERT-In empanelled auditor
Nov 2025	● DPDP Rules notified, with most obligations applying from May 2027
Jan 2026	● FIU-IND AML/CFT Guidelines 2026: travel rule, unhosted wallets, liveness, audit trails
Apr 2026	● Income-tax Act 2025 takes effect and carries forward the VDA tax and TDS regime
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: Ministry of Finance, FIU-IND, CBDT, CERT-In, RBI, MeitY, Supreme Court of India, G20, Gazette of India. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Smart contracts · Wallets & keys · Nodes & platforms · Forensics · SOC · Compliance

One partner from smart contract to cold wallet



Smart Contract Audits

Ethereum, Solana, Polygon



Wallet & Key Security

MPC, multisig, HSMs



Node & Platform Testing

Apps, APIs, nodes, cloud



Blockchain Forensics

Tracing, evidence, RCA



SOC & On-Chain Watch

Wallets, contracts, alerts



Compliance Support

CERT-In audit, FIU, DPDP

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Web3 start-ups, DeFi and NFT projects

- Smart contract audit (B11, B2)
- Web and wallet app test (B2)
- Admin key and upgrade review (B3)
- Launch-day monitoring (B7)

Assurance

Exchanges, brokers and wallet apps

- CERT-In audit for FIU (B4)
- Exchange and API VAPT (B1, B2)
- Wallet and custody review (B3)
- 24x7 managed SOC (B7)

Continuous Resilience

Large exchanges, custodians, DLT platforms

- Red team of withdrawal paths (B1)
- MPC, HSM and key review (B3)
- ISO 27001 and SOC 2 (B5)
- Hack response retainer (B8)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Register with FIU-IND as a PMLA reporting entity (2023 notification)	Registration readiness review	B4, B5
Cyber security audit by a CERT-In empanelled auditor (FIU-IND)	CERT-In empanelled audit	B4, B1
KYC with liveness, travel rule, tamper-proof trails (FIU-IND 2026)	AML control and log review	B4, B7
KYC and transaction records kept five years (CERT-In Directions)	Record and log architecture review	B3, B7
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	SOC, IR retainer, reporting support	B7, B8
Unhosted wallet and mixer risk controls (FIU-IND Guidelines 2026)	On-chain screening review	B7, B11
Safeguards and breach intimation for personal data (DPDP Act)	DPDPA programme	B6

Five new case studies, five broken chains

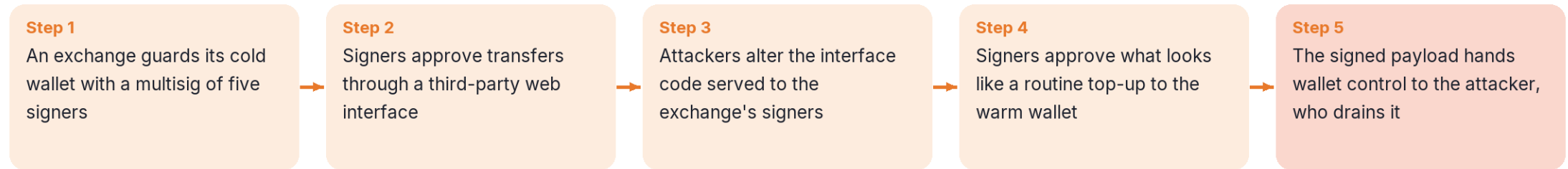
Illustrative composite scenarios written for 2026—not client engagements

1	The Withdrawal Everyone Approved	Tampered signing screens trick multisig signers; independent decoding and signing policies stop it	B3 · B9 · B8
2	The Account Nobody Watched	An unmonitored operational wallet is drained; one custody policy and on-chain watch prevent it	B3 · B7 · B8
3	The Upgrade That Changed One Line	An unaudited upgrade lets funds leave without collateral; audits and timelocks prevent it	B11 · B2 · B7
4	The Mint Page That Was Not Ours	A phished moderator posts a drainer link; MFA, brand monitoring and clear previews stop it	B10 · B2 · B7
5	The Consortium Node That Trusted Everyone	A member's phished node admin issues fake invoice tokens; baselines and HSMs stop it	B9 · B3 · B7

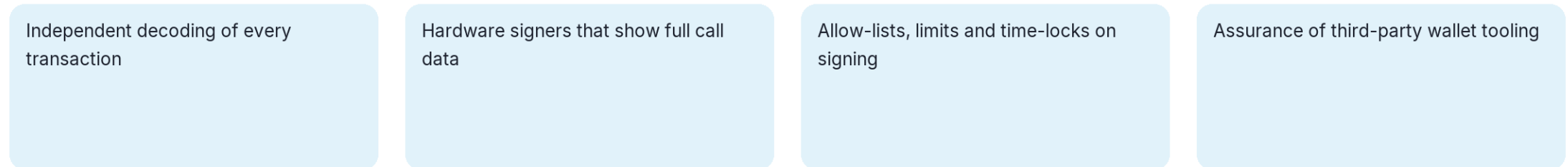
Example: catching a tampered approval

Case 1: The Withdrawal Everyone Approved

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: how each multisig or MPC transaction is proposed, decoded and approved, whether signers see the full call data on their hardware devices, whether allow-lists, limits and time-locks stop unexpected transfers, how the third-party wallet interface is delivered and protected, and how the exchange would freeze, trace and report a theft to CERT-In, FIU-IND, partners and users.

Why digital asset businesses choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018



Regulation-mapped

Mapped to the PMLA and FIU-IND Guidelines, CERT-In Directions and audit guidelines, the Income-tax Act, the IT Act and DPDP



Tests the whole chain

Technical, process and monitoring tests together



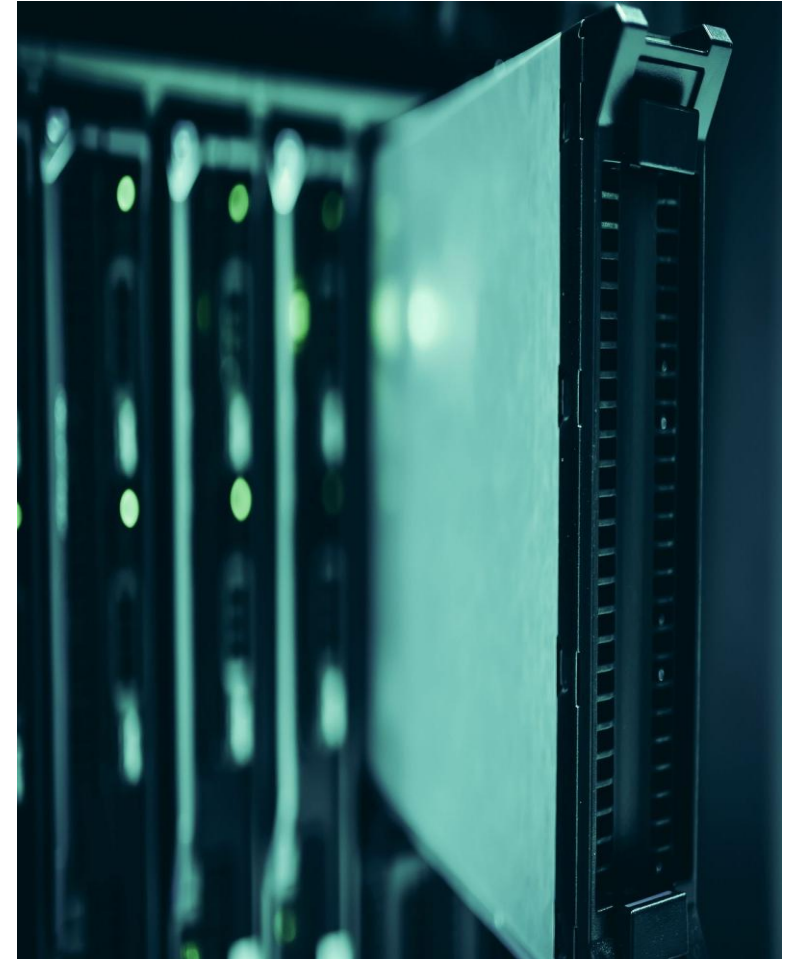
Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Hot, warm and cold wallets, MPC and multisig signing, HSMs, smart contracts and upgrades, nodes, RPCs and bridges, exchange apps and APIs, KYC and travel rule systems, partners and wallet tooling

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

 Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

 011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

 mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.