STATE OF DECENTRALIZED PRIVACY 2026
NEOCYPHERPUNK SUMMIT EDITION

"We've accelerated narratives enough.

Let's accelerate the cypherpunk privacy reality."

— Vitalik Buterin, 2026

WORKING HYPOTHESIS + 6 KEY SIGNALS

Across the world, people face circumstances where privacy is not a preference but a condition of safety. A journalist protecting a source in a country with press restrictions. An activist coordinating without exposing their network. An ordinary person in a jurisdiction where financial surveillance is a tool of political control. For these people, the question of whether decentralized privacy technology actually works; not in theory, not on a whitepaper, but in the hands of someone who has never heard of a zero-knowledge proof; is not an academic question. This report attempts to answer it honestly.

THE SWEENEY ARTISTS

"Without Privacy there is no Democracy"

The infrastructure is advancing faster than the people who need it can reach it. In 2025, more than 820 projects actively built privacy tooling across every major decentralized ecosystem. Over five billion dollars moved through Railgun since its launch, including a record $1.6 billion in 2025.
The Ethereum Foundation formed a 47-person team dedicated solely to making privacy practical. Zero-knowledge cryptography, once the domain of academic specialists, is now routinely shipped by two-person wallet teams.
The technology is ready. It is not yet reaching the people who need it most, and this report examines why.
Only one in four privacy projects has privacy on by default.

> **Every Ethereum wallet tested by independent research (Walletbeat) fails the most basic privacy criterion.**
> **The tools that offer the strongest privacy guarantees are, with few exceptions, unusable by anyone who hasn't already decided to learn them.**

Alongside this technical gap sits a political one.
Institutions and individuals do not agree on what "privacy" means.
Circle, the issuer of the world's second-largest stablecoin (USDC), launched a privacy product in 2025 that keeps a compliance record accessible to regulators on request. Users of Tornado Cash, where sanctions were lifted in March 2025, overwhelmingly choose DAI: the stablecoin that cannot be frozen. Both groups are seeking privacy. They are seeking different things.

This report is written for
activists, and anyone who
decentralized systems becc
human au
or whether they remain a f
privacy featı
afterthc

or builders, researchers,
ho has a stake in whether
come a meaningful tool for
autonomy;
a financial instrument with
atures as an
hought.

826 projects are tracked in total; 72 have been discontinued and are excluded from analysis. All percentages and breakdowns use the 754 active figure unless otherwise stated. All data collected from public sources, April–June 2026. Sources and limitations documented. Summit edition; full v2 report planned July–August 2026.

ON THE WORKING HYPOTHESIS

This research began with a hypothesis: that decentralized privacy is advancing rapidly at the infrastructure level, but real-world adoption is shaped by usability challenges, fragmented implementations, and growing tension between institutional and individual privacy needs. The evidence largely confirms it; with one refinement. The institutional–individual tension is not merely background. It is the organizing dynamic of the ecosystem, and how it resolves will shape who can use these tools, for what purposes, and under what conditions.

The central finding is not that decentralized privacy has failed. It is that infrastructure is running significantly ahead of adoption; and that the gap between the two is primarily a design problem, not a cryptographic one.

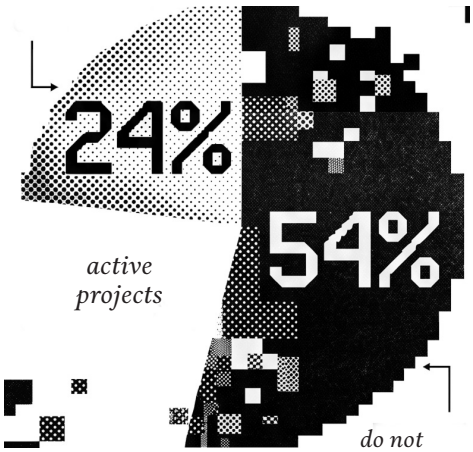
SIX SIGNALS FROM 2025

826

projects

mapped across the decentralized privacy ecosystem (applications, infrastructure, DeFi, social, hardware)

privacy on by default.



active projects

do not specify

8% → ~30%

of Zcash's circulating supply now held in shielded addresses (up from 8% in early 2024)

0/21

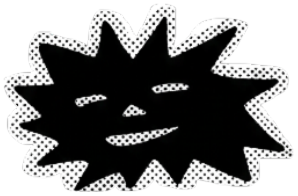
Ethereum wallets evaluated pass the most basic privacy criterions

$4.2B+

in stablecoin volume tracked across six privacy protocols in 2025

7.8%

of active projects have been independently security audited



Signal 1: Part A

THE PRIVACY ECOSYSTEM AT SCALE

The Web3Privacy Now Explorer database tracks decentralized privacy projects across all major ecosystems: 826 entries, 754 actively maintained. The project landscape is broader than a financial-privacy frame would suggest. Applications (378 projects) and infrastructure (303) account for 89% of the database. DeFi-specific projects represent 127. Social and communications tools account for 72. Hardware privacy devices account for 20.

Terminology Used

Zero-knowledge proof: a cryptographic method that lets one party prove something is true without revealing any underlying information; applied to transactions, where the sender proves a payment is valid without revealing who sent it, received it, or the amount.

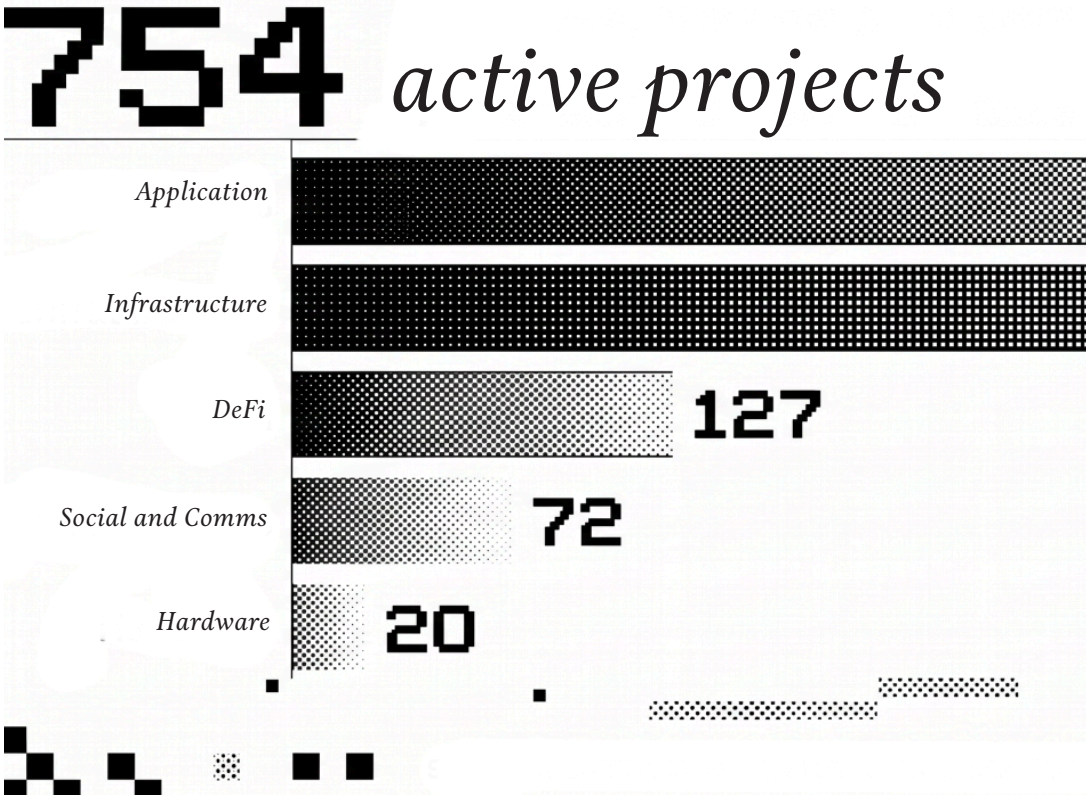
Shielded transaction: a transaction whose sender, receiver, and amount are hidden using cryptography.

Onchain: stored and verifiable on a public/private blockchain.

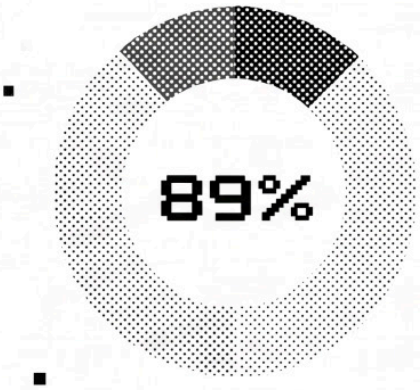
Stablecoin: a digital currency designed to hold a fixed value relative to a reference asset (usually one US dollar).

Default-on privacy: a system where the user receives privacy protection automatically, without needing to understand or configure anything. The opposite; opt-in requires a deliberate choice.

PRIVACY PROJECTS CATEGORIES



Applications and infrastructure together account for 89% of active projects (DeFi represents 17%).
Source: Web3Privacy Now Explorer, May 2026.



of all projects

account for applications and infrastructure together

Across 754 active projects, c

projects), private messaging

DAO governance (17), and V

(27) together represent a subst

Privacy technology is freque

tool for concealing financial

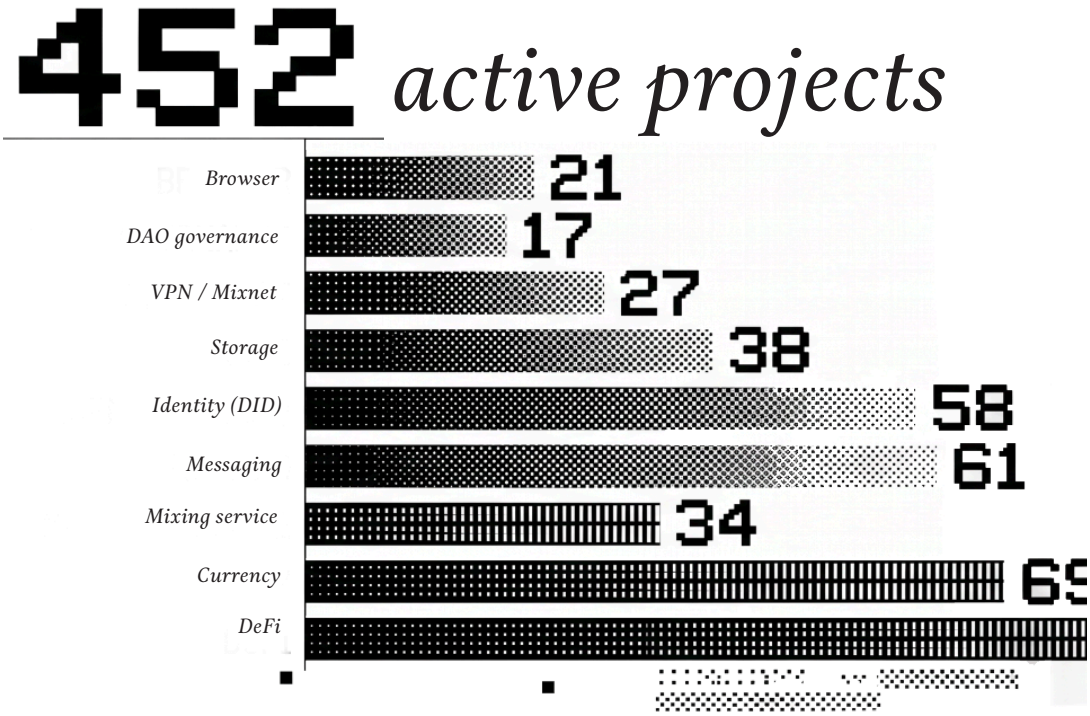
evidence does not support th

projects in this database are nc

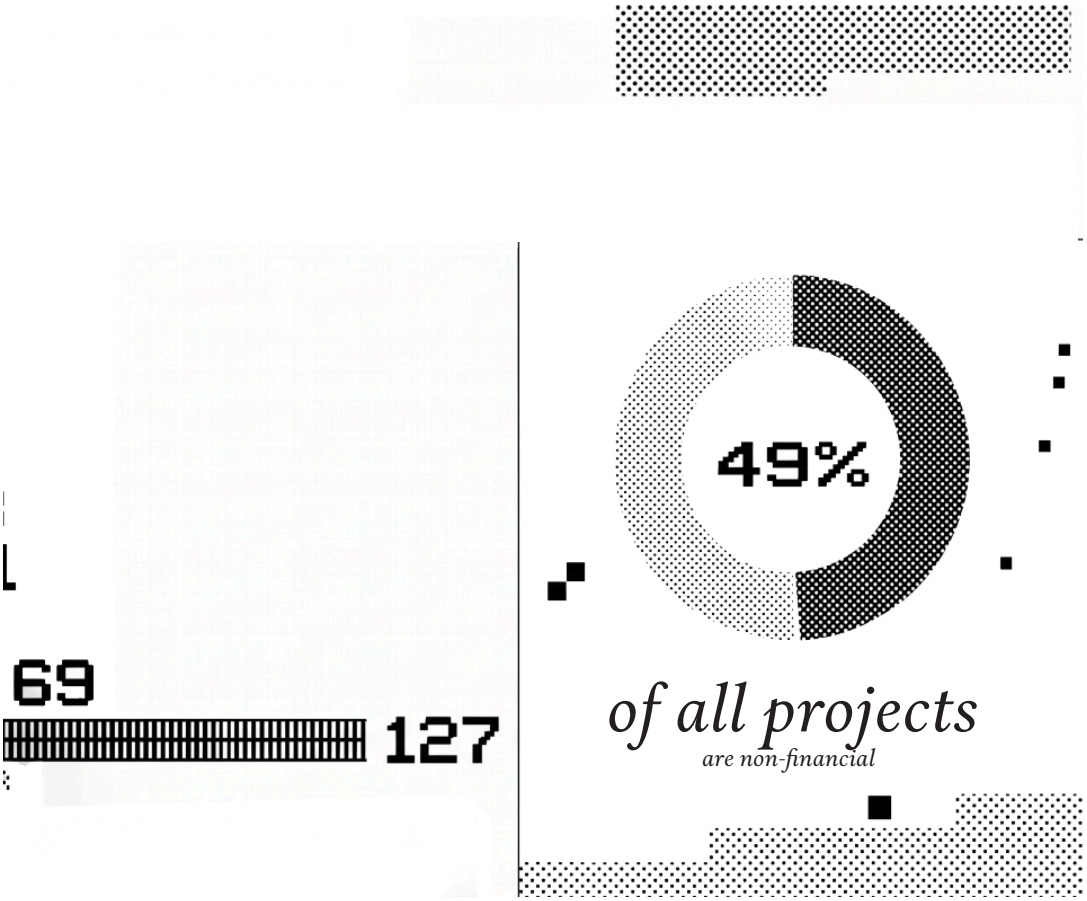
building infrastructure for a p

s, decentralized identity (58
ıg (61), private storage (38),
VPN/mixnet infrastructure
ɔstantial non-financial cluster.
ıently framed as primarily a
al activity. The project-level
that frame. The majority of
not building mixers. They are
ı privacy-respecting internet.

FINANCIAL VS. NON-FINANCIAL USE CASES



Non-financial privacy use cases (identity, messaging, storage, governance) account for nearly as many project tags as financial use cases.
Source: Web3Privacy Now Explorer, May 2026.



of all projects
are non-financial

Ethereum remains t
ecosystem with 248
follows with 101, Bitc
with 47. Only 171 p
support multiple chain
on Ethereum, combine
chain support, is

Source: Web3Privacy Now Explorer (explorer-data.web3privacy.info), May 2026.

s the dominant host
48 projects. Solana
coin with 81, Monero
projects explicitly
ns. The concentration
ned with limited multi-
s itself a finding.

Signal 1: Part B

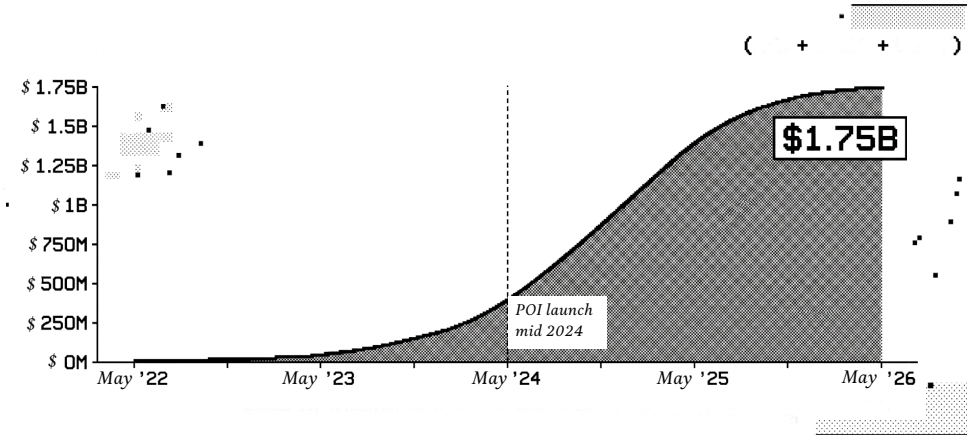
INFRASTRUCTURE IS GROWING

Across ecosystems and technical approaches; ZK proofs, FHE, trusted execution environments, stealth addresses, mixnets; 2025 was a year of significant infrastructure development. The question is not whether privacy infrastructure is being built. It is whether it is being used.

Onchain Usage

Railgun processed over $5 billion in private transactions since its 2021 launch; including a record $1.6 billion in 2025; making it the largest privacy protocol by transaction volume on Ethereum. The AMLBot stablecoin dashboard separately tracks $1.75 billion in stablecoin-only volume (DAI, USDC, USDT combined). These are distinct figures: the $5 billion covers all assets; the $1.75 billion covers stablecoins only. Monthly flow data shows sustained activity from mid-2024 through early 2026, with peak months exceeding $250 million. The fee line; consistently $300–600K per month from mid-2024; never approached zero across 48 consecutive months: the signature of a retained user base, not event-driven spikes.

Railgun cumulative stablecoin volume



Cumulative stablecoin volume reached $1,748,159,837 (May 14, 2026).
Steepest growth after POI launch mid-2024.
Source: AMLBot Dune dashboard, May 14 2026.

New milestone: May 6, 2026

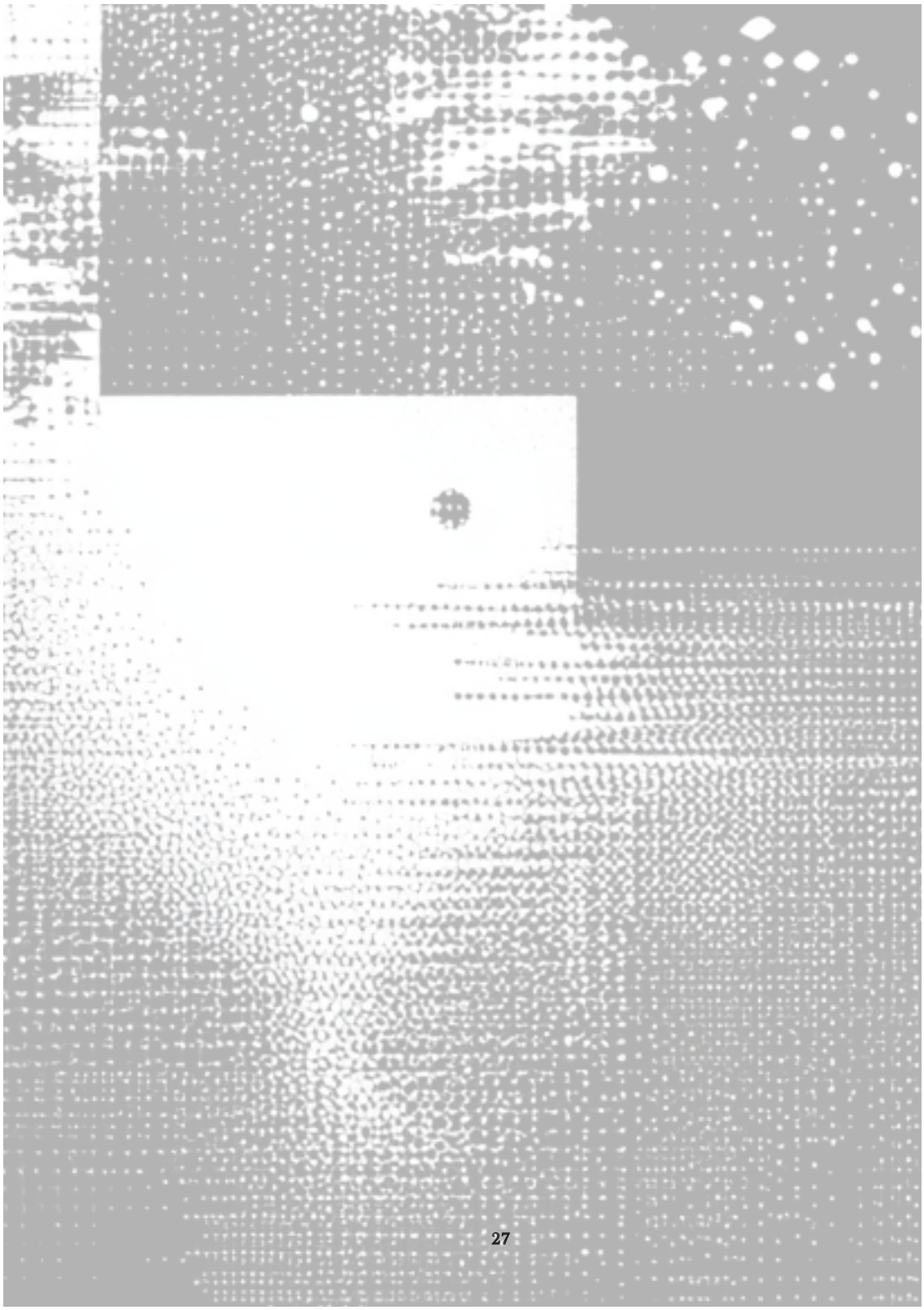
$2B+ shielded in a single week. Railgun TVL: $91.88M (all-time high). For context: this single- week figure exceeds the cumulative all-time volume of most other protocols in this report. Source: CoinMarketCap, May 6, 2026.

Developer infrastructure and ecosystem signals

The Ethereum Foundation's Kohaku SDK reached its first major milestone (ERC-4337 mempool relay for Railgun) on May 25, 2026. Ambire wallet is preparing a Kohaku integration. Tornado Cash and Privacy Pools integrations are in development with a Berlin Blockchain Week demonstration. Kohaku is also scheduled for the Hegotá hard fork in H2 2026.

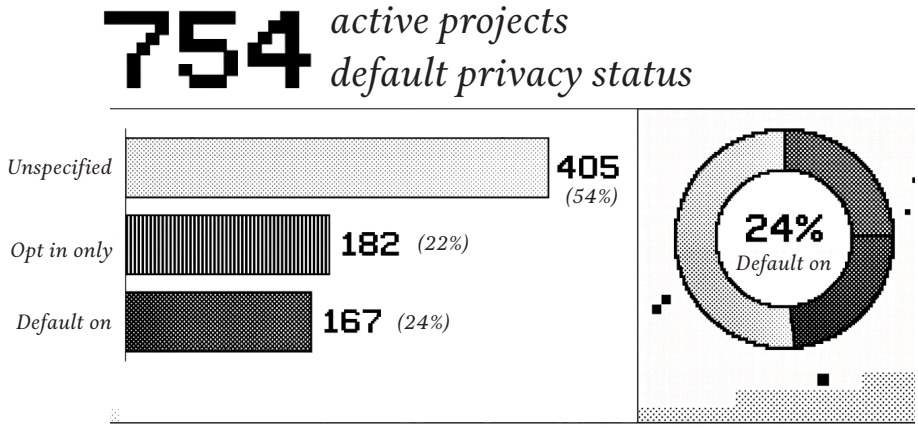
Solana's Confidential Balances was initialized for PayPal's PYUSD: the first major payment network to initialize a privacy-preserving transaction mechanism on a high-throughput public chain. Privacy Cash processed $200M+ since August 2025. Monero provides the baseline: ~23,000 transactions/day, $7–8B market cap, 58% of privacy coin market, mandatory protocol-level privacy with no opt-out. The Web3Privacy Now hackathon dataset (40 events, 5,194 projects) found 417 privacy projects (8%), with ZK at 32.4%.

Source: Railgun: Messari/DL News Oct 2025 · AMLBot Dune May 14 2026 · Railgun Dune June 1 2026 · Kohaku: The Defiant/CryptoBriefing May 25 2026 · CoinMarketCap May 6 2026 · W3PN hackathon dataset 2025 · coinlaw.io (Monero).



Signal 2
PRIVACY IS NOT THE DEFAULT

Of 754 active projects, 182 (24%) have privacy explicitly enabled by default. A further 167 (22%) have it as opt- in. The remaining 405 (54%) do not specify. Absence of data is not neutral: projects that have not recorded a default privacy stance are, in practice, not making privacy the default experience.

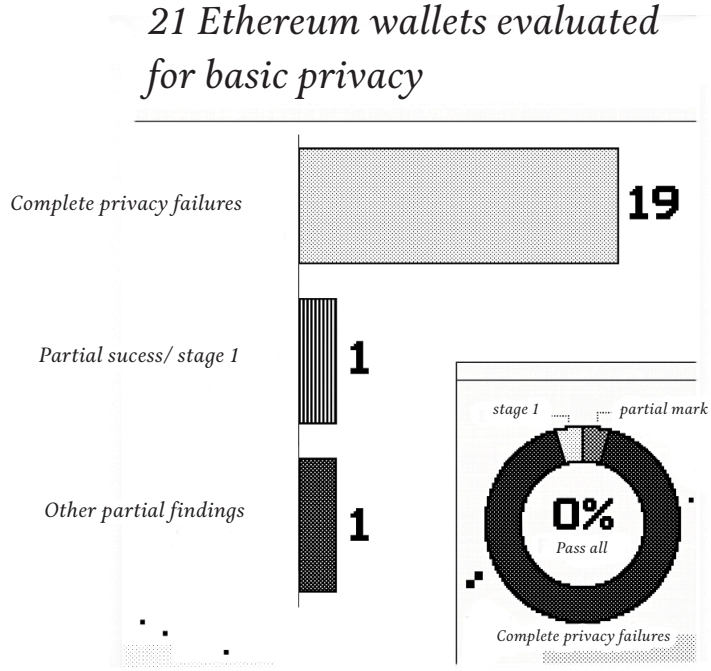


Only 24% of active projects have privacy on by default; 54% do not specify; opacity is itself a privacy failure.
Source: Web3Privacy Now Explorer, May 2026.

Among the 21 Ethereum software wallets evaluated by Walletbeat, zero pass the most basic privacy criterion: private token transfers by default.

The wallets most widely used (MetaMask, Rainbow, Phantom, Rabby, Zerion) all fail.

Daimo implements stealth addresses but leaks sender–receiver correlation, earning a partial rating only. Hardware wallets present a different problem: the Walletbeat framework does not yet define privacy criteria for hardware devices at all.



Zero out of 21 Ethereum wallets pass the private token transfer criterion. Most criteria are 'unknown' not a pass.

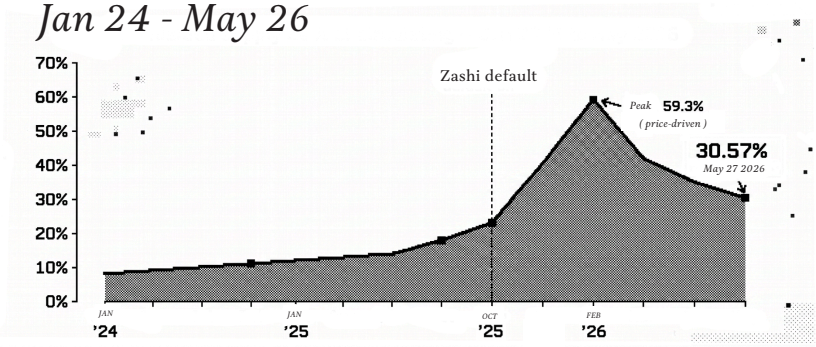
Source: Walletbeat (beta.walletbeat.eth.limo), May 2026.

The Zcash natural experiment

Between early 2024 and May 2026, the proportion of Zcash's circulating supply in shielded addresses grew from ~8% to ~30%; nearly fourfold in two years. The protocol did not change. The Zashi wallet (now Zodl) made shielded the default.

Previous Zcash price rallies showed shielded supply staying flat: speculation without usage. The 2024–2026 shift shows shielded supply growing alongside and sometimes ahead of price: deliberate adoption.

Zcash shielded supply as % of calculating
Jan 24 - May 26



Shielded % rose from 8% (early 2024) to ~30% (May 2026) driven by the Zashi wallet making shielded the default. Feb 2026 peak (59.3%) reflects price appreciation.
Source: zkp.baby May 27 2026; CoinMetrics Nov 2025; cryptonews.net June 2026.

Note: Zcash Orchard pool vulnerability disclosed June 5, 2026

On June 5, 2026 Shielded Labs disclosed a soundness vulnerability in the Orchard ZK circuit, present since Orchard's activation in May 2022. An emergency hard fork (NU6.2) deployed June 3 patched the flaw before public disclosure. No exploit was confirmed; turnstile accounting verified no unauthorized value creation. The bug was found by security engineer Taylor Hornby using an AI-assisted circuit audit specifically commissioned for this purpose.

This is the most vivid possible illustration of this report's audit-gap finding: the flaw existed for four years and required a specially commissioned AI-assisted audit to surface. The structural shielded adoption shift (8%→30%) remains valid and documented by multiple independent sources. But the disclosure is a material reminder that 'no trusted setup' is not the same as 'no vulnerability.'

Source: Explorer DB · Walletbeat May 2026 · zkp.baby May 27 2026 · CoinMetrics Nov 2025 · cryptonews.net June 2026 · CoinDesk June 5 2026 (Orchard bug) · BitMEX blog June 2026.

Signal 3

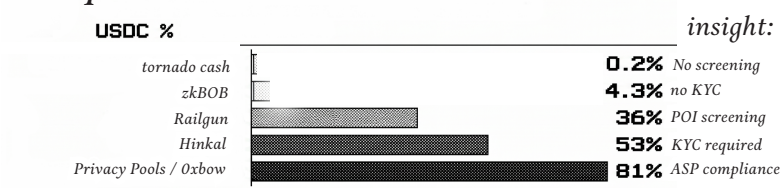
THE INSTITUTIONAL AND INDIVIDUAL TENSION

The most contested question in decentralized privacy in 2025 was not technical. It was political: who is privacy for, and on whose terms? The year produced two kinds of privacy product: one for individuals wanting autonomy without identifying themselves to any authority, and one for institutions needing confidentiality while remaining accountable to regulators. These are not the same thing, even though they are both referred to as "privacy."

What the onchain data shows

AMLBot's Dune dashboard tracks stablecoin composition across six privacy protocols. The stablecoin a user chooses is a revealed compliance preference. DAI cannot be frozen by any issuer. USDC can be frozen by Circle. The pattern across protocols is unambiguous.

The market has already sorted itself into compliance tiers:



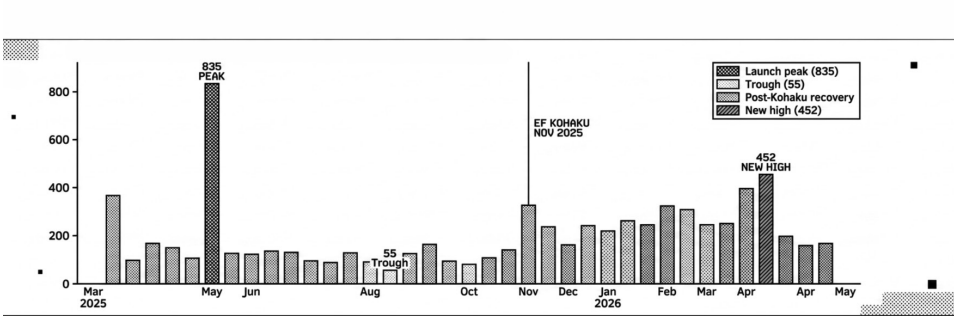
Railgun stablecoin-only (DAI+USDC+USDT), AMLBot Dune screenshot May 14 2026.

Total Railgun all-asset volume: $5B+ cumulative (Castle Labs / DeFi Llama, June 8 2026). USDC % rises directly with compliance stringency.

0xbow trajectory

Privacy Pools' weekly transaction count shows the adoption pattern of a new compliance-oriented protocol: 835- transaction peak (May 2025), 55-transaction trough (August 2025), and recovery to a new high of 452 (April 2026); aligned with the EF Kohaku integration as credibility catalyst.

Oxbox privacy pools weekly transactions, across chains
(Mar 2025 - May 2026)



Institutional developments in 2025

The Ethereum Foundation's Kohaku initiative deliberately embeds both compliance-compatible tools (0xbow) and anonymity-preserving tools (Railgun) in the same SDK. Wallet developers choose which to expose. This is a policy position expressed as architecture: the EF is not endorsing a single privacy model.

In December 2025, Circle launched USDCx on the Aleo blockchain; privacy-preserving USDC with transaction details hidden but a compliance record retained for law enforcement. This is "banking-level privacy": the confidentiality standard of SWIFT, not the anonymity standard of Monero. Both are legitimate responses to real demand. They are not compatible visions of what decentralised privacy should be.

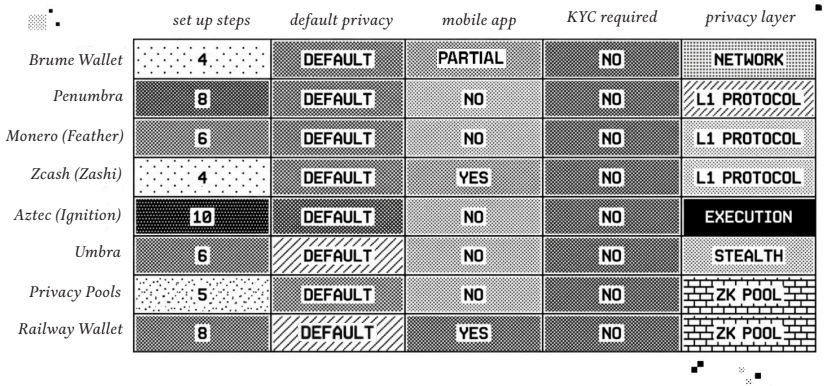
Source: AMLBot Dune screenshots May 14 2026 · 0xbow Dune screenshot June 6 2026 · GlobeNewswire Nov 18 2025 · The Defiant May 25 2026 · Fortune/The Block Dec 9 2025.

Signal 4

UX IS THE BOTTLENECK

The Zcash experiment establishes the principle: when privacy is the path of least resistance, people take it. The Web3Privacy Now desk audit of eight tools provides the specific evidence. Mean setup steps: 6.6 (range: 4-10). Six of eight tools have privacy on by default. None requires KYC. All provide an exit path.

UX desk audit *(8 privacy tools x 5 dimensions)*



Setup steps, default privacy, mobile availability, KYC, and privacy layer across 8 audited tools. Mobile is the most consistently absent feature. **Extended report is coming July-August 2026.**

Source: Web3Privacy Now desk audit, May 2026.

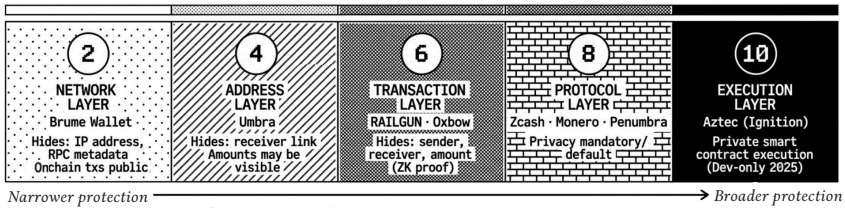
Mobile is the structural gap

Only two of the eight tools (Railway Wallet) and Zcash (Zashi/Zodl) have full mobile applications. Five tools are desktop or browser-extension only. Aztec Ignition has no consumer interface: it is a developer product. For people in high-risk environments where mobile is the only device available, this is not a minor inconvenience. It is a structural exclusion.

The privacy layer matters

Brume Wallet routes all network requests through Tor by default, protecting IP address and preventing metadata correlation. This does not make onchain transactions private. Brume is network-layer privacy. Railgun and 0xbow are transaction-layer. Monero and Zcash are protocol-layer. Aztec is execution-layer. These are complementary, not interchangeable. A user who installs Brume believing they have achieved financial privacy has not.

Privacy tools protect different layers of the stack



Source: W3PN UX desk audit, May 2026 (original brief research). Live device testing with broader selection is scheduled for v2 full report. Walletbeat May 2026.

The on-ramp surveillance before privacy begins

Onchain privacy tools address what happens inside the blockchain. They do not address how users arrive there. The dominant on-ramps (centralized exchanges) require government-issued identity verification before a user can acquire the digital assets they would use in a privacy tool. This creates a surveillance choke point upstream of every ZK proof: the user's identity, transaction history, and counterparty are logged before their first shielded transaction. Peer-to-peer on-ramp protocols, such as ZKP2P, attempt to address this by enabling fiat-to-crypto exchange without a centralized intermediary; a nascent but structurally important development. For the populations this report is most concerned about, the on-ramp is currently the weakest link.

Offchain correlation and the third-party cookie problem

Onchain privacy does not protect against offchain surveillance. When a wallet shares a user's public address with a website to build a transaction (standard practice across the ecosystem) that address can be logged by the site's analytics infrastructure, combined with browser fingerprinting data, and used to track the user across every site they visit. The mechanism is structurally identical to the third-party cookie that web privacy advocates spent twenty years fighting. A user can execute a perfectly shielded on-chain transaction while their wallet address is being recorded in a Google Analytics dashboard. Onchain ZK proofs and offchain address correlation protect entirely different threat models. The ecosystem has invested heavily in the former and almost nothing in the latter.

Why wallets default to "off"

The structural reason privacy features are off by default in most wallets is not technical. It is economic. Wallet providers earn revenue through fee-sharing on swaps, bridges, and perpetual trading; integrations where the protocol pays the wallet a percentage of each transaction. Privacy protocols do not have equivalent revenue- sharing models. There is no privacy fee flowing back to the wallet provider. A wallet that enables private transfers by default earns nothing from doing so; a wallet that routes a swap earns basis points on every transaction. The rational outcome is to make revenue-generating features the prominent defaults and treat privacy as an opt-in feature.

> *Privacy ends up as a privilege rather than a default capability of the network. That is not a technical failure. It is an economic design choice with a technical consequence, and it will not be resolved by cryptography alone.*

Signal 5

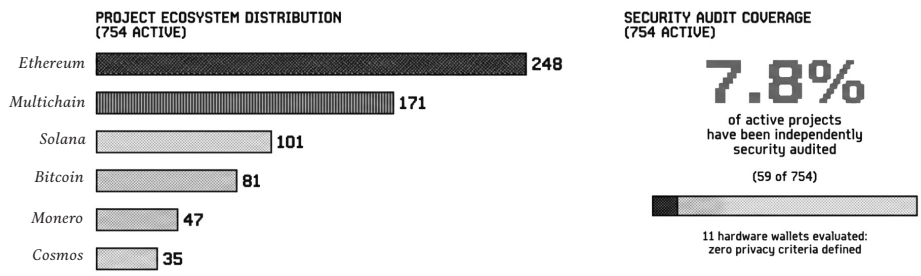
FRAGMENTATION AND THE STANDARDS GAP

The decentralized privacy ecosystem is not one ecosystem. It is several, with limited interoperability and no shared standards governing how privacy properties are defined, communicated, or measured.

Ecosystem silos

Of 754 active projects: 248 on Ethereum, 101 on Solana, 81 on Bitcoin, 47 on Monero, 35 in Cosmos. Only 171 explicitly support multiple chains. Phala Network's migration in November 2025 (from a Polkadot parachain to an Ethereum Layer 2) illustrates the gravitational pull of the dominant ecosystem and the difficulty of sustaining privacy infrastructure on smaller chains.

Fragmentation *(siloed by chains, unmeasured by standards)*



Ethereum hosts 33% of projects; only 23% are explicitly multichain. 7.8% of active projects have been independently audited.

Source: Web3Privacy Now Explorer · Walletbeat, May 2026.

The encryption label problem

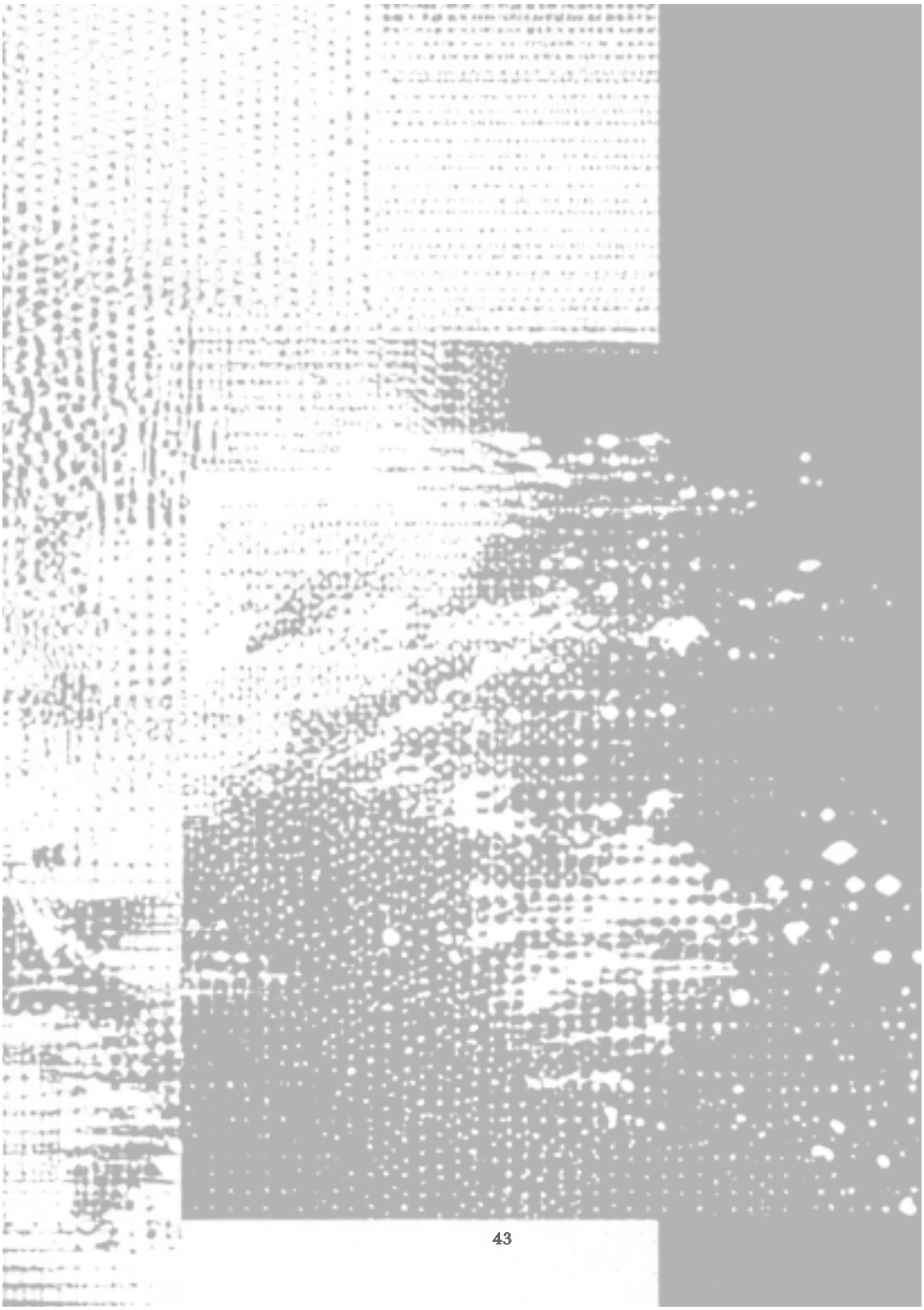
The 'encryption' field in the Explorer database contains over 100 distinct values. Some are precise technical terms. Some are product names. Some describe physical properties. The absence of a shared taxonomy means researchers, regulators, and users have no common language for comparing the privacy guarantees of different tools.

The audit gap, and what the Zcash disclosure tells us

59 of 754 active projects (7.8%) have undergone an independent security audit. On June 5, 2026, Shielded Labs disclosed a soundness vulnerability in Zcash's Orchard ZK circuit that had existed, undetected, since May 2022. The bug was found by a security engineer using an AI-assisted audit specifically commissioned for this purpose. No exploit occurred. But the flaw had been live for four years in one of the most scrutinized cryptographic systems in this ecosystem.

If a four-year soundness flaw can persist in Orchard, the implications for the 92.2% of active privacy projects with no published security audit are significant. Across 11 hardware wallets evaluated by Walletbeat, no privacy criteria exist in the evaluation framework. The Ledger data breach of January 2026 is a reminder that privacy failures in the hardware ecosystem often do not originate in the cryptography.

Source: W3PN Explorer · Walletbeat hardware evaluation May 2026 · Phala Network Nov 2025 · CoinDesk/Shielded Labs June 5 2026 · BitMEX blog June 2026 · Ledger breach reporting Jan 2026.



Looking ahead

FIVE SIGNALS TO WATCH IN 2026

This report is a snapshot, not a forecast. The five signals below are observations about live processes; things underway at the time of writing and developing further as you read this. They are offered as starting points for today's discussions.

1. Will Kohaku reach wallets?

The Kohaku SDK reached its first major milestone on May 25, 2026. Ambire wallet is preparing integration. A browser extension wallet is in development. Tornado Cash and Privacy Pools integrations are being demonstrated this week at Berlin Blockchain Week. Kohaku is scheduled for the Hegotá hard fork in H2 2026 alongside EIP-8250. The question is not whether the SDK works. It is whether users encounter privacy options as a default or as a buried menu item.

2. When does Aztec become usable?

Aztec Ignition launched November 2025 as a developer network; ZK L2 with private smart contract execution by default, including from the sequencer. Block time: 72 seconds at launch (targeting 3-4 seconds end of 2026). No consumer wallet. Alpha network does not migrate state between releases. The gap between technical ambitions and current usability is the largest of any project in this report.

3. Is FHE research or infrastructure?

Fhenix reported 25% month-on-month activity growth in March 2026. Zama released a Confidential Token Standard with OpenZeppelin. FHE proving overhead has fallen from ~1M× slower to ~100-1,000× slower. The next two years will determine whether FHE crosses from experimental to deployable.

4. Is the ecosystem preparing for post-quantum?

Vitalik Buterin estimated a 20% probability of quantum computers capable of breaking elliptic curve cryptography before 2030. Zcash's NU7 includes a post-quantum roadmap. One of 417 hackathon privacy projects addressed post-quantum. The Orchard circuit disclosure of June 5, is a reminder that vulnerabilities in complex cryptographic systems can persist for years; post-quantum readiness deserves the same scrutiny.

5. Is Solana, becoming a go-to institutional-first privacy network?

Solana's Confidential Balances, using ElGamal encryption, was initialized for PayPal's PYUSD in 2025; the first major payment network on a performant public chain with privacy-preserving transactions. Solana's approach is explicitly compliance-first. Whether it becomes the model for institutional payment privacy, or is superseded by more privacy-preserving alternatives, is one of the more consequential open questions in this space.

> The infrastructure exists. The standards do not. The defaults are wrong. These are solvable problems; if the people building the tools, the people writing the standards, and the people who need the protection are in the same room.

A full version of this report; with extended case studies, live UX testing results, refined methodology, and additional datasets; is planned for July-August 2026.

If you have data, case studies, or findings to contribute, contact Web3Privacy Now at https://web3privacy.info.

Summit: s26ber.web3privacy.info · Explorer: explorer.web3privacy.info · Research: github.com/web3privacy/research

Methodology

DATA SOURCES AND LIMITATIONS

This research was conducted between April and June 2026. All data was collected from public sources. No private datasets, paid subscriptions, or embargoed information were used.

The report distinguishes between observation and interpretation. Findings are stated as findings; claims are sourced; limitations are acknowledged. Full and extended report is coming July-August 2026.

Selected secondary sources

DL News/Messari Oct 2025 (Railgun) · The Defiant/CryptoBriefing May 25 2026 (Kohaku SDK) · CoinMetrics Substack Issue 338, Nov 18 2025 (Zcash) · cryptonews.net/crypto.news June 2026 (Zcash shielded 30%) · CoinDesk June 5 2026 (Orchard bug) · Shielded Labs/BitMEX blog June 2026 (Orchard disclosure) · Fortune/The Block Dec 9 2025 (Circle USDCx) · GlobeNewswire Nov 18 2025 (0xbow) · Metaverse Post Apr 24 2026 (AMLBot analysis) · CoinMarketCap May 6 2026 (Railgun ATH) · Castle Labs / DeFi Llama.

Limitations

UX audit is a desk audit. Some dimensions (e.g.: time-to-first-transaction, proof generation time, error count) require live device testing. Explicitly omitted from current analysis; scheduled for v2 full report.

Explorer database self-reported fields (default_privacy, kyc, audits) may be incomplete. 54% of projects do not specify default_privacy; reported as 'unspecified,' not inferred as opt-in.

Post-collection development: on June 5, 2026, Shielded Labs disclosed a soundness vulnerability in Zcash's Orchard ZK circuit (present since 2022, patched June 3 via NU6.2 hard fork, no exploit confirmed). ZEC price and shielded USD value figures reflect May 27, 2026; shielded ZEC count (~5M ZEC, ~30% of supply) is materially unchanged as of report date.

This report covers Ethereum, Zcash, Monero, Solana, Cosmos, and Polkadot. Enterprise permissioned blockchains (Canton Network, Hyperledger Fabric) are outside scope.

Primary data sources

SOURCE	URL	COVERS	DATE
W3PN Explorer DB	*explorer-data.web3privacy.info*	826 projects — categories, usecases, ecosystem, default_privacy, kyc, audits, sunset	May 2026
W3PN Hackathon dataset	*github.com/web3privacy/research*	40 events, 5,194 projects, 417 privacy submissions, 2025 only	2025
Walletbeat	*beta.walletbeat.eth.limo*	21 software + 11 hardware wallets, privacy criteria	May 2026
W3PN UX desk audit	*Original primary research*	8 tools, D1–D10 criteria (D2/D3/D4 require live testing)	May 2026
AMLBot Dune	*dune.com/amlbot/stablecoin-turnover-in-privacy-tools*	$4.2B stablecoin by protocol, DAI/USDC/USDT split	May 14 2026
RAILGUN Dune	*dune.com/railgun_project/railgun*	Monthly flows, fee line	June 1 2026
0xbow Dune	*dune.com/0xbow_io/privacy-pools-v1*	Weekly transaction count	June 6 2026
Zcash live explorer	*zkp.baby*	Shielded pool %, pool breakdown, total supply	May 27 2026

About Web3Privacy Now

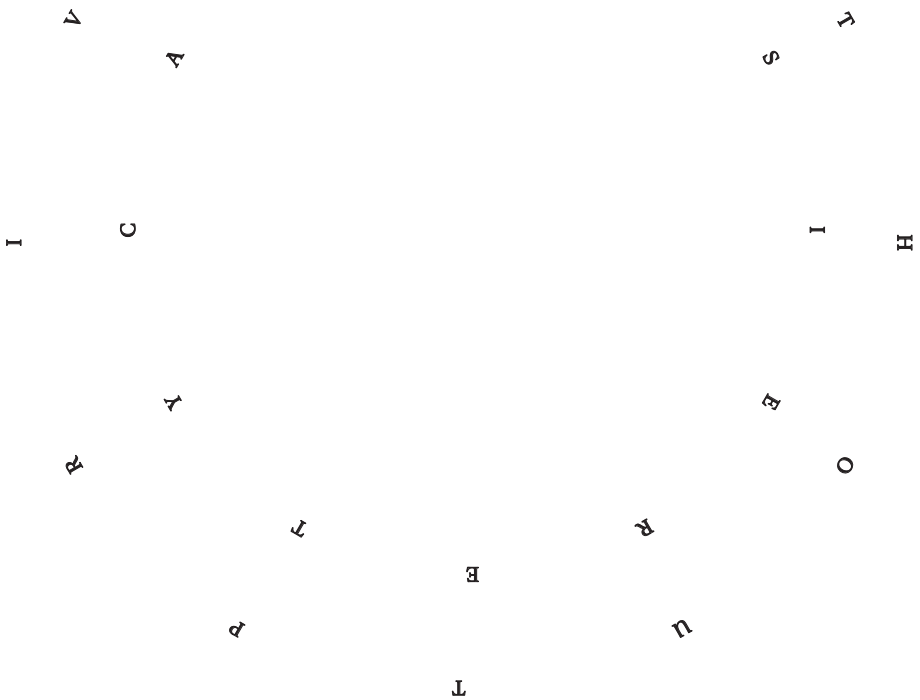
Web3Privacy Now is an independent research and advocacy organization focused on privacy in the Web3 ecosystem.

This report is an independent research initiative and does not represent the views of any protocol, foundation, or investor.

State of Decentralized Privacy 2026 ·
Neocypherpunk Summit Edition ·
Funkhaus Berlin · June 14, 2026 ·

Web3Privacy Now

https://web3privacy.info
https://s26ber.web3privacy.info
https://explorer.web3privacy.info
https://github.com/web3privacy/research



D

E

M

O

C

R

A

C

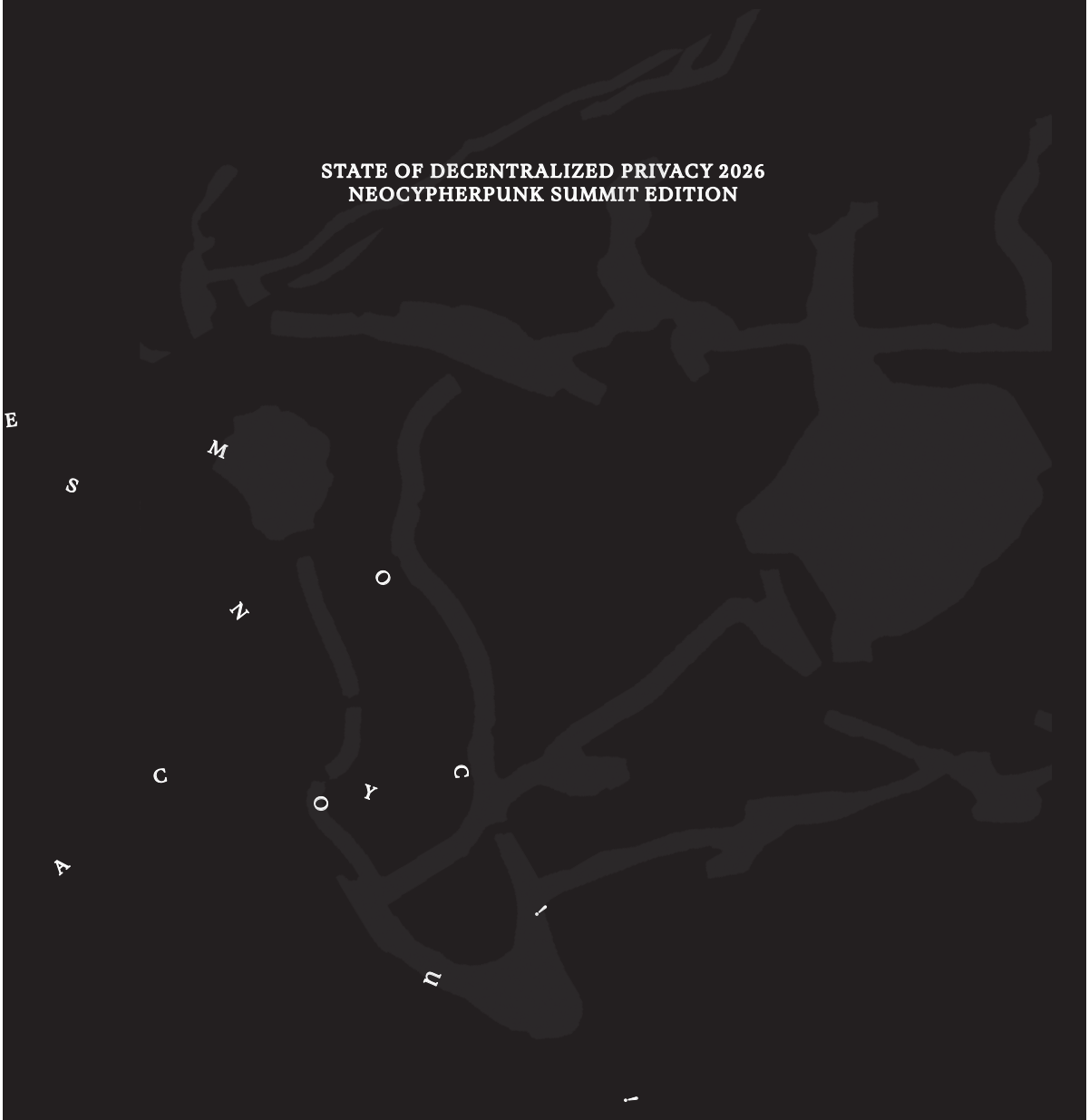
A

I

"Privacy is the power to selectively reveal oneself to the world"
— Eric Hughes, 1993

State of Decentralized Privacy 2025 ·
Neocypherpunk Summit #1 · Funkhaus Berlin · June 14, 2026 ·

STATE OF DECENTRALIZED PRIVACY 2026
NEOCYPHERPUNK SUMMIT EDITION



web3privacy now