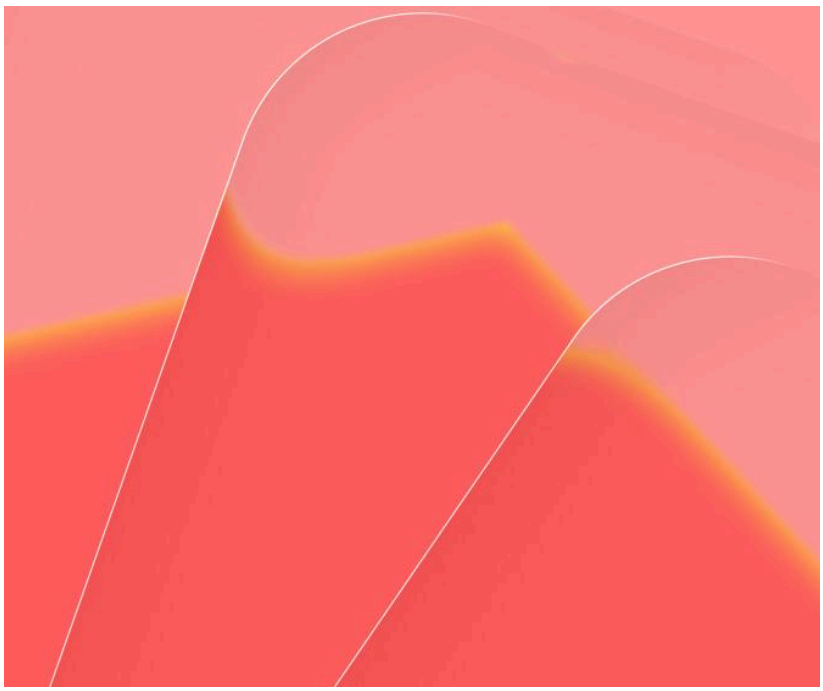
CHAINAR

# The Binance over USD 6 billion “dream hack” is not only the “Binance problem” to handle - the case study

**November 13, 2026**



# Contents


00 Introduction — Page 3

01 The regulatory status and the liability — Page 4

02 The new risk assessment and compliance aspects — Page 7

03 The role of external organisations — Page 16

04 The final conclusions — Page 20

# Introduction

A theft of more than USD 6 billion from Binance is not a security incident for one crypto-asset exchange to investigate and resolve. The crypto-asset ecosystem should bring this case to the point of a broad dialog as it has been a major stress test. Whereas for the institutions, and especially for the new players (banks), blockchain infrastructure providers, LEAs and regulators, increasingly involved in new risk assessments, it brings great lessons for the future decisions on building systems' enhancements.

The stolen crypto-assets left a globally operating exchange. The responsibility for managing the consequences does not remain within the boundaries of one platform. The funds move across thousands of wallets, multiple blockchains, cross-chain bridges, decentralised services, liquidity pools, privacy-enhancing services and newly created tokens. The movement of the funds has so far involved stablecoin issuers capable of freezing assets, blockchain analytics providers tracing illicit flows, some protocols (governance bodies with emergency intervention powers), finally reaching different compliance teams monitoring complex illicit funds exposure and law enforcement authorities, different players who are attempting to coordinate action across jurisdictions.

The Binance case therefore exposes a fundamental reality of cross-border on-chain finance. The security is only as strong as the ecosystem's ability to prevent, detect but also respond to an attack across its interconnected infrastructures.

The incident also raises difficult questions about responsibility and accountability. Who should act when stolen funds enter a decentralised protocol? Who has the technical ability, as well as the legal authority, to freeze and recover crypto-assets? What happens when a particular platform is designed specifically so that its operators cannot control transactions? And how should regulated financial institutions assess the risks of interacting with infrastructure that may be technologically decentralised but still governed through upgrade mechanisms or emergency intervention powers?

The response to the theft has demonstrated that the ecosystem can coordinate at scale. Crypto-asset trading platforms, stablecoin issuers, blockchain analytics tool providers and other participants can trace, freeze and contain significant volumes of illicit assets. Yet successful containment should not be confused with successful prevention. If billions remain outside the reach of recovery mechanisms, the key lesson is clear: the ability to respond after billions have been stolen cannot replace the ability to prevent the theft in the first place.

For banks, crypto-asset service providers, LEAs and regulators, the Binance theft is therefore not merely a story about one exchange being hacked. In this case study we should examine the operational resilience of the entire crypto-asset ecosystem, including having a discussion in context of this case being a warning that “institutional adoption” requires institutional-grade security, governance, accountability and incident-response capabilities across all interconnected participants.

# Part 1. The regulatory status and the liability

## 1.1. The legal accountability and regulatory perimeter. The AML at Binance and why it matters for business and individual customers, crypto-asset trading platforms and counterparties.

We should discuss the necessity of having a complete understanding of who Binance regulators are and what steps they will take now, in context of Binance customers but also the crypto-asset ecosystem, especially entities involved in crypto-asset trading including EU licensed CASPs (their liquidity providers and their customers).

The following statement was issued on October 30th by Binance on their official LinkedIn profile after the hack: "We are completing the purchase of the remaining amount by buying token assets through market channels and OTC channels." On that same LinkedIn profile we may learn: "Technology, Information and Internet. Everywhere." suggesting an interpretation that Binance has a global reach and is offering its services in all markets and to all customers. We may understand the possible risks and that there could be regulatory challenges turning into compliance problems. Eventually this may evolve into a more significant compliance burden not only for Binance (source information part 1, point 1).

The crypto industry players, as well as the regulators including the FSAs which supervise Binance, and LEAs involved in the investigation, should be actually asking the following questions in context of the substantial value of the stolen crypto-assets:
1. Which parties were involved in sell-buy transactions? Which market channels and which OTC channels (in which jurisdictions, and what is the EDD for a third-party risk), also which tokens, does Binance mean exactly by “We are completing the purchase of the remaining amount (…)”?
2. Furthermore, which Binance entities have been involved in purchases and in accordance with which applicable AML law? Has this purchasing process triggered any additional obligations, and if so, has it been coordinated in compliance with for example Travel Rule? Are those Binance entities registered in jurisdictions which have comprehensive and efficient regulatory frameworks for crypto-asset service providers? A reference to “Binance” alone does not identify the legal person.

Binance does not act as a single legal entity with one domicile or one regulator. It acts as a global group and brand operating through multiple legal entities, with different functions, jurisdictions and regulatory permissions. Binance's current global platform structure includes separate ADGM-regulated entities, entities responsible for exchange activities, clearing and custody and broker-dealer services. Where an incident concerns the custody, control, loss or compromise of crypto-assets, the key question is: which specific legal entity was responsible for the relevant activity, system, assets or custody arrangements at the time of the incident? The relevant entity and its regulatory status should therefore be disclosed.

Binance has no EU MiCA CASP licence, no authorisation in the UK.

Based on the recent statements, emails sent by Binance to some EU based customers (France, Italy, Poland, Spain) informing about account closures in particular countries, there is a concern about Binance MiCA strategy and the transition period as well as the EU market access questions. According to the reported communications, users are being asked to withdraw their crypto-assets before a particular deadline, with monthly fees potentially applying from 29 November and accounts reportedly scheduled for closure by 31 December 2026. The grandfathering window for crypto-asset service providers that were already operating under national rules closed on 1 July 2026 at the latest, and member states were free to shorten it (MiCA Article 143(3)). A crypto-asset withdrawal deadline which is running to December 31, 2026 is past that date, and the transition alone does not explain it. The developments appear particularly notable in the context of Binance's previously stated commitment to the European market and subsequent indications of a revised licensing strategy. "Our commitment to Europe remains unchanged, and we are actively progressing our authorization pathway. December 31, 2026: Affected Binance accounts will be closed. November 29, 2026: Monthly fees begin on remaining crypto balances: 0.025% or 10 USDC, whichever is higher. Deposits are blocked, but affected customers can still withdraw their crypto and fiat balances." The winding down of customer accounts, operated through certain European Binance entities, is not followed by an announcement of a permanent exit from the entire European market. It also raises broader questions about how market access is managed in practice, including the role of digital distribution channels such as mobile app stores (Google and Apple) in relation to crypto-asset services offered to EU customers by entities which haven't secured MiCA authorisation (source information part 1, point 2).

Following the information available on the Binance website we may learn that "Binance ADGM entities are regulated by the FSRA of the Abu Dhabi Global Markets (ADGM)" (source information part 1, point 3). "On 5 January 2026, Binance's global platform began operating through three companies supervised by the Financial Services Regulatory Authority ("FSRA") of the Abu Dhabi Global Market ("ADGM"): Nest Exchange Limited, Nest Trading Limited, and Nest Clearing and Custody Limited. Binance said customers would continue using their existing accounts, while services would be provided by the companies responsible for them under the new structure." (source information part 1, point 4).

In November 2023, Binance pleaded guilty to US anti-money laundering, unlicensed money transmission and sanctions violations. US residents cannot use Binance(dot)com, Binance US serves customers in supported states. New York, Texas and 14 other states and territories remain unsupported as of June 3, 2026 list (source information part 1, point 5).

Binance filed for a Brazil crypto license, hours before the Oct 30, 2026 deadline. It matters because of the fact that Brazil is LatAm's largest economy (source information part 1, point 6).

Binance Holdings Limited was incorporated in George Town, Cayman Islands, on September 12, 2017. Its corporate records are not available for public inspection. For context, the Cayman Islands

Monetary Authority previously stated that Binance Holdings Limited and the Binance Group were not authorised by it to operate a cryptocurrency exchange from or within the Cayman Islands, illustrating why incorporation and regulatory supervision should not be treated as interchangeable concepts.

Another entity of Binance is the Binance Capital Management Co., Ltd. ("Binance"), a crypto exchange and custodian (allowing users to buy, sell and store digital assets), holding a Money Service Business Registration in the United States. Binance receives service through Nest Services Limited and their registration indicates an address in Seychelles (source information part 1, point 7).

Binance has been operational in India since mid 2024 after registering as a reporting entity with the Financial Intelligence Unit–India (FIU-IND) under the Prevention of Money Laundering Act (PMLA). The company resumed services and registered as a VDA reporting entity following a resolution that included a $2.25 million penalty for prior non-compliance.

## 1.2. The risk and compliance challenges

In assessing new risk, incoming and outgoing on-chain exposure of Binance, we should take into consideration that a reference to "Binance" alone does not identify the legal person that holds the relevant assets (Binance wallets and clusters), operates the relevant systems, or owns the applicable regulatory and contractual obligations. In context of the USD 6.3 billion hack, it would be important to establish: (i) which legal entity had operational responsibility; (ii) which entity held custody or control of the relevant assets or credentials, also which entity is purchasing the tokens (covering losses); (iii) and which financial supervisory authority had jurisdiction over that entity and activity.

Establishing these points has real consequences. The following examples illustrate some of the key challenges and risks that organisations may need to address:

1. If customers have a legal claim only against the entity that held their assets, and the protections they can count on, like segregation of customer funds or how they are treated in insolvency, depend on where that entity is licensed, and how comprehensive and efficient the regulatory framework for crypto-asset service providers is in that particular jurisdiction. Therefore two customers of Binance could end up in very different positions after another incident like this recent hack (if customers funds are stolen). One might have assets with an entity whose regulator requires customer funds to be kept separate and recoverable. The other customer might be dealing with an entity under no such obligation, and become an unsecured creditor waiting in line. The registration in particular jurisdiction also determines which supervisor can investigate and which rules apply.

2. For business customers transacting with Binance (such as Binance being a liquidity provider), there is a direct impact on their own exposure and risk assessments too. Blockchain analytics tools may label the brand, not the legal person and regulatory compliance, and also the labelling is done under their own calculations and risk assessments. However DD and EDD, risk ratings and other applicable obligations, all depend on knowing which entity you as a business customer are actually

dealing with, what is your organisation's exposure to Binance clusters and wallets, and whether particular Binance entity is authorised and supervised as your business actually needs (under AML and other applicable law). With a group structure as opaque as Binance's, a group which serves more than 335 million users worldwide, extensive average daily trading volumes of approximately $95 billion, that is not always easy to establish.

These are the issues which compliance teams should map out in advance including a new risk assessment, because an incident is the worst time to start asking questions.

Source information part 1, points:

1. https://www.linkedin.com/posts/binance-has-begun-recovering-affected-assets-share-7521887842936070144-4K4I
2. https://www.coindesk.com/business/2026/11/07/binance-users-in-some-european-countries-told-to-pull-crypto-before-fees-kick-in-with-accounts-closing-by-year-end
3. https://www.binance.com/en
4. https://www.legal500.com/intelligence/united-arab-emirates/finance-and-banking/binances-adgm-structure-why-one-virtual-asset-platform-uses-three-regulated-companies
5. https://www.reuters.com/markets/us/us-authorities-set-unveil-settlement-with-binance-source-2023-11-21/
6. https://crypto.news/binance-files-for-brazil-crypto-license-ahead-of-oct-30-deadline/
7. https://www.justice.gov/usao-ma/media/1390101/dl?inline

# Part 2. The new risk assessment and compliance aspects

## 2.1. How to protect your organisations, and yourself as a customer, from exposure to illicit funds, including when a similar incident occurs in the future? What should we expect from blockchain analytics tool providers?

Will you, as an individual customer or a counterparty, be exposed to illicit funds in a scenario where Binance, after the hack, purchased tokens of the remaining amount, such as:
A. tokens which are non-compliant in particular jurisdictions (such as non-MiCA-compliant USDT, sanctioned stablecoins),
B. tokens which may have illicit exposure (to mixers, sanctions, swapping services),
C. tokens which could be purchased via non-compliant/non-regulated/offshore trading platforms (such as no/low KYC, DEXs, OTC brokers)?

In a scenario where a crypto-asset exchange is exposed to buying crypto-assets with illicit exposure or via non-compliant or non-regulated third-parties, then eventually their own clusters' percentage of illicit incoming exposure (of particular clusters and wallets involved) will change to higher percentage. In that scenario it should also reflect a change of that particular exchange risk scoring in the blockchain analytics tools. In some tools, Binance still appears by default as a "low risk" exchange, and that cannot be changed by the user of the tool (risk settings can be managed by alerts).
We could discuss if this is a correct "low risk" setting by default, or an inappropriate risk score calculation by the blockchain analytics tool providers (calculation based on the % of incoming and % of outgoing illicit exposure versus the total amounts in USD)? This topic should be included in the upcoming meetings agenda of the risk-owning teams.

In general the "low risk" of Binance score in the Know-Your-Transaction (KYT) set ups might be reconsidered by entities involved in crypto-asset trading/counterparties, however not only those operating within the EU (under MiCA and AMLR). Furthermore, a new risk assessment for Binance as it comes to incoming/outgoing transfers and business relations should be conducted, and adequate alert settings (including the context of the Binance hack and stolen funds) should follow accordingly.

Additionally, we may learn from the Chainalysis team that "We continue to see funds being laundered quite actively. The attackers are layering these funds across many thousands of addresses, across thousands of deposits" (source information part 2, point 1).

Therefore, the question to ask now is: what measures will compliance teams at CASPs' (as well as at other entities involved in crypto-assets trading) decide on in light of the recent hack and will they, for example, make changes in the risk settings of their KYT/on-chain monitoring systems for the incoming/outgoing transfers with exposure to Binance and be more diligent in checks for origin of the funds in context of stolen funds, or have they already done that?

The illicit funds exposure related to the hack (including "stolen funds", "reported hack" visible in the blockchain analytics tools, as well as layering of the funds) should be a topic for a detailed discussion.

## 2.2. The events following the fraud - money laundering and a third party security incident

### 2.2.1. The money laundering scheme

Some of the key challenges and new risks that organisations should address are the ability of attackers to fragment stolen crypto-assets (across more than 10,000 digital wallets) and use multiple services and privacy-enhancing tools to obscure the flow of funds, making freezing of the stolen funds harder. Looking at the practical challenges, which also the law enforcement faced, significant volumes of illicit assets can continue moving through decentralised services whose developers or operators may argue that they lack the technical or governance mechanisms to block transactions.

Chainalysis stated that more than $46 million in stolen crypto-assets passed through THORChain during the first 72 hours after the attack. The FBI has urged THORChain node operators to block transactions linked to Binance's hack. Those transactions generated more than $200,000 in fees for the service's operators. THORChain faced criticism in 2025 when it was handling funds stolen from Bybit, including claims that participants earned millions in fees while hackers converted stolen assets into Bitcoin. Nearly $4 million in the Binance hack was also routed through Wasabi Wallet. Developers associated with decentralised services have been arguing that their systems are not designed to give operators centralised control over individual transactions (source information part 2, point 2).

A part of the money laundering scheme post Binance hack, used by the North Korean hackers, is to mint meme coins. Rather than transferring stolen funds directly between wallets, laundering networks can create low-value tokens, seed or trade them through DEXs, liquidity pools, and use multiple controlled wallets to obscure the apparent transaction path. The technique does not necessarily make transactions untraceable, blockchain analytics can still reconstruct the flow, but it can significantly increase investigative complexity and delay intervention. The low cost of creating such tokens makes the approach particularly scalable: short-lived tokens, newly established pools and concentrated trading activity among a small number of wallets may become important financial crime risk indicators. "In the $6.4bn Binance case we have seen this technique on Tron and NEAR, along with a closely related approach on Solana. Elliptic first reported its use in the laundering of the funds stolen from Bybit in 2025. The amounts involved are small so far, with about 117,000 NEAR (around $430,000) of stolen funds passing through home-made meme tokens on NEAR, but the technique is cheap to run and could carry far larger sums." (source information part 2, point 3).

For risk and compliance teams, a critical lesson is that funds emerging from a DEX, liquidity pools, should not automatically be treated as "low risk". An effective KYT and transaction monitoring framework should assess the origin of funds before and beyond the immediate counterparty, particularly where transactions involve newly created tokens, recently established liquidity pools, unusually concentrated wallet activity or other indicators of artificial markets or cross-chain activities. This development reinforces the need for risk-based, specific AML controls capable of identifying indirect exposure to stolen assets.

As laundering techniques become cheaper and more automated, effective compliance will increasingly depend on combining on-chain analytics, behavioural indicators, transaction and asset type with a third-party context (monitoring the cash out networks), jurisdiction and timely human investigation where possible enforced by AI (including human-in-the-loop and critical thinking), maintaining clear audit trails for particular DD/EDD decisions. Relying solely on whether a transaction originates from a "seemingly legitimate decentralized protocol" is so called "compliance on paper", definitely not enough these days, and it will not hold up in the event of an inspection by the regulator.

### 2.2.2. The recent Chainalysis security incident

On 30 October 2026, Chainalysis published findings relating to the Binance hack. On the same day, Chainalysis disclosed a security incident involving an external actor that reportedly used “offensive agentic techniques” to gain unauthorised access to certain systems and internal tools, an event where the majority of crypto-asset ecosystem players including trading platforms, investigators and government agencies rely on tools to trace stolen crypto-assets but also comply with AML to evaluate and manage risks. The security incident led the company to temporarily restrict access to certain services while investigating and strengthening its security controls. Chainalysis has published a few statements since the incident, and we may learn that "Customer data, such as user IDs, full names, email addresses, and organization role labels for users provisioned on our platform were accessed, including such information relating to your organization and users. While we investigated, we removed access to Reactor and Data Solutions. At this time we continue to have no evidence that any investigation data has been accessed or Chainalysis attribution data has been manipulated," the company said.

The company stated that, based on the evidence available at the time of its updates, it had found no indication that investigation content, transaction or query results had been accessed, and that there was no evidence of manipulation of its attribution data. However, the incident demonstrates that the sensitivity of compromised information cannot be assessed solely by traditional data classification criteria. A dataset containing investigators’ names, employers, email addresses and organisational roles could create significant operational and security risks by providing bad actors with a highly targeted list of personnel, working in financial institutions, and other on-chain investigations and reporting staff. The main concern is therefore spear phishing and social engineering. Such information may enable bad actors to create highly convincing communications impersonating Chainalysis, colleagues, financial institutions or other trusted counterparties, and to target personnel with access to sensitive investigations, compliance systems or financial infrastructure. A recent case example “Revolut allegedly fed customer information to hackers impersonating an Italian government agency for five months.” (source information part 2, point 4).

Another lesson for entities is the proper risk assessment for a third-party service provider and efficient frameworks at your organisation. The dependence on the data for monitoring on-chain transactions (KYT) via the tool, in context of a service access pause, means a stall in suspicious activity reporting and slow down of your compliance-related checks and transaction decisions. But it also means that your organisation’s employee and investigator metadata can itself constitute valuable operational intelligence. Third-party providers handling information about the personnel should therefore apply enhanced protection to such data, recognising that the exposure of a list of investigators and their organisations may create risks comparable to the exposure of sensitive operational information. The incident also reinforces the need for targeted phishing awareness, strengthened identity and access controls, and rapid third-party incident-response procedures across the crypto-asset ecosystem (source information part 2, point 5).

## 2.3. The effective AI governance - the risk and compliance challenges

The security incident at Chainalysis illustrates a potentially significant shift in cybersecurity risk where AI may increase the speed, scale and sophistication with which bad actors can identify vulnerabilities and execute attacks. Where activities that previously required a coordinated team can be supported by AI, the barrier to conducting sophisticated cyber attacks may fall substantially. In the emerging cybersecurity environment, we could simply say that an attacker without AI support may increasingly resemble a coachman in the age of modern transport: still possible, but progressively disadvantaged by the technology available to everyone else. At the same time, AI is becoming an essential defensive capability. Organisations are using large language models to review and strengthen aspects of its security posture. It is a broader trend in which both attackers and defenders increasingly rely on AI-enabled capabilities. The strategic challenge leads to a broad question: can organisations govern, secure and deploy AI solutions more effectively and faster than the bad actors targeting them?

From an article published by Binance on Nov 3rd, clarifying the attack preparation and the next steps in relation to AI, we may learn that "On 20 October — use of an internal AI tool as a springboard. The attacker leveraged the compromised computer of engineer B and used an internal AI tool to gain control over the Wallet DevOps Engineer A and another Wallet Software Engineer C. The perpetrator soon discovered Wallet DevOps Engineer A had a container deployment permission token on his computer. What we have done: As of Nov 3, 2026, we have taken the following actions: Rebuilt the affected internal AI tool and access controls. Enhanced AI-based behavioural anomaly detection." (source information part 2, point 6).

We could have learned more if Binance had clarified the information about the AI tool (its functionality etc.) and how exactly the internal AI tool was misused by the bad actors. "While many initially speculated that the hackers had used AI to break into Binance, the company's account shows how they instead relied primarily on conventional phishing tactics. At the same time, Binance added that AI did play a role. This occurred when the hackers, after gaining control of the engineer's laptop, used Binance's own internal AI tools to compromise other accounts." (source information part 2, point 7).

When permissions become a risk in case of AI agents? An AI agent does not need to be hacked to cause a security incident, it may misuse the access it has been granted. The key risk lies in the combined capabilities and permissions of interconnected agents. Individually reasonable access rights can create unintended actions and pathways for sensitive data disclosure when agents communicate and act across systems. Organisations should therefore assess not only individual agent permissions but also end-to-end data flows, delegated authority, access boundaries as well as potential unintended actions. To prevent unauthorised disclosure companies need to implement an effective AI governance. In case of AI agents this means defining least-privilege access, controlled inter-agent communication, monitoring of agentic actions including human oversight (with human-in-the-loop (HITL) approval where appropriate) and setting auditable safeguards

(maintaining audit trails). It is of importance to ensure that accountability remains with the organisations and its authorised decision makers.

For the purpose of effective AI governance, the risk and compliance teams should be monitoring if other teams' members, and which teams exactly, call an AI use case a "green risk", "high risk" or a "risk level 4". And what does this actually mean, since if it says nothing about what it could cost in legal and compliance liabilities, further testing and moving on to deployments might not work as everyone assumed.

## 2.4. Cross-border marketing and solicitation risk. The direct and indirect marketing activities of Binance across different partnerships and jurisdictions - the scale and challenges to the regulatory supervision.

It is also worth noting that Binance conducts marketing activities across multiple jurisdictions. Given the cross-border nature of these activities and the participation of international attendees at promotional events, particular attention should be paid to compliance with applicable regulations, especially where such activities may facilitate access to potential new customers or counterparties.

### 2.4.1. The partnerships during CV Summit 2026

Binance entered into a partnership with an international organisation Women in Web3 and performed offline and online marketing activities (addressing international audience) during an event in Switzerland.

Following the announcement published in October 2026 on LinkedIn, by one of Binance partners, we could learn: "The CV Summit 2026 Institutional Breakfast, co-hosted by Binance and Women in Web3 Switzerland brought together a room of investors, founders and builders to discuss where digital assets and traditional finance are heading. Women in Web3 Switzerland (...) a community of 780 members across 30 nationalities and 15 global chapters, built around the conviction that the people building the infrastructure of the next financial system should not all look the same. CV Labs, running accelerators across Switzerland, the UAE, South Africa and beyond, backing 150+ startups with a sub-2% acceptance rate and 21x returns, is quietly one of the most serious early-stage operators in the space. Three organizations. One breakfast." (source information part 2, point 8).

The regulatory challenge extends beyond Binance's own direct advertising to the potential international reach created through partnerships with organisations such as Women in Web3, and CV Labs, which operate accelerators across multiple jurisdictions and support individuals and entities. Where partners promote, feature or distribute content relating to Binance through their websites, events or social media channels, this may create questions about whether crypto-asset services are actually being marketed indirectly on a cross-border basis.

From an EU regulatory perspective, the key issue is whether such partnership activity could amount to solicitation or marketing of crypto-asset services towards potential EU customers in circumstances where the relevant entity is not authorised (no CASP license) to provide those services under MiCA. The assessment should therefore consider the substance and targeting of the communications (offline and online), the intended and actual audience, the role of the partners, and whether the arrangements could circumvent restrictions on actively (directly or indirectly) soliciting clients in/from jurisdictions where authorisation is required.

### 2.4.2. The partnerships during India Blockchain Week (IBW) Conference 2026

Binance entered into a partnership with an organizer of a conference (who also partnered with A7 International) and performed on-site and online marketing activities (addressing international audiences) during an event in Mumbai.

Another event worth examining is the India Blockchain Week (IBW) Conference, held in Mumbai, India, on 1–2 November 2026. The organisers promoted the event as its fourth edition, featuring two new forums, 130 speakers and 20 sponsors. We also know that one of the sponsors is A7 International, addressed by the organizers as: “A7 International joins IBW2026 as a Gold Sponsor. A7 International provides global cross-border payment infrastructure that enables direct USDT-to-SWIFT payments to partners and suppliers abroad. With A7 International, businesses and individuals can pay international invoices in USDT, while recipients get funds via a standard bank transfer without needing a crypto wallet. Launched in October 2026, A7’s new international payment service supports major currencies, including US dollars, euros, UAE dirhams and Chinese yuan.” (source information part 2, points 9 and 10).

At the event in Mumbai the Binance team members were present on the stage, whereas the A7 International was also promoted.

The A7 network (including the A7A5, a ruble-backed stablecoin) is already sanctioned, and these are actual government sanctions. A7 International is assumed to be directly connected to the A7 network. India Blockchain Week’s sponsor page provided a link to A7.biz and A7’s 12 October 2026 announcement describing A7 International as a USDT-to-SWIFT payment service launched within the Russian A7 network created with Promsvyazbank (source information part 2, point 11). A7 International is marketing its own services as: "USDT to SWIFT in one transfer. Global cross-border payment infrastructure.", their services are addressed to businesses that are currently unable to make cross-border payments. You may provide your overseas supplier's invoice, then send them the corresponding amount of USDT (add a 0.3% fee), and the required currency will be sent to the supplier via a regular SWIFT bank transfer (source information part 2, point 12).

The stablecoin A7A5 functions primarily as a bridge between rubles and Tether’s USDT, with significant conversion activity taking place through the issuer’s own exchange and additional transactions occurring through decentralised exchanges such as Uniswap. Following reported U.S.

and UK sanctions, the migration of the exchange's hosting infrastructure from Europe to Yandex-hosted Russian infrastructure may illustrate an unintended consequence of sanctions: rather than eliminating activity, restrictions can contribute to the relocation of liquidity and operational infrastructure into jurisdictions that are more difficult for Western institutions to monitor and influence.

The A7 off-chain networks - according to the TRM Labs and the Financial Times article we may learn that "A7 used a web of front companies across the UAE, Hong Kong and Kyrgyzstan to reach the SWIFT system, and hid them behind an industrial forgery operation." Using thousands of corporate stamps and falsified invoices in which customs codes for sanctioned goods were replaced with codes corresponding to non-restricted goods. Payments were split into multiple smaller transactions to keep it under reporting thresholds, and just over half of the funds ended up in Chinese accounts (source information part 2, point 13).

The timeline raises significant compliance and reputational questions: the U.S. Treasury reportedly sanctioned the A7 Network on 1 October 2026 as a transnational criminal organisation, followed shortly thereafter by the launch of A7 International's global payment service on 13 October 2026 ~and its subsequent appearance as a Gold Sponsor at India Blockchain Week.

India hasn't taken steps to regulate usage of stablecoins and stablecoins operate outside a legal framework and without any meaningful customer protection (source information part 2, point 14).

India does not have a formal crypto-exchange licensing framework from the Reserve Bank of India (RBI) or SEBI. However Binance was performing its services before in non-compliance with the law. Following a temporary ban and a $2.25 million penalty in early 2024 for non-compliance with the Prevention of Money Laundering Act (PMLA). Interestingly the FIU in India addressed its "Order in original No. 10/DIR/FIU-IND/2024 in the matter of Binance u/s Section 13, dated 19.06.2024" to the entities of Binance registered in Cayman Islands, Seychelles, and Switzerland (source information part 2, point 15).

Following the announcement issued by Press Information Bureau, Government of India, Ministry of Finance (dated Dec 23, 2023), we may learn: "As part of compliance action against the offshore entities, Financial Intelligence Unit India (FIU IND) has issued compliance Show Cause Notices to following nine offshore Virtual Digital Assets Service Providers (VDA SPs) under Section 13 of the Prevention of Money Laundering Act, 2002 (PMLA). Director FIU IND has written to the Secretary, Ministry of Electronics and Information Technology to block the URLs of said entities that are operating illegally without complying with the provisions of the PML Act in India." (source information part 2, point 16).

Binance is currently operational in India as a registered Virtual Digital Asset Service Provider (VDA SP) with the Financial Intelligence Unit-India (FIU-IND). Binance registered as a reporting entity with the Financial Intelligence Unit-India. Binance's website and mobile apps were restored across India after fulfilling anti-money laundering (AML) and reporting requirements.

## 2.5. The regulatory and compliance challenges

In light of possible distant onboarding of new individual and business customers based in jurisdictions where Binance is not authorised to operate, which steps should the National Competent Authorities take now?

For financial institutions, the crypto-asset ecosystem and event partners, this underlines the importance of enhanced due diligence beyond brand names and marketing activity, including careful assessment of ownership, control, corporate links, sanctions exposure (including on-chain activities) and the relationship between affiliated entities operating across jurisdictions.

Furthermore, the case underlines the importance of monitoring not only sanctioned assets and entities, but also changes in infrastructure, hosting, liquidity routes and decentralised exchanges activity that may alter sanctions evasion and financial crime risk.

Source information part 2, points:


1. https://www.bbc.com/news/articles/cwj34gdmnly4o
2. https://www.wsj.com/finance/currencies/the-shadowy-crypto-services-helping-the-binance-hackers-launder-stolen-billions-28641737
3. https://www.elliptic.co/insights/north-korea-meme-coins-binance-hack/
4. https://www.securityweek.com/revolut-data-breach-5-months-680-high-profile-accounts-3m-ransom/
5. https://www.chainalysis.com/blog/security-incident-october-30/
6. https://www.linkedin.com/pulse/29-october-binance-security-incident-initial-findings-response-modgf/
7. https://fortune.com/2026/11/03/binance-hack-details-linkedin/
8. https://www.linkedin.com/company/wiw3ch/posts/
9. https://www.linkedin.com/posts/ibwofficial_karthik-selvaraj-head-of-operations-events-activity-7523396157931200513-OoVL?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAsVNwIB1y1EmiI3f5URjZ5g4KtKNLFkFFo
10. https://www.linkedin.com/posts/ibwofficial_a7-international-joins-ibw2026-as-a-gold-activity-7521800144477032448-jF28
11. https://www.ft.com/content/372d018c-df75-4bf8-9699-7f87b8511c37
12. https://www.linkedin.com/feed/update/urn:li:activity:7515772750746193920/
13. https://www.linkedin.com/feed/update/urn:li:activity:7508079529198886912
14. https://www.grantthornton.in/insights/articles/stablecoin-use-rising-india-no-regulation/
15. https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf
16. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1991372&lang=2&reg=48

# Part 3. The role of external organisations

## 3.1. The Ethereum upgrade EIP-7702

What role do external organisations, such as the Ethereum Foundation, play in situations like the hack of Binance, as well as in fostering a secure environment - supporting the expansion of crypto-assets and the building of trust?

Based on the information shared by a team member of the blockchain analytics tool provider Chainalysis, regarding the upgrade EIP-7702, we know it was misused by the bad actors in the Binance hack. The upgrade is an essential point for the case investigators: "A recent Ethereum upgrade (EIP-7702) lets a normal wallet hand control of its behaviour to a piece of software. Think of it as giving someone a power of attorney over a bank account. The attacker got Binance's wallet to sign one of these "power of attorney" authorisations. The authorisation pointed to known wallet-draining software. After that, the attacker didn't need Binance's keys again. They pressed a single "sweep everything" button, and the software moved the wallet's whole balance out in one go. That same draining kit had already been flagged before this attack, and it is linked to an operator whose funds came through Tornado Cash, a crypto mixing service used to hide where money comes from." (source information part 3, point 1).

The upgrade was also clarified by Binance itself on November 3rd 2026: "The attacker then used the signing service to exploit Ethereum's EIP-7702 authorization mechanism. EIP-7702 allows an account to delegate certain execution rights to a smart contract without exposing the private key. In this case, the attacker used that mechanism to give an attacker-controlled smart contract partial execution rights over a Binance hot wallet." (source information part 3, point 2).

We should be able to understand who exactly (a group of people) and for what purpose/use case approved the Ethereum upgrade EIP-7702. What was the risk assessment before the decision of that particular upgrade was made and was that documented? Is there an effective risk management plan that the Ethereum core developers follow?

We know there have been signals coming from the independent firms and crypto ecosystem community about risks, such as mentioned in the article by Audita dated March 21, 2025, titled "Risks of Implementing EIP-7702 from Ethereum's Pectra Upgrade", where the authors mentioned that it is a "security ticking time bomb, can be exploited to drain whole wallets" (source information part 3, point 3).

In April 2025 Vitalik Buterin, the Ethereum Co-founder, warned and responded to security concerns over the new Pectra upgrade. He responded to the Ethereum community's concerns regarding the protocol's latest upgrade EIP-7702. The debate highlighted a fundamental risk of introducing greater flexibility and functionality into blockchain infrastructure: technical innovation can also create

new pathways for fraud, phishing and the unauthorised loss of digital assets. Concerns focused on the possibility that wallet users could delegate authority to external smart contracts. Critics argued that, while wallets may block known suspicious websites, users could still be exposed to potentially fraudulent delegation requests that appear legitimate. A single approval or signature could, depending on the permissions granted and the implementation of the relevant smart contract, create significant exposure for a user's crypto-assets.

Another comment on the upgrade: “Cryptography and Security (submitted on 13 Dec 2025), EIP-7702 Phishing Attack. We also present the first empirical measurement of EIP-7702 usage across major EVM chains. Analyzing over 150k authorization and execution events involving 26k addresses and hundreds of delegator contracts, we assess the protocol's real-world footprint. Our findings show that EIP-7702 authorizations are highly centralized, dominated by a small number of contract families linked to criminal activity and repeatedly reused across incidents. Corresponding loss data reveals substantial theft of ETH, ERC-20 tokens, and NFTs. These results provide practical evidence that the attack surface we identify is not merely theoretical, but is already being exploited at scale. We conclude by proposing protocol-level defenses to mitigate the delegation-based phishing vector introduced by EIP-7702.” (source information part 3, point 4)

According to additional feedback on the upgrade: "One user shared a statement from X user @nftchance, who pointed out the “non-viability” of EIP-7702. The user pointed out that the wallet blocks websites that are not suspicious. However, it still allows delegations for potentially fraudulent contracts to pass through, which could leave users vulnerable to potential security breaches like phishing and other cyber hacks. “Meanwhile they’re going to allow arbitrary delegation that can result in complete portfolio loss in one signature.” stated the user on X." (source information part 3, point 5).

## 3.2. The Ethereum Foundation - reorganisation, and the Ethereum based solutions

Several important questions concerning the Foundation itself warrant further examination, particularly regarding its recent activities and developments.

The Ethereum Foundation is registered as Stiftung Ethereum, a Swiss Foundation, located in Zug, Switzerland. On 23 June 2026, the Foundation announced a significant organisational restructuring, eliminating 54 positions, that is approximately 20% of its workforce and reducing its 2026 operating budget by 40%. The remaining organisation is being reorganised around five domain-focused clusters, supported by dedicated operations and management functions, according to a post published by Vitalik Buterin on the EF's official blog. Beyond the immediate cost reductions, the restructuring raises broader questions about how and by whom the critical blockchain infrastructure is governed, secured, funded and sustained over the long term.

Vitalik Buterin in a recent interview (at Devcon in Mumbai, India, Nov 2026) commented on the status of the work as well as the Ethereum's future: “The AI informal verifications are really huge. The amount of work that is done in the rest of the roadmap, thanks to AI we are able to do it so much faster. Thanks to the AI-enabled formal verification we can ensure that all of the code that’s being written, all of these algorithms that are being developed, are actually safe. As an L2 you should be innovating, and doing something different, like Ethereum by itself does not do, and there are lots of projects that do right like high performance DeFi and various privacy protocols are the big ones, Aztec and Intmax, and enterprise - if you are an enterprise you can take the existing logic that’s inside your existing server to manage your supply chain records, health records, manufacturing records, anything, stick to the chain like a hash of the data. Everything we build is open source. And all those questions how safe they are against AI and quantum, it’s ultimately up to them. If they want to go crazy they have the power to go crazy.” (source information part 3, points 6, 7, 8 and 9).

As AI becomes embedded in decision-making, operational processes and automated activities, AI failures can create risks extending far beyond traditional IT incidents. Incorrect AI outputs may lead to flawed management decisions (especially if AI governance is not effective), financial losses from autonomous or agentic transactions, business disruption, regulatory consequences and significant reputational damage, including through the automated generation or dissemination of misinformation. A key challenge is that AI systems can behave dynamically and, in some cases, operate with a degree of autonomy that makes all risks difficult to identify in advance. Organisations should therefore plan not only for prevention, but also on the assumption that AI incidents can occur despite preventive controls. This requires strong detective and response capabilities designed to identify incidents quickly, assess their impact, contain abnormal behaviour and minimise resulting harm.

In connection with the Binance hack, and the blockchain based solutions, such as Ethereum based, there are additional governance and risk-related concerns. We may currently witness the countermeasures which have been taken by the security councils, committees, such as the one at Arbitrum. “Arbitrum’s council moved $30 million of Binance hack funds without the hacker’s key. A 12-person committee briefly rewrote one of Arbitrum’s core contracts to spend from an address it held no key for, then put the code back. It’s the second time this year.”. Arbitrum is Ethereum’s Layer 2 scaling solution, designed to make transactions faster and cheaper while relying on Ethereum for security. Arbitrum’s 12-member Security Council reportedly moved more than 8,425 ETH and 74 million ARB (worth approximately USD 30 million) from an address linked to the Binance exploit, without the hacker’s private key or involvement, that was on Friday October 30th. Whereas the FBI attributed the Binance hack to the TraderTraitor group a day later, on October 31st. The transfer was enabled through Arbitrum’s emergency governance powers. With approval from at least nine council members, the council temporarily modified the code of Arbitrum’s Inbox contract, introducing a function that allowed transactions to be executed as if they originated from the exploiter’s address (the replacement code added a function called *sendUnsignedTransactionOverride*). The original code was subsequently restored. The council stated that it exercised powers granted by the DAO and publicly disclosed the actions. This was not an isolated intervention: in April 2026, the council reportedly used similar powers to recover 30,766 ETH, then worth approximately USD 71 million,

from the KelpDAO exploiter. Although the recovery demonstrates the potential value of emergency intervention mechanisms in protecting assets, it exposes a fundamental tension between security and decentralisation. In particular, it illustrates that control over a protocol's upgrade mechanism may, in exceptional circumstances, override the usual requirement for a wallet's private key to authorise transactions. The authority to modify core contracts therefore carries significant implications for asset control, governance integrity and accountability (source information part 3, points 10, 11 and 12).

## 3.3. The compliance and security challenges

When entities, including the regulated financial sector, depend more and more on the blockchain infrastructure and are accelerating their adoption of the DLT as well as asset tokenization, we need clarity about the blockchain networks' governance, including but not limited to the process for risk assessment of the planned updates/upgrades, the AI role, as well as blockchain audits (blockchain networks' security, functionality and compliance with industry standards).

For financial institutions and businesses building on blockchain infrastructure, organisational changes within key ecosystem participants are worth monitoring. While decentralised networks are designed to operate independently of any single organisation, foundations and core development teams can continue to play an important role in ecosystem development, technical coordination and the evolution of standards.

The blockchain networks also have the governance rules which consist of the protocols as well as voting procedures that dictate how a network operates, upgrades and resolves conflicts without a central authority (on-chain, off-chain, hybrid governance).

The blockchain infrastructure has evolved rapidly. The next challenges are to make it usable at scale but also secure and up to certain standards. The broader lesson for the ecosystem is that blockchain adoption should be assessed not only through the resilience of the technology itself. For the purpose of performing broad risk assessments, there should be clarity and access to disclosures such as about the governance, resources and long-term sustainability of the organisations and ecosystems supporting it.

Source information part 3, points:

1. https://www.linkedin.com/feed/update/urn:li:activity:7521724018601803777/
2. https://www.linkedin.com/pulse/29-october-binance-security-incident-initial-findings-response-modgf/
3. https://audita.io/blog-articles/risks-of-implementing-eip-7702-from-ethereum-s-pectra-upgrade
4. https://arxiv.org/abs/2512.12174

5. https://crypto.news/vitalik-buterin-responds-to-security-concerns-over-new-pectra-upgrade/
6. https://blog.ethereum.org/2026/06/23/ef-structure
7. https://www.coindesk.com/tech/2026/05/18/the-ethereum-foundation-is-facing-a-wave-of-high-profile-departures-as-its-internal-shakeup-deepens
8. https://ethereum.foundation/ef
9. https://youtu.be/Tx7RwC_ZZX4?si=VaqdHwmwRuCOxLut
10. https://bitcoinsuisse.com/eu/news/what-is-arbitrum
11. https://docs.hyra.network/docs/development_documentation/intro/
12. https://www.coindesk.com/tech/2026/11/03/arbitrum-s-council-moved-usd30-million-of-binance-hack-funds-without-the-hacker-s-key

## The final conclusions

In the age of bad actors targeting internal AI systems and using AI to enforce their fraud tactics, the Binance hack represents a major stress test for the entire DLT and crypto-assets ecosystem, testing not only the security systems but also the ability of stablecoin issuers, DeFi protocols, regulators, LEAs, compliance teams and blockchain analytics tool providers to coordinate and respond at scale.

For entities adopting AI solutions, calling your AI use cases a “low risk”, "high risk" or a “risk level 3” says nothing about what it could cost an organisation in legal and compliance liabilities.

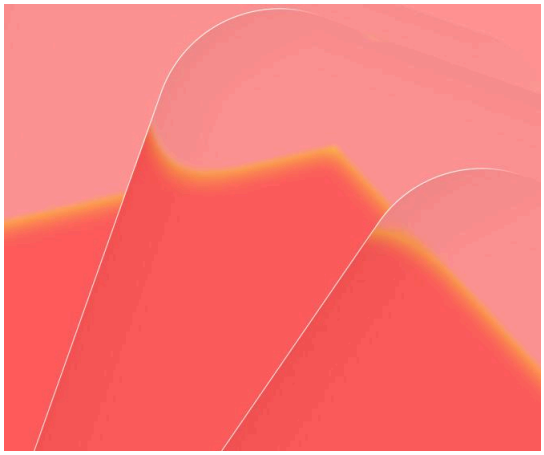
With approximately less than 50% of stolen funds, which is USD 2.84 billion, subsequently frozen, the incident demonstrates both the growing capacity of the ecosystem to contain illicit activity and the significant limitations of relying on intervention after an attack has already occurred.

The response of the crypto-asset industry players highlights three critical lessons for the future of digital finance:

1. The stablecoin issuers are increasingly becoming part of critical financial infrastructure, as their ability to freeze or restrict illicit funds can play a material role in the financial system's defence mechanisms. Such powers require clear governance, accountability and appropriate processes and procedures.
2. Cybersecurity must evolve towards bank-grade financial resilience. The protection of private keys alone is no longer sufficient. Institutions need robust access controls, effective risk and governance frameworks including the AI governance, cybersecurity and data protection, transaction authorisation frameworks, segregation of duties, continuous monitoring and the ability to detect and stop malicious activity before losses reach systemic levels.

3. The next generation of financial infrastructure will increasingly be judged by its ability to respond effectively when things go wrong. In connection with the mature standards/mature support, real-time blockchain transparency and analytics (including but not limited to diligent and constant labelling), evidence-based trust and security, coordinated incident response, intervention capabilities and institutional-grade controls are becoming essential components of operational resilience.

However, successful containment does not erase unsuccessful prevention. The fact that billions of dollars reportedly remain unfrozen (over 50% of stolen funds) demonstrates the limits of post-incident recovery. The central lesson for institutional adoption is therefore clear: the crypto-asset industry is increasingly capable of responding at scale, but institutional-grade infrastructure must ultimately be designed to prevent attacks at scale, not merely manage their consequences.



***Contact our team to discuss your matters and our solutions related to regulatory compliance in the area of crypto-assets, blockchain and AI (www.chainar.se).***

***Disclosures:*** *The case study article was written by Team Chainar, with partial AI tool assistance (including human verification). The material is provided for general informational purposes only and does not constitute legal, tax, financial, investment or other professional advice. It should not be relied upon as a substitute for obtaining advice tailored to specific circumstances. To the extent permitted by applicable law, Chainar AB accepts no liability for any decisions, actions or omissions taken by any person in reliance on, or in connection with, the use of this material. Chainar AB does not guarantee that the information contained herein is complete, accurate, up to date or suitable for any particular purpose. This material may contain links to third-party websites that are not owned or controlled by Chainar AB. The inclusion of, or access to, such links does not imply that Chainar AB is affiliated with the relevant websites or their operators, or that Chainar AB endorses, approves or recommends them or their content. To the extent permitted by applicable law, Chainar AB accepts no responsibility or liability for any products, services, information or other content made available through third-party websites.*