Bitkaya

BITKAYA RESEARCH — PRIMER SERIES

Wallet Monitoring in the Crypto Industry

What wallet owners and compliance specialists should understand about how blockchain screening works, how the industry uses it, and where its limits lie.

July 2026 · A Bitkaya Research Primer

Abstract

Public blockchains record every transaction permanently and transparently. That property has given rise to an entire industry of wallet and transaction monitoring: exchanges, custodians, banks, and regulators now rely on blockchain analytics to assess the risk associated with a wallet or transfer before deciding whether to accept, delay, or reject it. This paper explains what wallet monitoring is, how the practice developed, how it technically works, how the industry and its regulators use it, how risk scores are generated, and what wallet owners and compliance specialists should each understand about its capabilities and its limits. It closes with a look at the emerging challenges facing the field and the broader debate about surveillance and privacy that wallet monitoring sits within. It is written as general background for a broad audience and does not constitute legal, regulatory, or compliance advice for any specific situation.

1. Why Blockchain Activity Gets Monitored

Public ledgers such as Bitcoin and Ethereum are pseudonymous, not anonymous. An address is not inherently linked to a real-world identity, but every transaction it has ever made — and ever will make — is permanently visible to anyone who looks. Once an address is connected to an identity, whether through a know-your-customer (KYC) exchange, a data leak, a traceable payment for identifiable goods, or a voluntary disclosure, its entire transaction history, and the history of every address it interacts with, becomes analyzable in both directions.

This transparency is precisely what wallet monitoring tools exploit. They build models of the entities behind addresses and estimate the risk of transacting with them. Adoption of these tools has accelerated as institutional participation in crypto has grown, as high-profile hacks, ransomware payments, and sanctions-evasion cases have drawn regulatory attention, and as virtual asset service providers (VASPs) — exchanges, custodians, and brokers — have come under similar anti-money-laundering (AML) and counter-terrorist-financing (CFT) obligations to those long applied to banks.

KEY TAKEAWAY

Blockchain transparency cuts both ways: it protects the network's integrity, but it also means a wallet's history is permanent, cumulative, and analyzable by anyone with the right tools.

A brief history

Blockchain analytics grew out of academic and law-enforcement interest in de-anonymizing Bitcoin in the years following its creation, when researchers first demonstrated that clustering heuristics could group addresses into real-world entities. The practice moved from research curiosity to commercial industry after a string of early, high-profile cases — including the shutdown of darknet marketplaces and the collapse of exchanges following major hacks — showed that transaction trails on public blockchains could be reconstructed and used as evidence, even without cooperation from the parties involved. As institutional and regulatory interest in crypto grew through the following

decade, dedicated analytics firms emerged to package this capability as a commercial service, and regulators progressively began to expect VASPs to use it as part of standard AML/CFT compliance.

2. What "Wallet Monitoring" Actually Means

Two related but distinct practices sit under this term. Address (or wallet) screening is a point-in-time check of a specific address against watchlists and risk categories before a transaction is processed — conceptually similar to sanctions screening in traditional banking. Transaction monitoring is the ongoing surveillance of a customer's transaction flows over time, looking for patterns such as structuring, rapid layering, or a sudden shift toward newly flagged counterparties.

Underneath both practices sits a common technical process:

- **Clustering** — heuristics such as common-input-ownership and change-address detection group many addresses together into a single "entity" believed to be controlled by one actor.
- **Attribution** — clusters are labeled ("Exchange A," "Darknet market B," "Ransomware wallet," "Sanctioned entity") using a mix of licensed data, public information, law-enforcement disclosures, and voluntary reporting.
- **Exposure analysis** — for any given wallet, the tool calculates how much of its historical fund flow, direct and indirect, across a configurable number of transactional "hops," touches labeled high-risk clusters, and converts that into a composite risk score.

Because attribution databases, clustering heuristics, and scoring weights differ from one analytics vendor to the next, the same wallet can receive different scores from different providers — and a score can change retroactively as a provider updates its database or reclassifies a counterparty.

How confident is attribution, really?

Attribution is inferential, not verified fact. A label such as "Exchange A" or "Ransomware wallet" reflects a vendor's confidence that a cluster belongs to a given entity, built from evidence such as a KYC'd withdrawal to a known address, a scraped forum post, a law-enforcement seizure notice, or a voluntary self-report. Some labels are highly reliable — a large, long-observed exchange cluster, for instance — while others rest on thinner or older evidence and can be wrong, outdated, or reversed. Vendors generally do not publish a confidence score alongside a risk score, which is one reason a single number should not be treated as ground truth.

3. Categories of Risk Exposure

Analytics providers typically group counterparties into broad categories, and a wallet's score is built from its exposure across these categories. The categories below are illustrative of common industry practice rather than a fixed or universal taxonomy — providers vary in how finely they subdivide them.

Category	Description
Sanctioned entities	Individuals, groups, or addresses formally designated by a sanctions authority (for example OFAC's SDN list). Usually treated with zero or near-zero tolerance regardless of aggregate score.
Terrorist financing / state actors	Addresses linked to designated terrorist organizations or state-sponsored threat actors, such as groups associated with large-scale theft or sanctions evasion.
Darknet markets	Marketplaces facilitating the sale of illicit goods or services, typically accessed via anonymized networks.
Ransomware / extortion	Wallets used to receive ransom or extortion payments, often identified through incident response and law-enforcement cooperation.
Stolen funds	Proceeds of hacks, exploits, or fraud, traced from the point of theft through subsequent transfers.
Mixers and privacy tools	Services designed to obscure the trail between sending and receiving addresses, which reduce (but do not always eliminate) traceability.
Unregistered or high-risk exchanges	Platforms operating without appropriate licensing or with weak KYC/AML controls in their jurisdiction.
Gambling and high-risk merchants	Not inherently illicit, but often assigned an elevated risk weighting due to historical association with layering activity.
High-risk jurisdictions	Counterparties concentrated in jurisdictions identified by FATF or national regulators as having strategic AML/CFT deficiencies.

4. How the Industry Uses It

Exchanges, custodians, and payment processors use screening and monitoring as part of customer onboarding and transaction-level AML/CFT controls, often because it is a condition of their license. A small number of specialist blockchain analytics firms — among them Chainalysis, Elliptic, and TRM Labs — supply much of the attribution data and scoring engines that VASPs plug into; results are not identical across vendors, and none of them constitutes an official or regulatory determination. Regulators and law-enforcement agencies use comparable techniques to investigate fraud, ransomware, and sanctions evasion, and increasingly expect VASPs to demonstrate that screening and monitoring controls are in place. Traditional banks that offer accounts to crypto businesses, and insurers that underwrite custody risk, increasingly request or rely on the same analytics as part of their own due diligence.

A typical screening workflow

While implementations vary, a transaction passing through a VASP's compliance stack commonly follows a sequence similar to this:

- The incoming or outgoing address is checked against sanctions and watchlists, and a risk score is pulled from one or more analytics providers.
- The score and its underlying exposure categories are compared against the VASP's own internal thresholds and rules, not just the vendor's default tiers.
- Transactions within accepted parameters proceed automatically; those that breach a threshold, involve a flagged category (especially sanctions), or trip a separate rule (large amount, new wallet, unusual pattern) are routed to manual review.
- A compliance analyst reviews the flagged case, may request supporting documentation (source of funds, business rationale) from the customer, and decides to clear, hold, reject, or escalate the transaction.
- Where required by local law, a suspicious activity or transaction report (SAR/STR) is filed with the relevant financial intelligence unit, and the decision and its rationale are documented for audit purposes.

Regulatory backdrop (general, non-exhaustive)

The Financial Action Task Force (FATF), the global AML/CFT standard-setter, has extended its long-standing “Travel Rule” (Recommendation 16) to virtual asset transfers, expecting VASPs to collect and share originator and beneficiary information above set thresholds. National and regional regulators implement FATF's standards in their own rules: in the European Union, the Markets in Crypto-Assets Regulation (MiCA) and the recast Transfer of Funds Regulation apply Travel-Rule-style obligations to crypto-asset service providers; in the United States, FinCEN's Bank Secrecy Act framework treats many crypto businesses as money services businesses subject to the existing funds-transfer recordkeeping rule, and the Treasury's Office of Foreign Assets Control (OFAC) maintains sanctions lists that have, at various points, included specific virtual-currency addresses tied to sanctioned individuals or groups. Other jurisdictions, including the United Kingdom and Singapore, have adopted broadly comparable licensing and AML regimes for crypto businesses built on the same FATF baseline.

READ WITH CARE

Regulatory thresholds, sanctioned-address designations, and even the legal status of specific designations change over time and have been subject to litigation in some jurisdictions. This section is general background, not a current legal statement — always verify specific requirements and lists against FATF, national regulators, and OFAC directly before relying on them operationally.

5. The Travel Rule in Depth — and Why Monitoring Fills Its Gaps

The Travel Rule is worth examining more closely, because the practical relationship between it and wallet monitoring is one of the more misunderstood parts of crypto compliance: the two controls answer different questions, but monitoring has become the default fallback wherever the Travel Rule's identity-exchange model cannot reach.

What the Travel Rule actually requires

The rule originates in traditional wire-transfer regulation. FATF Recommendation 16 requires financial institutions to obtain, hold, and pass on certain originator and beneficiary information whenever they send or receive a funds transfer above a threshold, so the information "travels" with the payment through any intermediary institutions. In the United States, the equivalent sits in the Bank Secrecy Act's implementing rule at 31 CFR 1010.410(e)-(f): it applies to non-bank money transmitters at a $3,000 threshold and requires the sending institution to obtain and pass on the transmittor's name, address, and account number, the transfer amount and date, and the recipient's name, address, and account number, to the extent that information is received. FinCEN's long-standing guidance treats many crypto exchanges as money transmitters, which is the basis on which this framework has been applied to virtual-currency transfers. In the European Union, Regulation (EU) 2023/1113 (the recast Transfer of Funds Regulation) extended comparable obligations to crypto-asset service providers, reportedly without the minimum-amount exemption that applies to some traditional transfers. FATF's 2019 update to Recommendation 15 and its Interpretive Note is the underlying global standard both regimes implement, and FATF's 2021 updated guidance for a risk-based approach to virtual assets sets out how VASPs are expected to apply it.

Why crypto transfers are harder than bank wires

The Travel Rule was designed for correspondent banking, where a message — historically over a network like SWIFT, or a domestic clearing system — natively carries the compliance data fields alongside the payment instruction, because the sending and receiving institutions are both parties to the same messaging network. A blockchain transaction has no equivalent built-in channel: the chain itself transmits value, not identity information, and a public address on its own reveals nothing about who controls it. To comply, a sending VASP must identify which entity operates the receiving wallet, establish a side-channel with that counterparty, and exchange the required originator and beneficiary data — commonly using a shared data model such as IVMS 101 — separately from, but alongside, the actual on-chain transfer. That is a materially harder problem than passing fields through an existing wire network, and it depends on two independently operated compliance programs successfully connecting, which does not always happen even when both sides intend to comply.

The sunrise problem and unhosted wallets

Because countries have adopted and enforced the FATF standard at different speeds, a VASP in a jurisdiction with a mature Travel Rule regime often cannot complete a compliant data exchange with a counterparty in a jurisdiction that has not yet implemented equivalent requirements, or that uses an incompatible messaging solution — a timing and interoperability mismatch the industry commonly calls the "sunrise problem." A more fundamental gap arises

when funds move to or from a self-hosted (unhosted) wallet: a personal, non-custodial wallet has no operator to identify or contact, so there is no counterparty compliance program to exchange data with in the first place. FATF's guidance acknowledges this scenario directly and points VASPs toward risk-based mitigating measures rather than a data exchange that has no counterparty to receive it.

How transaction monitoring steps into the gap

This is the gap wallet and transaction monitoring fills. Where a VASP cannot obtain or verify counterparty identity data — because the counterparty VASP is unreachable, runs an incompatible messaging solution, sits in a jurisdiction that has not implemented the rule, or does not exist at all, as with a self-hosted wallet — it typically substitutes exposure-based screening of the address itself: pulling a risk score, checking it against sanctions and watchlists, and assessing the categories of counterparties that address has touched. In effect, when the compliance question “who is on the other end of this transfer?” cannot be answered through the Travel Rule's identity-exchange channel, VASPs commonly fall back to a different question they can usually answer instead: “what does this specific address's on-chain history look like?” That shift, from verifying identity to scoring exposure, is why transaction monitoring functions in practice as a working substitute for Travel Rule compliance across a large share of real-world transfers — particularly those flowing to or from self-hosted wallets, which by some industry estimates represent a substantial and growing portion of crypto transaction volume.

TWO DIFFERENT CONTROLS, NOT ONE

Travel Rule compliance and wallet risk scoring answer different questions, and regulators do not treat them as interchangeable. Where a counterparty VASP is identifiable and the rule technically applies, substituting wallet monitoring for the required data exchange does not, by itself, satisfy the legal obligation — supervisors can still expect evidence that a VASP attempted to identify and exchange data with a compliant counterparty. Monitoring is best understood as a compensating control for scenarios the Travel Rule's messaging model does not reach — unhosted wallets and sunrise-related gaps — rather than a substitute a VASP may choose instead of pursuing Travel Rule compliance where it is genuinely achievable.

6. Understanding the Risk Score

A risk score is a vendor-generated estimate, not a regulatory or legal determination, and not an inherent property of a wallet, a transaction, or a token. It typically reflects the category of counterparties a wallet has touched (exchange, DeFi protocol, mixer, darknet market, sanctioned entity, stolen funds), how directly it is exposed to them (a single hop versus several intermediary hops), and what proportion of the wallet's total activity that exposure represents.

Many providers and VASPs group scores into broad tiers — commonly some variation of low, medium, high, and severe risk — but the exact cut-offs are set by each vendor or each VASP's own risk appetite; there is no single regulatory percentage that applies industry-wide. Composition typically matters more than the headline number: a low aggregate score built on a small amount of direct sanctions exposure is often treated more seriously than a higher score arising mainly from indirect exposure to a regulated exchange.

7. What Wallet Owners Should Know

- **Your history is permanent and cumulative.** Every counterparty a wallet has ever interacted with remains part of its analyzable history; moving funds to a different token, chain, or new wallet does not erase that history if the provenance of the funds can still be traced, for example through a bridge or a swap.
- **You can inherit risk.** Receiving funds from a wallet with a problematic history can affect how your own wallet is scored, even without any wrongdoing on your part.
- **A favorable score is not a guarantee.** Even a wallet with a low score can be delayed, held, or asked for supporting information by a specific exchange, custodian, or bank, because each platform layers its own monitoring rules on top of any third-party score.
- **Basic hygiene helps.** Keep records of the source of significant funds, be cautious about routing value through services you do not understand (particularly mixers or unfamiliar bridges) if you intend to use regulated platforms, and expect that large or unusual transfers may trigger manual review regardless of your wallet's score.
- **Errors do happen.** Because attribution is inferential, a wallet can occasionally be mislabeled or associated with a counterparty in error; if you believe a screening result is wrong, most VASPs and analytics vendors have a process to submit supporting evidence for review.

8. What Compliance Specialists Should Know

- **Treat scores as one input, not a decision.** A risk-based approach means controls should be calibrated to your own institution's risk appetite and the specific facts of a transaction, not to a single number imported from a counterparty or vendor.
- **Composition over aggregate.** Two wallets with an identical score can carry very different risk depending on whether the exposure is direct and sanctions-related or indirect and diffuse; reviewing the underlying exposure categories is usually more informative than the percentage alone.
- **Set and document your own thresholds.** Because vendor scores and methodologies diverge and change over time, a defensible compliance program defines its own escalation criteria and records the rationale, rather than adopting a counterparty's threshold as a binding rule.
- **Screen and monitor continuously.** A wallet's score can change after the fact as attribution databases are updated, so a one-time check at onboarding is generally not sufficient for higher-risk or long-term relationships.
- **Sanctions exposure is different in kind.** Many jurisdictions apply strict, or near-strict, liability to dealings with sanctioned addresses, so direct or close proximity to a sanctioned entity typically warrants escalation regardless of the aggregate score.
- **Keep a human in the loop.** Automated scores should support, not replace, a documented judgment call by a named, accountable compliance officer — particularly for edge cases and large or unusual transactions.

- **Consider multiple providers for material decisions.** Given that vendors diverge, cross-checking a second source before rejecting a significant transaction or relationship can reduce the risk of acting on a single provider's blind spot.
- **Keep records proportionate to risk.** Retain the score, its underlying composition, the decision made, and its rationale for higher-risk or escalated cases, consistent with your own recordkeeping obligations and policy.
- **Give unhosted-wallet transfers extra weight.** Where Travel Rule data exchange is not possible — most commonly with self-hosted wallets — wallet risk scoring is often your primary de facto control for that transfer, not a secondary one; treat it with the same rigor you would apply to a completed identity check.

9. Emerging Challenges and Limitations

Coverage varies by chain and technique. Transparent account- or UTXO-based chains such as Bitcoin and Ethereum are relatively traceable with today's tooling, while privacy-focused coins, mixing services, and techniques such as “peel chains” or rapid cross-chain bridge-hopping can meaningfully reduce traceability. As decentralized finance (DeFi) protocols and non-custodial wallets grow in importance, monitoring tools face a harder problem: many DeFi interactions involve smart contracts rather than identifiable counterparties, and there is often no intermediary VASP in the flow of funds to apply screening at all.

Cross-chain bridges add a further layer of complexity, since assets can move between blockchains with different levels of analytics coverage, sometimes breaking the continuity of a traceable history or making it harder to attribute the same underlying value across chains. Clustering heuristics and attribution labels remain inferential rather than verified in every instance, so false positives and false negatives occur — with a real cost to legitimate users who are delayed or de-banked based on an incorrect or overly broad label. There is also no cross-vendor standardization: comparing scores across providers, or treating any single score as an industry-wide benchmark, requires care. Finally, the field faces a degree of regulatory fragmentation, as jurisdictions move at different speeds and with different thresholds, leaving VASPs to reconcile multiple, sometimes inconsistent, compliance regimes.

10. The Privacy–Surveillance Debate

Wallet monitoring sits inside a broader, ongoing debate about the balance between financial oversight and individual privacy. Proponents argue that the same transparency and traceability that make monitoring possible are essential tools for recovering stolen funds, disrupting ransomware and sanctions evasion, and giving regulated institutions the confidence to serve the crypto industry at all — without which access to banking and exchange services would likely be far more restricted. Critics counter that aggregated risk scoring can function as a form of financial surveillance applied to ordinary users, that inherited or indirect risk can unfairly penalize people with no wrongdoing of their own, and that opaque, proprietary scoring methodologies make it difficult for an affected individual to understand or contest a decision made about them.

Both perspectives draw on legitimate concerns, and the appropriate balance between them is ultimately a policy question being worked out differently across jurisdictions, rather than a settled technical one. Readers forming a view on this question may find it useful to weigh the crime-prevention and market-access benefits described by

industry and regulators against the due-process and privacy concerns raised by digital-rights and civil-liberties organizations.

11. Conclusion

Wallet monitoring has become a core part of how the crypto industry meets AML/CFT expectations, but it remains a probabilistic, vendor-dependent tool rather than a definitive verdict. For wallet owners, the key practical point is that transaction history is permanent, cumulative, and inheritable. For compliance specialists, a score is a starting point for a risk-based judgment, not a substitute for one — and, in the substantial share of transfers involving self-hosted wallets or sunrise-affected counterparties, it is often the primary risk control available where the Travel Rule's identity-exchange model cannot reach. And for the industry as a whole, the field continues to face real technical and policy challenges — from DeFi and cross-chain complexity to the broader question of how much financial surveillance is appropriate. Both practitioner audiences are better served by understanding how the underlying analysis works than by treating any single number as authoritative.

Glossary of Key Terms

Term	Meaning
VASP	Virtual Asset Service Provider — a business (exchange, custodian, broker) that provides services involving virtual assets and is generally subject to AML/CFT regulation.
Travel Rule	A FATF standard (Recommendation 16) requiring originator and beneficiary information to travel with a funds transfer above a threshold; extended to virtual assets.
IVMS 101	A common data model used by Travel Rule messaging solutions so originator and beneficiary information can be exchanged in a consistent, machine-readable format between VASPs.
Sunrise problem	The industry term for the gap that arises when counterparties are in jurisdictions or on systems that have not yet implemented the Travel Rule at the same pace, preventing a full compliant data exchange.
Unhosted / self-hosted wallet	A wallet controlled directly by an individual rather than by a custodial VASP, meaning there is no counterparty institution with which to exchange Travel Rule data.
Cluster	A group of blockchain addresses inferred to be controlled by a single real-world actor, identified through heuristic analysis.
Attribution	The process of labeling a cluster with a real-world identity or category based on available evidence.
Hop	One step in a chain of transactions; “direct” exposure is one hop away, “indirect” exposure is several hops away.
Risk-based approach	A regulatory principle, endorsed by FATF, under which controls are calibrated to the level of risk presented rather than applied uniformly.
SAR / STR	Suspicious Activity Report / Suspicious Transaction Report — a filing made to a financial intelligence unit when suspicious activity is identified, per local law.
Sanctions list	A list maintained by a government authority (such as OFAC's SDN list) naming individuals, entities, or in some cases addresses subject to restrictions.
Mixer	A service designed to obscure the link between the sender and recipient of funds by pooling and redistributing them.
Peel chain	A pattern of successive small transfers from a larger balance, sometimes used to obscure the ultimate destination of funds.

Selected References for Further Reading

- **Financial Action Task Force (FATF).** Guidance for a Risk-Based Approach to Virtual Assets and VASPs — fatf-gafi.org
- **FinCEN.** Bank Secrecy Act guidance on convertible virtual currencies — fincen.gov
- **31 CFR § 1010.410(e)-(f).** Recordkeeping and transmittal-order requirements for the U.S. funds-transfer ("Travel") Rule — ecfr.gov
- **U.S. Treasury, Office of Foreign Assets Control (OFAC).** Sanctions List Search and FAQs — ofac.treasury.gov
- **European Union.** Markets in Crypto-Assets Regulation (MiCA) and recast Transfer of Funds Regulation — eur-lex.europa.eu

Disclaimer

This document reflects general, publicly available industry and regulatory information available to Bitkaya at the time of writing (July 2026) and is provided for informational purposes only. It is not legal, regulatory, or compliance advice for any specific transaction, entity, or situation, and should not be relied upon as such.

Regulatory thresholds, sanctioned-address designations, and the legal status of specific designations change over time and have been subject to litigation in some jurisdictions; specific requirements and lists should always be verified against FATF, national regulators, and OFAC (or the equivalent authority) directly before being relied upon operationally.

Bitkaya makes no representation or warranty, express or implied, as to the accuracy or completeness of the information in this document and accepts no liability for any loss arising from any use of, or reliance on, it.