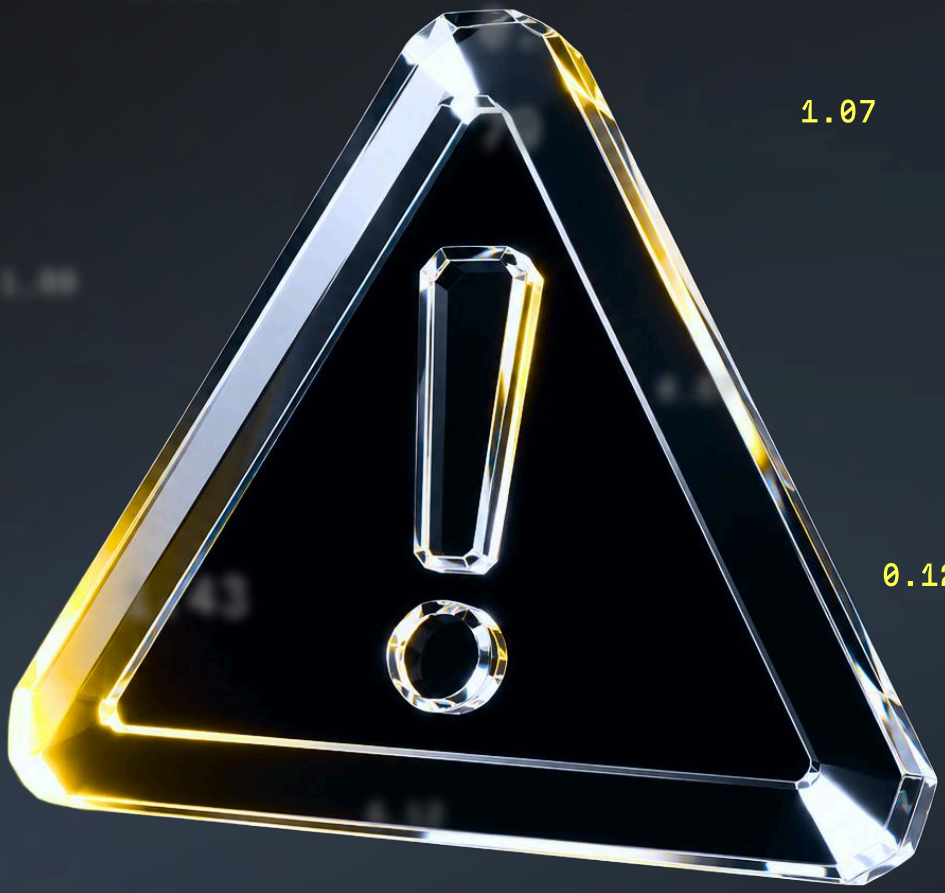
Crystal Intelligence



A CRYSTAL INTELLIGENCE REPORT

Compliance Blindspots

How criminals move value through the gaps between blockchain analytics, payment infrastructure, and physical cash conversion.

SERIES
Crystal Investigations

AUDIENCE
Regulators, compliance, law enforcement

PUBLISHED
Jul 2026

Contents

Executive summary 02

The structural gap 03

Mobile wallet settlement: the hidden layer 07

Crypto-funded payment cards: the off-ramp 11

Red flags and indicators 17

Recommendations 20

Methodology 23

About Crystal Intelligence 24

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Executive summary

Blockchain analytics has a structural blindspot. The industry traces digital assets once they appear on-chain, but the moments of highest compliance risk - where fiat becomes crypto and where crypto converts back to spendable cash - fall outside the systems built to monitor them.

Crystal Intelligence's research across three separate investigations documents the scale of this gap. The unified finding: compliance frameworks treat crypto and fiat as separate domains, and criminals have learned to move value through the gaps between them.

What the research found

HONG KONG CASH-DESK VOLUME	P2P ADS	CRYPTO-CARD ON-CHAIN INFLOWS
$2.5B	57,829	$1.18B

VASP FLOWS	HIGH-RISK CARD INFLOWS TRACED	CRYPTO-CARD YOY GROWTH
$403M	$166M	66%

01

Hundreds of active services globally.

Hong Kong alone processed over **$2.5B** in cash conversions in 2024. **33%** of identified service activity involves unlicensed exchanges; **97%** of funds flow on to major international exchanges as ordinary deposits.

02

The dominant rail where crypto is restricted.

Analysis of **57,829 peer-to-peer crypto advertisements** across ten emerging markets shows mobile wallets dominate settlement where crypto is restricted - **Bangladesh 83%, Egypt 65%**. These transactions are invisible to mobile operators and domestic regulators alike.

03

$1.18B traced - 67.7% with no real KYC.

Crystal identified almost **100 providers** with over $1.18B in traced on-chain flows. **67.7%** offer no or low- friction identity verification. **$166M** in high-risk inflows were traced - exposure to sanctioned entities, dark markets, ransomware and terrorism-financing indicators.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 1:

The structural gap

AML programs at financial institutions, crypto exchanges and payment providers all face the same constraint. They monitor transactions within their own systems but have limited visibility into the infrastructure that converts value between physical cash, mobile payments, and blockchain assets.

CASH-FOR-CRYPTO DESKS

Convert physical currency to digital assets at locations most analytics providers cannot identify.

MOBILE-WALLET RAILS

P2P crypto trades settle via mobile wallets - to operators, they look like any other person-to-person transfer.

CRYPTO-FUNDED CARDS

Loaded crypto exits the digital asset world as ordinary card payments at merchants and ATMs.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Where crypto AML doesn't meet payments

A parallel problem for blockchain analytics

Blockchain analytics providers face a parallel version of this problem. They trace funds on public ledgers with increasing sophistication, but the conversion moments - cash becoming crypto, crypto settling through a mobile wallet, crypto loading onto a payment card - occur either before or after the on-chain record. By the time a transaction reaches a monitoring system, the point of highest compliance risk has already passed.

None of this is hypothetical. Each channel has been documented through Crystal's research using physical intelligence collection, peer-to-peer market monitoring, and blockchain forensic analysis. The two sections that follow present the detailed evidence for the settlement and off-ramp channels. The on-ramp channel - cash-to-crypto services - is where the gap begins.

The on-ramp: cash-to-crypto services

A deposit lands on a major crypto exchange. It arrives from a self-custody wallet, passes automated screening, and is added to the platform's liquidity pool. Nothing about it looks unusual. Two days earlier, the funds were physical banknotes handed across a counter at an unlicensed cash desk in a Hong Kong commercial district.

The exchange's compliance team has no way to know this, and no tool in their current stack can tell them. The industry analyzes transactions after the fact. It does not map the physical infrastructure where fiat becomes crypto - the conversion point that exists before any blockchain transaction is recorded.

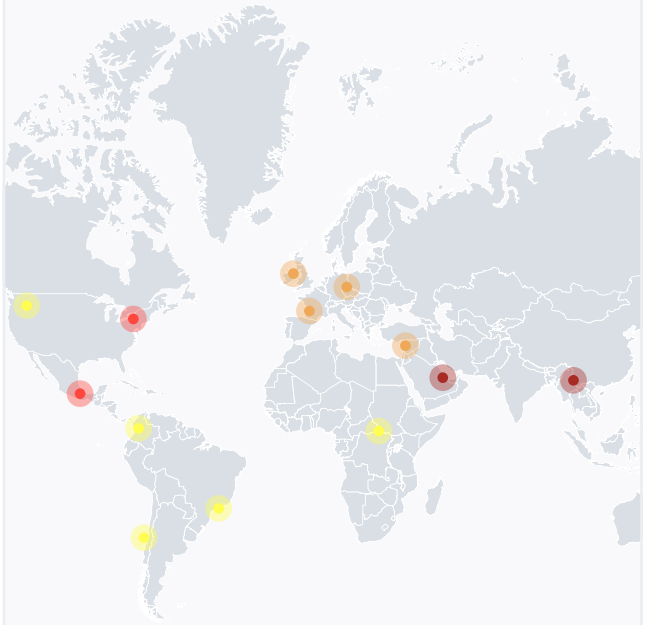
Cash-to-crypto is therefore the clearest illustration of the structural gap: the moment of highest risk happens entirely off-chain, in the physical world, before any monitoring system can see it.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

The hidden infrastructure, mapped

Cash-to-crypto services identified globally

Cash desks identified through Crystal's research



Crystal's research team has identified hundreds of active cash-for-crypto services across multiple continents, operating from commercial districts in cities ranging from Vancouver to Hong Kong. The volumes are substantial. Hong Kong's cash desks alone processed over $2.5B in cash transactions in 2024.

Not all of these are criminal operations. Many serve real needs: faster, cheaper remittances; access to international markets for small businesses; and financial services in countries with currency restrictions.

Russian-speaking communities rely on them extensively - Crystal has documented services in resort areas across Thailand, Sri Lanka and Egypt.

Where the compliance risk emerges is in how these services are structured. Crystal's analysis shows 33% of identified service activity involves unlicensed exchanges. Many impose minimal or no identity checks. And 97% of the funds flowing through these services end up at major international cryptocurrency exchanges, arriving as ordinary deposits with no trace of their cash origins.

Why compliance programs miss this

The problem is structural, not technical. AML monitoring starts after cash has already been converted to crypto. An individual brings cash to an unlicensed service, receives crypto in a self-custody wallet, and deposits it to an exchange days later. The exchange's compliance team sees a routine self-custody deposit. The moment that mattered - the physical cash handover - happened off-chain and off-screen. No amount of blockchain analysis can retroactively reveal that a deposit originated from a cash conversion. The risk materializes before the on-chain record begins.

Read more about Crystal's investigations into cash-for-crypto services *here.*

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Two views of the same problem

For law enforcement

These services present accessible targets. They operate from identifiable physical locations. Many advertise openly on messaging platforms. Crystal's intelligence has documented their locations, operating hours, and advertising channels. The bottleneck is resource allocation.

For compliance teams at exchanges

The implication is more uncomfortable. These funds are arriving on your platform now. Without intelligence linking physical cash-service locations to on-chain deposit patterns, there is no way to flag them.

HONG KONG CASH-DESK VOLUME

$2.5B

A single data point that illustrates why ground-truth physical intelligence is not optional for closing the on-ramp blindspot.

Takeaways

↓

Hundreds of active cash-for-crypto services documented across multiple continents; Hong Kong alone processed $2.5B+ in cash conversions in 2024.

↓

33% of identified service activity involves unlicensed exchanges; 97% of funds flow on to major international exchanges as ordinary deposits.

↓

Blockchain analysis cannot retroactively reveal cash origin. The risk materializes before the on-chain record begins.

↓

Targets are physically identifiable. The constraint on enforcement is resource allocation, not intelligence collection.

→

Crystal's cash-to-crypto mapping is ongoing. Detailed on-chain analysis for this channel will appear in a future edition of the Compliance Blindspots series.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 2:

Mobile-wallet settlement

A buyer confirms a crypto trade on an Egyptian peer-to-peer marketplace. The listing specifies bank transfer, but the seller's message says otherwise: "Send 5,000 EGP via Vodafone Cash to this number." To Vodafone, it looks like any other person-to-person transfer. What happens next - the conversion to USDT, the transfer to an exchange, the onward flow to a sanctions-exposed wallet - is invisible to every regulator in the chain.

P2P LISTINGS ANALYZED	EMERGING MARKETS COVERED	VASPS TRACED ON-CHAIN	TOTAL CRYPTOFLOWS DOCUMENTED
57,829	10	45	$403M

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

A global pattern across ten markets

When regulators ban crypto or lean on banks to block transactions, trading does not stop. Settlement migrates to mobile wallets - faster, more accessible, and subject to far less scrutiny. Crystal documented this across ten emerging markets between November 2025 and January 2026, analyzing 57,829 peer-to-peer crypto advertisements.

Mobile-wallet dependence ranges from 83–85% in Bangladesh and the Ivory Coast to a near-even split in Colombia (48%).Even at the low end, close to half of all peer-to-peer crypto settlement runs through mobile money.

COUNTRY	MFS SHARE	P2P ADS	PROVIDERS
WEST AFRICA			
Ivory Coast	85%	1,301	MTN MoMo, Orange Money, Airtel Money
Ghana	76%	1,863	MTN MoMo, Vodafone Cash, Airtel / Tigo
Nigeria	45%	10,771	OPay, PalmPay, Chipper Cash, PAGA
NORTH AFRICA			
Algeria	67%	815	BaridiMob, CCP
Egypt	65%	3,471	Vodafone Cash Orange Cash, WePay
SOUTH ASIA			
Bangladesh	83%	5,021	bKash, Nagad, Rocket, Upay
India	66%	18,147	UPI, IMPS, Paytm, PhonePe
Pakistan	58%	9,059	Easypaisa, JazzCash, NayaPay
Philippines	51%	5,603	GCash, PayMaya, GoTyme
LATIN AMERICA			
Colombia	48%	1,778	Nequi, Daviplata, Movii

Above: mobile-financial-services share of P2P crypto listings across ten emerging markets, November 2025 – January 2026. Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Why regulators miss the connection

The blindspot exists because mobile wallet-to-crypto transactions fall between authorities; and none of them sees the full picture.

A mobile-wallet operator processes a domestic, KYC-verified, peer-to-peer transfer for 5,000 Egyptian Pounds. It sits within normal limits. It looks like any of the millions of daily transfers for rent, groceries or family support. The operator has no visibility into what happens next - whether the recipient converts those pounds to USDT, or whether that USDT flows to a sanctioned entity.

Meanwhile, Egypt's Central Bank prohibited banks from facilitating crypto in 2018. But the regulator has no systematic means of tracking unlicensed VASPs, blockchain transactions or the links between mobile payments and crypto settlements. The mobile payment, the VASP conversion and the blockchain destination exist in three separate worlds. No single institution connects them.

This is partly a consequence of how the regulations were designed. By restricting crypto through banks, regulators diverted activity to payment channels they were not equipped to monitor.



Above: what the mobile-wallet operator sees inside its system - versus what happens next, outside its visibility and regulatory scope. The transfer is fully KYC-verified and AML-screened. The crypto trade, exchange flow and onward sanctions exposure all occur after the operator's responsibility ends. Source: Crystal Intelligence.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

What blockchain analysis reveals: Egypt case study

Case study · Egypt · Ebtoo

HIGH-RISK INBOUND (1.8%)

$3.4M

LINKED TO ILLEGAL SERVICES

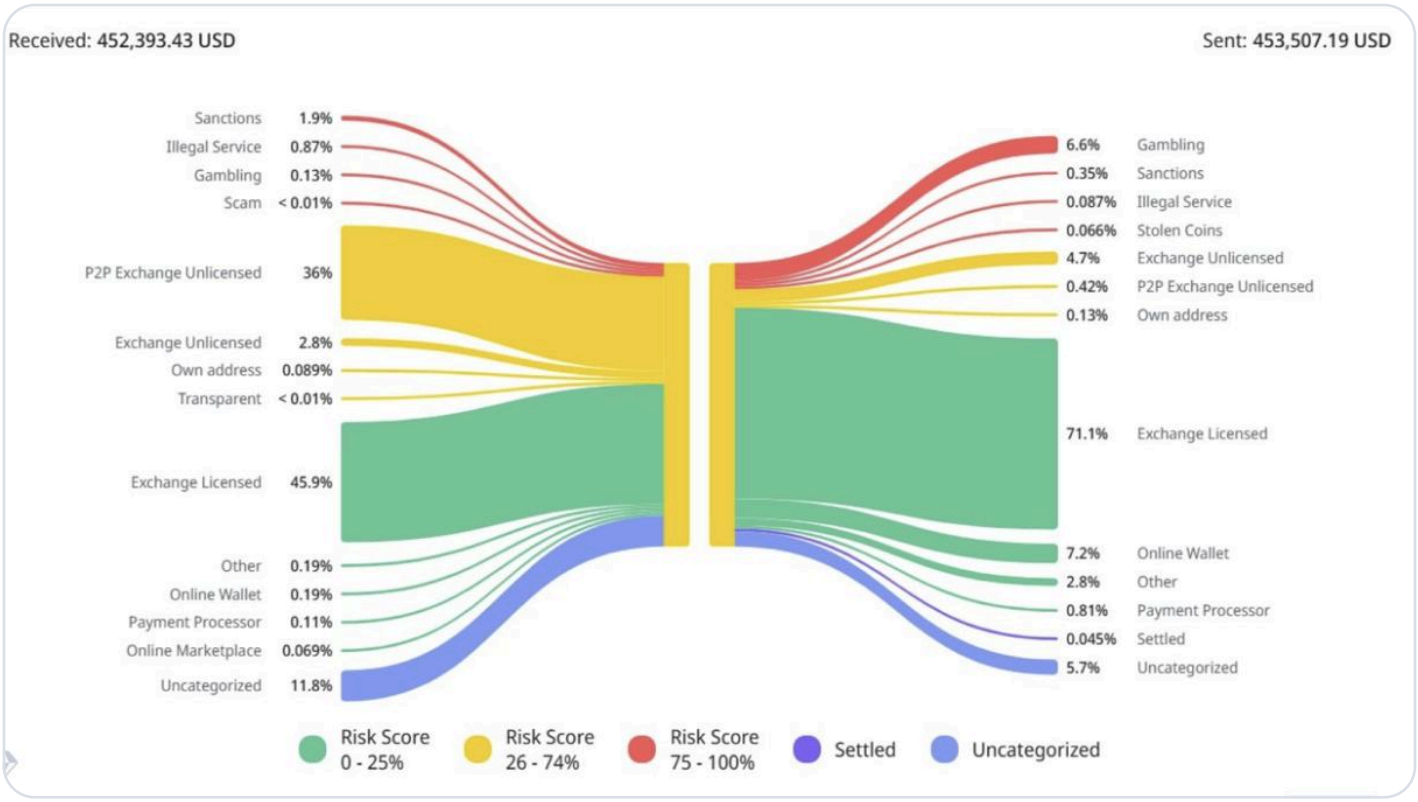
$1.4M

SANCTIONS-EXPOSED ENTITIES

$534K

Crypto trading is technically illegal in Egypt, yet the country has 50 million mobile-wallet accounts and 65% of the P2P advertisements Crystal analyzed settle via mobile money. The investigation of Ebtoo - an Egyptian VASP where 65% of ads specify mobile-wallet settlement - found 2.9% high-risk inflows and 6.9% high-risk outflows. Sanctions-linked entities accounted for 1.9% of inbound flows. Gambling exposure dominated the outbound side at 6.6%.

Read more case studies in our full mobile wallets report here.



Above: Ebtoo inbound and outbound on-chain flows by counterparty type and risk score. Received: $452,393 USD. Sent: $453,507 USD. The right-hand side (outbound) carries the heavier high-risk concentration - gambling 6.6%, sanctions 0.35%. Source: Crystal Intelligence.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 3:

Crypto-funded payment cards

Funds from a wallet with exposure to OFAC-sanctioned addresses move to a crypto-card provider registered in Georgia. No identity verification is required. The funds load onto a virtual debit card issued through a BIN sponsor and, within hours, are spent at a retail terminal in Western Europe. The acquiring bank processes it as a routine card payment. Nobody in the payment chain can see where the money came from.

NO-KYC OR LOW-FRICTION	PROVIDERS IDENTIFIED	TRACED ON-CHAIN INFLOWS	HIGH-RISK INFLO
67.7%	~100	$1.18B	$166M

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Scale and growth

The card payment ecosystem was built to monitor card transactions, not to screen the deposit of funds before they reach the payment network. When those funds originate from a blockchain wallet exposed to sanctioned entities, dark markets or fraud, the risk passes into traditional financial infrastructure undetected.

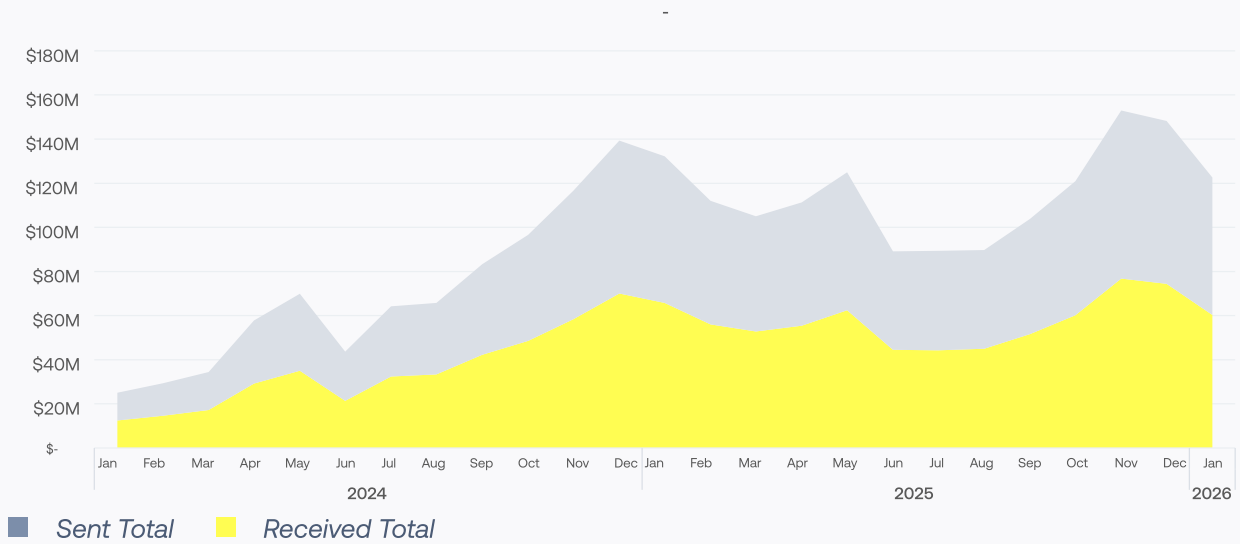
The gap is structural, not a failing of any single participant. Card networks set rules and onboard BIN sponsors, not individual cardholders. BIN sponsors onboard card-program providers, not end users. And the crypto providers issuing cards often operate with weak or absent identity verification. No single regulated entity in the chain has a complete view of the end user or the origin of their funds. Blockchain analytics can close that gap by providing upstream visibility that card-side monitoring cannot.

Crystal identified almost 100 crypto-funded payment-card providers and traced over $1.18B in on-chain flows linked to card-funding wallets between January 2024 and January 2026. The market is growing quickly: inbound volume rose approximately 66% year-over-year, with monthly volumes increasing more than fivefold between January 2024 and December 2025.

YEAR	TOTAL RECEIVED	TOTAL SENT	YOY GROWTH (RECEIVED)
2024	$415.5M	$410.7M	-
2025	$689.8M	$690.3M	+66%

Above: Crystal recorded a 66% increase in inbound on-chain flows from January 2024 to December 2025. Source: Crystal Intelligence

Growth patterns for crypto card services 2024-2026



Above: Mobile-financial-services share of P2P crypto listings across ten emerging markets, November 2025 – January 2026. Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Identity verification and high-risk exposure

Identity verification across the ecosystem

Crystal tested platforms by registering accounts, completing onboarding and reviewing identity requirements. The results reveal a systemic weakness: 67.7% of providers offer no KYC or only low-friction identity verification, in which users supply basic information that is never meaningfully verified.

Several platforms issued cards without completing any identity verification. Multiple providers showed weak or absent geographic restrictions, meaning cards are accessible in jurisdictions where financial services are restricted or prohibited - including sanctioned countries. Of the providers identified, 87.9% operate through websites or SaaS platforms.

The remaining 12.1% operate primarily through Telegram, where low- or no-verification card issuance is openly advertised.

High-risk exposure

Crystal traced $161.7M in high-risk inflows across the analyzed wallets.

Gambling accounts for 92.4% of this volume, but the remaining categories carry investigative weight.

$3.8M linked to sanctioned entities, $3.5M in stolen coins, $2.5M connected to scams, $1.7M through mixers, $1.5M from illegal services, and smaller amounts from dark markets, ransomware, and terrorism financing indicators.

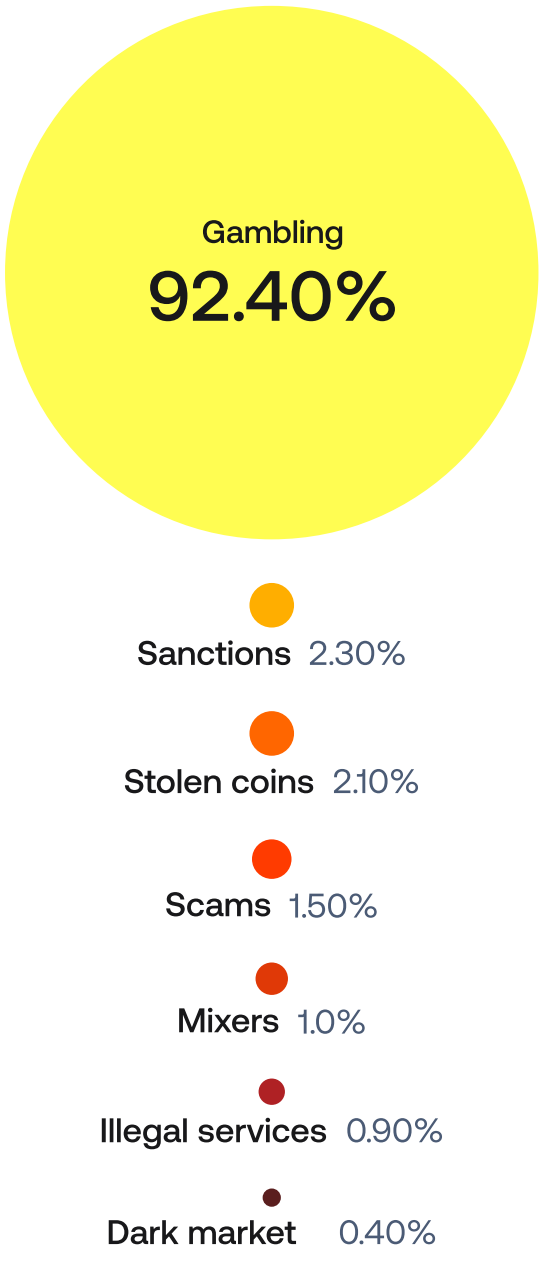
ENTITY TYPE	TOTAL	RECEIVED	SENT
Gambling	$153.8M	$153.6M	$148K
Sanctions	$3.8M	$2.55M	$1.27M
Stolen coins	$3.5M	$1.33M	$2.19M
Scams	$2.5M	$1.91M	$619K
Mixers	$1.7M	$1.58M	$108K
Illegal services	$1.5M	$1.47M	-
Dark market	$593K	$429K	$163K
Ransomware	$238K	$59K	$178K
Terrorism financing	$6.2K	$261	$5,891

Above: High-risk inbound and outbound flows traced across crypto-funded card provider wallets.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

How cards reach the payment network

Percentage of high-risk flows by type



Above: Percentage of high-risk flows by type across crypto-funded card provider wallets. Gambling dominates at 92.4%. The remaining categories (sanctions, stolen coins, scams, mixers, illegal services, dark market) sum to a smaller fraction, but each carries materially higher per-flow severity. Source: Crystal Intelligence.

Crypto-funded card programs access payment networks through BIN sponsorship arrangements with issuing banks.

Crystal identified 54 BINs associated with over 35 card providers across nine countries. Of these, 32 BINs (59%) are linked to providers that do not require KYC at the point of card issuance. Most identified BINs operate through one of two major global card networks.

The compliance gap sits in the layered structure of the card-program model. Card networks set rules and oversee BIN sponsors. BIN sponsors onboard crypto-card providers.

But neither the card network nor the BIN sponsor has direct oversight of the crypto provider's onboarding process for individual cardholders.

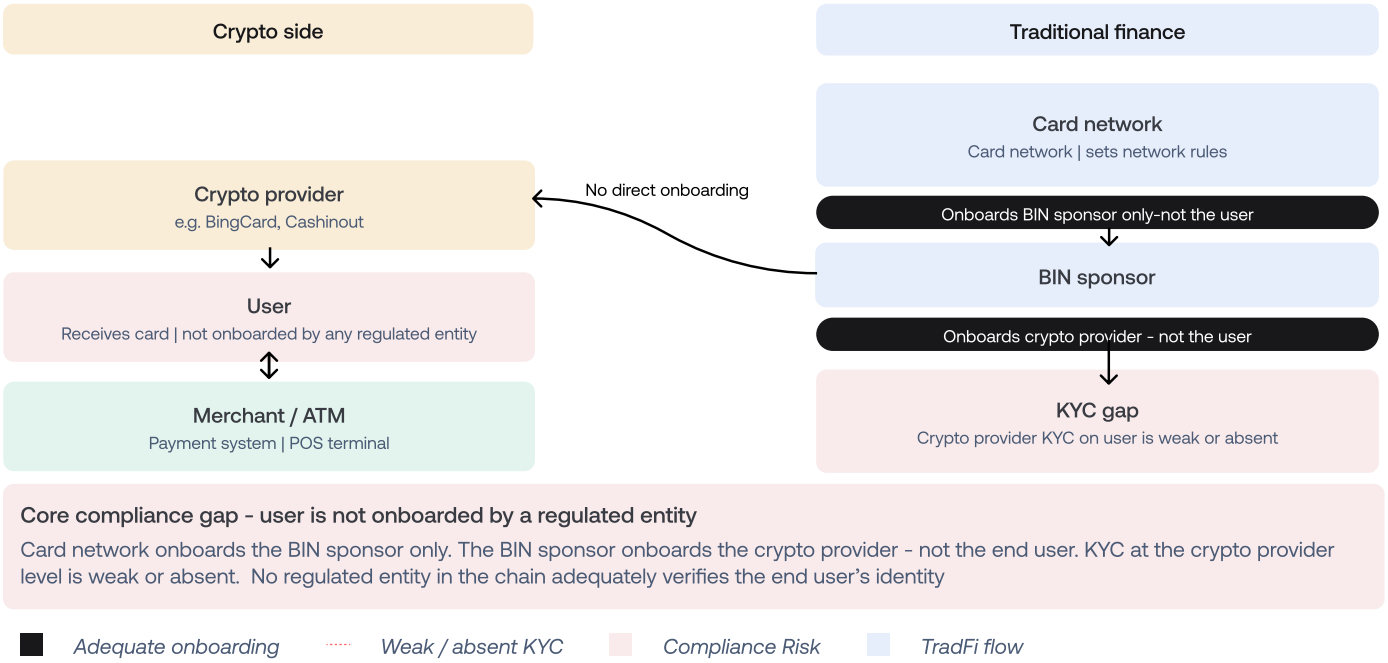
When that onboarding is weak or absent, the end user enters the traditional payment system without any regulated entity having verified their identity or the origin of their funds. This is a visibility problem that blockchain analytics can address directly.

By tracing on-chain flows into the wallets that fund card programs, it becomes possible to identify risk exposure before funds enter the payment network - the one point in the chain where the upstream origin is still visible.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

BIN concentration and jurisdiction

Schematic of the crypto-funded payment card life cycle

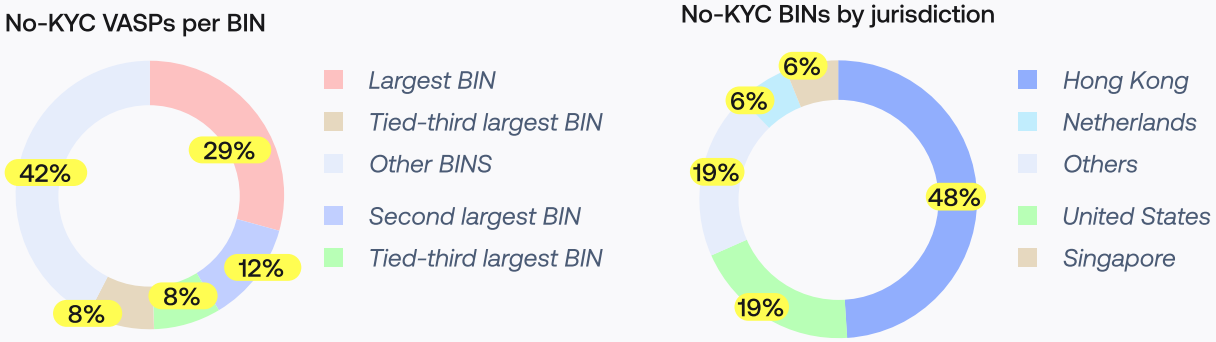


Above: schematic of the crypto-funded payment-card process. Card networks onboard the BIN sponsor only. The BIN sponsor onboards the crypto provider - not the end user. KYC at the crypto-provider level is weak or absent. No regulated entity in the chain adequately verifies the end user's identity.

Geographically, no-KYC card issuance concentrates in a handful of jurisdictions. Hong Kong accounts for nearly half of identified records (47%), with the United States at 16% and smaller shares from the Netherlands and Singapore.

A single BIN is shared by seven distinct no-KYC providers; the highest concentration identified. Targeted compliance intervention at even a small number of BIN sponsors could materially reduce the availability of anonymous crypto-funded cards.

No-KYC crypto cards: BIN concentration & jurisdictional distribution



Above: Schematic of the crypto-funded payment-card process. Card networks board the BIN sponsor only. The BIN sponsor onboards

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Entity A and Entity B

ENTITY A

Unlicensed provider, Georgia

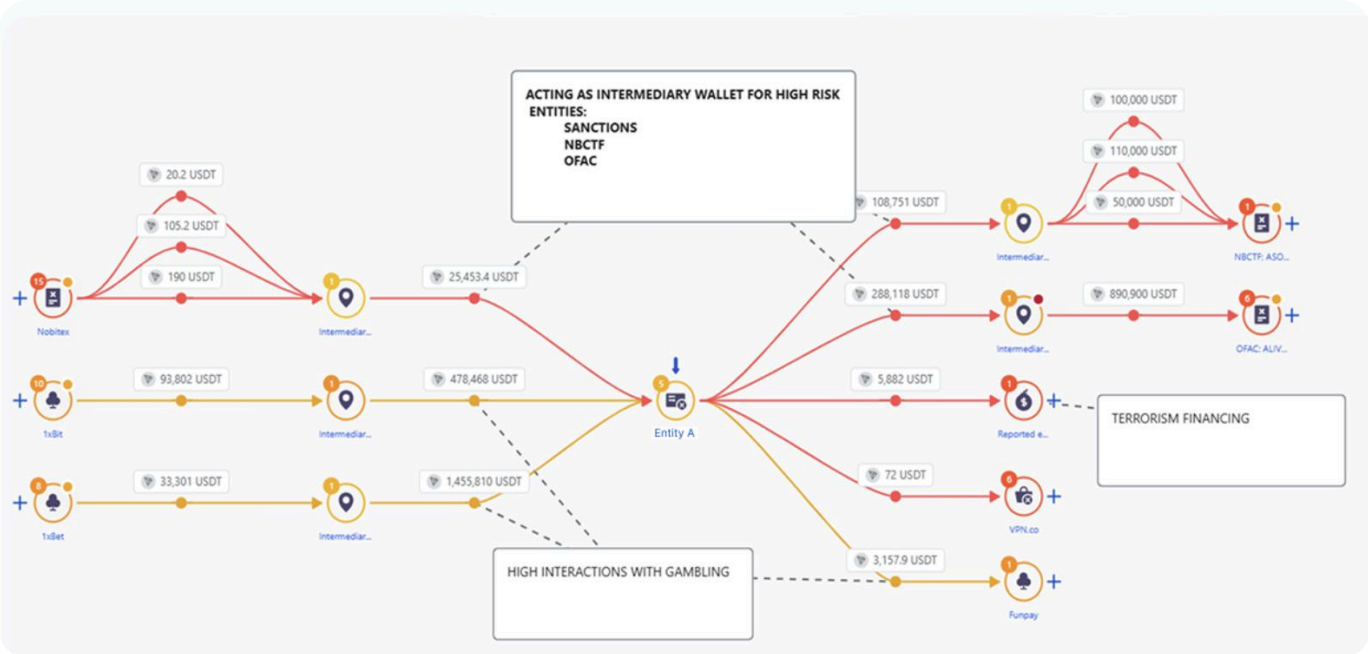
A crypto-based financial-services platform offering virtual payment cards and payment infrastructure, operated by a Georgia-registered company without a license for virtual-asset activity.
Entity A's linked wallets processed approximately $478.8M in inflows and $378.4M in outflows on TRON. On-chain tracing uncovered interactions with OFAC-sanctioned addresses, addresses designated by the National Bureau for Counter Terror Financing of Israel (NBCTF), gambling platforms and fraud-linked wallets. The platform promotes crypto-to-fiat conversion, international payments and virtual-card issuance via BIN sponsorship - all accessible without meaningful identity checks.

ENTITY B

Unlicensed provider, Georgia

A platform advertising virtual payment cards funded directly with crypto. Users can obtain and fund cards without completing identity verification. Entity B's wallets processed approximately $4.23M in inflows and $4.90M in outflows on BNB Smart Chain.

Tracing identified direct interactions with gambling platforms (500 Casino, CryptoLeo, RAMZINEX, Stake), sanctioned entities (OFAC: TASK, Versland), and addresses reported for fraud. The platform references Canada as its jurisdiction but discloses no verifiable legal entity or license.
Learn more about crypto-funded payment cards *here.*



Above: Entity A - on-chain interactions. Acting as intermediary wallet for high-risk entities including SANCTIONS, NBCTF and OFAC-designated addresses. High interactions with gambling platforms (1xBit, 1xBet, Funpay) and terrorism-financing-reported wallets. Source: Crystal Expert.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 4:

Red flags and indicators

The research behind this report surfaces patterns that compliance teams and investigators can use to assess their exposure to crypto-fiat conversion risks. Organized by channel - though the indicators often overlap. A single case may touch all three.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Red flags and indicators

Cash-to-crypto services

- **Deposit patterns that don't match individual use**
  Regular, round-number deposits arriving at consistent intervals from self-custody wallets with no prior on-chain history. A newly created wallet receiving a lump sum and depositing it to an exchange within days is consistent with a cash-to-crypto conversion, particularly if the pattern repeats across multiple accounts.

- **Geographic concentration signals**
  Jurisdictions with known concentrations of cash-desk operations - Hong Kong, Thailand, the UAE, parts of Eastern Europe - should receive additional scrutiny in counterparty risk assessments.

- **Multiple accounts funded from a narrow cluster**
  Where multiple accounts fund from the same wallet or a narrow cluster of wallets, the pattern is more consistent with intermediary activity than personal trading.

Mobile-wallet settlement

- **Counterparty exposure to restricted-market VASPs**
  VASPs operating in jurisdictions where crypto is banned or heavily restricted - particularly Egypt, Algeria, Bangladesh and Pakistan. In these markets, 58–83% of P2P settlement runs through mobile wallets, meaning on-ramp activity is systematically invisible to domestic regulators.

- **Chain selection signals**
  TRON and BNB Smart Chain dominate retail-scale P2P settlement because of low fees and high throughput.
  Outbound flows from VASPs in restricted markets to unlicensed exchanges or sanctioned entities should be treated as elevated risk.

- **Brokerage-shaped transaction patterns**
  Many small inbound transactions consolidating into fewer, larger outbound transfers to licensed exchanges - patterns suggesting the account is operating as an intermediary rather than a personal trader.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Red flags and indicators

Payment-card off-ramps

- **Outbound flows to known no-KYC card-provider deposit addresses**
  A direct risk indicator. Crystal's research identified 32 BINs across nine countries associated with card programs that do not require identity verification. Where card-funding wallets show high-risk upstream exposure like gambling, mixers or sanctioned entities, the risk compounds.

- **USDT on TRON as dominant chain**
  USDT on TRON is the dominant funding asset across the crypto-card ecosystem, consistent with the low-fee, high-volume profile that characterizes both legitimate and illicit use of these products.

- **Jurisdictional concentration**
  Hong Kong (47% of no-KYC BIN records), the United States (16%), and a small number of other jurisdictions account for the majority of anonymous crypto-card issuance.

- **Providers with no disclosed legal entity**
  Transactions originating from providers with no disclosed legal entity or verifiable license warrant the highest scrutiny.

22

unique BINs underpin every no-KYC crypto-card flow Crystal traced.

Takeaways

- *The indicators across the three channels overlap - a single case may touch cash desk, mobile wallet, and crypto card all at once.*
- *Geographic concentration is the most actionable common thread: Hong Kong, Eastern Europe, Egypt, Bangladesh, Pakistan, Ivory Coast all surface in multiple ways.*
- *Chain selection (TRON, BSC) and provider jurisdiction (Hong Kong, USA) are practical screens that can be applied at the wallet and BIN levels respectively.*
- *The indicators are useful precisely because they cross the fiat-crypto boundary. Pure on-chain rules miss them. Pure card-side rules miss them.*

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Recommendations: exchanges, VASPs, banks, and PSPs

Exchanges and VASPs

- **Incorporate no-KYC card-provider deposit addresses into outbound transaction monitoring**
  When funds leave your platform and flow to a wallet associated with a card provider that does not verify its users, that is a measurable risk event. The same logic applies to cash-desk intermediary patterns: accounts receiving regular, round-number deposits from wallets with no on-chain history should be flagged, not treated as routine self-custody activity.

- **Apply counterparty-VASP weighting to restricted markets**
  In markets where mobile financial services dominate peer-to-peer settlement, counterparty VASP exposure deserves particular attention. If a significant share of your platform's activity involves VASPs in jurisdictions where crypto is banned, the probability of exposure to unlicensed intermediaries and sanctions-linked flows increases.

- **Integrate physical intelligence into counterparty risk assessments**
  Integrating physical intelligence on cash-for-crypto services into counterparty risk assessments - rather than relying solely on on-chain data - closes a gap that purely digital analysis cannot address.

Banks and payment service providers

- **Run BIN-level risk assessment for crypto-funded card programs**
  For banks and PSPs, the exposure is less direct but no less real. Card transactions funded by unverified crypto are flowing through acquiring infrastructure now, and the standard card-monitoring toolkit was not designed to catch them. Identify which BINs are associated with no-KYC crypto providers and incorporate those into transaction monitoring.

- **Extend counterparty risk to crypto-fiat conversion channels**
  Counterparty risk assessments need to account for crypto-fiat conversion channels - not just direct exchange relationships. The correspondent bank that discovers its client exchange receives hundreds of millions from undocumented cash services has a different risk profile than the one whose client exchange does not. That distinction requires intelligence beyond what on-chain data alone provides.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Recommendations: card networks, BIN sponsors, and regulators

Card networks and BIN sponsors

- **Target due diligence at the issuer level**
  The risk is clear: 59% of identified BINs linked to crypto-card providers operate without meaningful KYC. A small number of BIN sponsors and issuing entities underpin a disproportionate share of no-KYC card issuance, which means that targeted due diligence at the issuer level can have an outsized effect.

- **Enhance monitoring of crypto-funded card programs**
  Include verification of the crypto provider's licensing status, KYC practices and geographic restrictions. Blockchain analytics offers a tool that card-side monitoring does not: the ability to see where funds originated before they reached the card. BIN sponsors that integrate upstream intelligence into their onboarding and ongoing monitoring would close a gap that currently allows high-risk funds to enter the payment system undetected.

Regulators

- **Card networks and BIN sponsors**

  The central regulatory challenge is jurisdictional fragmentation. No single authority currently oversees both the crypto side and the card-network side of crypto-funded payment cards. Similarly, no single regulator monitors both mobile-wallet transactions and the crypto settlements they facilitate. Cross-domain frameworks - connecting crypto AML obligations with card-network regulation and mobile-payment supervision - are the structural answer, though they will take time to develop.

- **Jurisdictions that ban crypto need blockchain monitoring capability**

  Prohibition without detection creates unenforceable policy. The research shows clearly that banning crypto does not stop it but rather pushes settlement to channels with less oversight.

- **Adapt existing payment-fraud frameworks for crypto typologies**

  Frameworks like PSD2 can be adapted to screen for crypto settlement typologies in mobile-money transfers, using indicators such as high-frequency transfers between unrelated parties and velocity patterns inconsistent with normal consumer use.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Recommendations: Law enforcement and investigators

For investigators, the most actionable finding in this report is that blockchain analytics can trace funds to the card-loading point, providing an evidence trail that traditional card-investigation data cannot. The on-chain record exists up to the moment funds convert to card spending power. That boundary is where card-side investigation and blockchain investigation need to meet.

Treat cash-for-crypto enforcement as a resource-allocation problem, not an intelligence problem

Many are physically accessible and operationally visible: they advertise on Telegram, list on P2P platforms and operate from identifiable commercial locations. Enforcement against the most prominent unlicensed operators - particularly in jurisdictions where crypto is prohibited - would establish deterrent effects without requiring sophisticated cyber capabilities. The intelligence on these targets already exists. The constraint, as multiple investigations have shown, is resource allocation rather than target identification.

Build cross-border cooperation around the full process

Regardless of the channel being exploited - cash entering at a desk, settling through a mobile wallet, and exiting via a payment card across multiple jurisdictions - cross-border cooperation frameworks remain essential for law enforcement and investigators. The laundering typology documented in this report is inherently multi-jurisdictional, and the investigative response needs to match.

Across all of our audiences, the underlying instruction is the same: move the monitoring across the boundary. Compliance can no longer be a wall built around the visible system. It has to be intelligence operating on both sides of every fiat-to-crypto edge in the process.

The on-chain record exists up to the moment funds convert to card spending power. That boundary is where card-side investigation and blockchain investigation need to meet.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Methodology

This report draws on three Crystal Intelligence investigations published between October 2025 and April 2026. Each used distinct but complementary research methods.

Physical intelligence collection

Crystal's research team identifies and documents unlicensed VASPs and cash-for-crypto services through on-the-ground intelligence work. Researchers locate operations, record their advertising and service offerings, and map their physical presence. This ground-truth approach surfaces patterns that purely digital analysis cannot reach.

Peer-to-peer market analysis

Crystal collected and categorized 57,829 peer-to-peer cryptocurrency advertisements across Ivory Coast, Ghana, Nigeria, Algeria, Egypt, Bangladesh, India, Pakistan, the Philippines and Colombia. Data was gathered from major P2P platforms between November 2025 and January 2026. Payment methods were classified into mobile financial services, traditional bank transfers and other methods, with the percentage share calculated for each market.

Blockchain forensic analysis

Crystal traced on-chain flows from identified VASPs and payment-card providers. For the mobile-wallet investigation, 45 VASPs were traced across 10 countries between January 2023 and December 2025.
For the payment-card investigation, approximately 120 wallets associated with card-provider infrastructure were identified, 66% of which were unique deposit and operational wallets.

Counterparties were categorized using Crystal's entity database. High-risk categories include sanctioned entities, gambling platforms, illegal services, stolen funds and scam-related addresses.

Limitations

P2P advertisement data reflects listed payment preferences, not confirmed transaction volumes. VASP tracing captures on-chain flows but not fiat-side values. Risk categorization depends on Crystal's entity labelling, which is continuously updated but may not capture all illicit activity. The cash-for-crypto mapping is ongoing and represents a documented subset of a larger ecosystem.

Research outlook

Crystal's work on crypto-fiat conversion infrastructure continues. Current research includes expanded cash-desk mapping in additional jurisdictions, peer-to-peer market analysis in further Latin American markets, and ongoing monitoring of the crypto-card ecosystem. Findings will appear in future editions of the Compliance Blindspots series.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

About Crystal Intelligence

Crystal Intelligence is a decision intelligence company for digital assets headquartered in Amsterdam. Founded in 2016, Crystal works with law enforcement agencies, financial institutions and cryptocurrency exchanges worldwide.

Three intelligence layers

1 Physical intelligence

On-the-ground research documenting unlicensed VASPs, cash services and conversion infrastructure - field-collected ground truth that tells the rest of the analytics where to look.

2 Market intelligence

Systematic monitoring of peer-to-peer platforms to track payment preferences and settlement patterns - the layer that produced the 57,829 listings underpinning Part 2 and the ~100-provider coverage underpinning Part 3.

3 Blockchain analysis

Tracing flows from identified entities to downstream destinations, quantifying exposure to sanctioned entities and high-risk counterparties across 330+ blockchains. ISO 27001 certified, GDPR compliant, EU-based data governance.

This research was conducted using Crystal Expert.

For country-specific intelligence, investigation support, or to discuss how ground-truth intelligence can strengthen your compliance or investigative capabilities - request a demo or contact our research team.

Get a demo →



Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Crystal Intelligence

© 2026 Crystal Intelligence. All rights reserved.

This report is intended for informational purposes only. The data provided herein is based on information publicly available and analysis conducted by Crystal Intelligence. Crystal Intelligence accepts no liability for actions taken based on this information. Readers are advised to perform independent verification and seek professional advice where necessary.