



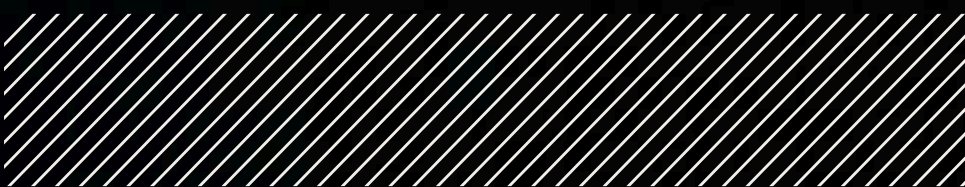
ZAMA

A look into Confidential DeFi

RESEARCH REPORT 2026

Table of Contents

Executive Summary	3
Why Now?	4
The Establishment of Confidential DeFi — A New Category	9
Technology Deep Dive: Inside the Zama Protocol	15
Ecosystem & Use Cases	20
Metrics: Tracking the Category	27
Risks & Open Questions	31
Outlook & Conclusion	35
Appendix	38



Executive summary

- Public blockchains make institutional balance sheets and positions fully visible — capping capital efficiency and blocking use cases like payroll and treasury management that need confidentiality by default, not just protection from front-running.
- Confidential DeFi (excluding mixers) is up 170% over 18 months to \$197.6M, with protocol count up 117% (18→39) — currently at an all-time high in both TVL and breadth simultaneously
- The opportunity dwarfs the current footprint: \$197.6M in category TVL vs. \$96.2B in DeFi TVL, \$310.4B in stablecoins, and \$350.0B in tokenized RWAs — with a single partner commitment (Apex Group's \$100B T-REX pipeline) now approaching total DeFi TVL today
- ERC-7984, co-developed by Zama and OpenZeppelin, is the category's standardization moment — backed by the three-org Confidential Token Association and real distribution (OpenZeppelin, Dfns, Blockscout) — though adoption remains concentrated in Zama's own ecosystem.
- FHE is the fastest-growing approach: Zama hit \$100M shielded in 25 days after mainnet launch (vs. 860–1,580 days for peers), and FHE's share of category TVL has risen monotonically from 23.1% to 41.7% as of Sept 18, 2026, entirely at ZK's expense.
- September 2026 marked a step-change in ecosystem depth: a single vault became a 16-vault suite across 5 curators, alongside a new Confidential Swap Protocol, live RWA/OTC/payroll/custody deployments, and a four-partner compliance stack (OpenZeppelin, Blockscout, Elliptic, Hypernative).
- DefiLlama's independent tracking (\$82.7M TVL, +39.0% 30d) and Zama's own live dashboard (\$81.8M Shielded TVL, \$982.8M cumulative volume) point the same direction.
- Key risks: cross-approach fragmentation, standardization concentrated in one ecosystem, unresolved regulatory treatment, and concentration in a single vault venue (Morpho) and chain (Ethereum).
- Watch for: a second major curator ecosystem beyond Morpho, a non-Zama project adopting ERC-7984, and first-quarter usage data for the Swap Protocol — the three triggers for mainstream adoption.





ZAMA

Why Now?

RESEARCH REPORT 2026

Why Now?

Institutional Capital's Transparency Problem

On a public blockchain, everything is visible. Every wallet balance, every position, every trade can be tracked in real time — and pending trades can be seen in the mempool before they even settle. For an institution, this means its balance sheet and its trading positions are legible to anyone watching the chain, not just to counterparties it has chosen to disclose to.

That legibility is the actual constraint, and it goes well beyond protecting a single trade from front-running. It caps capital efficiency, because institutions must either avoid onchain venues for size-sensitive activity or accept the strategy and cost of doing so being visible to competitors. And it rules out entire categories of use cases that require confidentiality by default rather than as an afterthought — payroll, where salary amounts can't be public; commercial contract payments, where deal terms are commercially sensitive; treasury management, where rebalancing activity signals strategy to the market before it completes. None of these are addressable by hiding how a transaction reaches the chain — they require the balance and the transaction amount itself to be confidential.

The narrower version of this problem — that visible positions and pending trades can be directly exploited — has already been measured: A 2025 study of Ethereum sandwich attacks ("Sandwiched and Silent," Mancino & Rezzoli) analysed transaction data from November 2024 to February 2025, and found that the industry's go-to fix, private transaction routing, does not work as well as people assume.

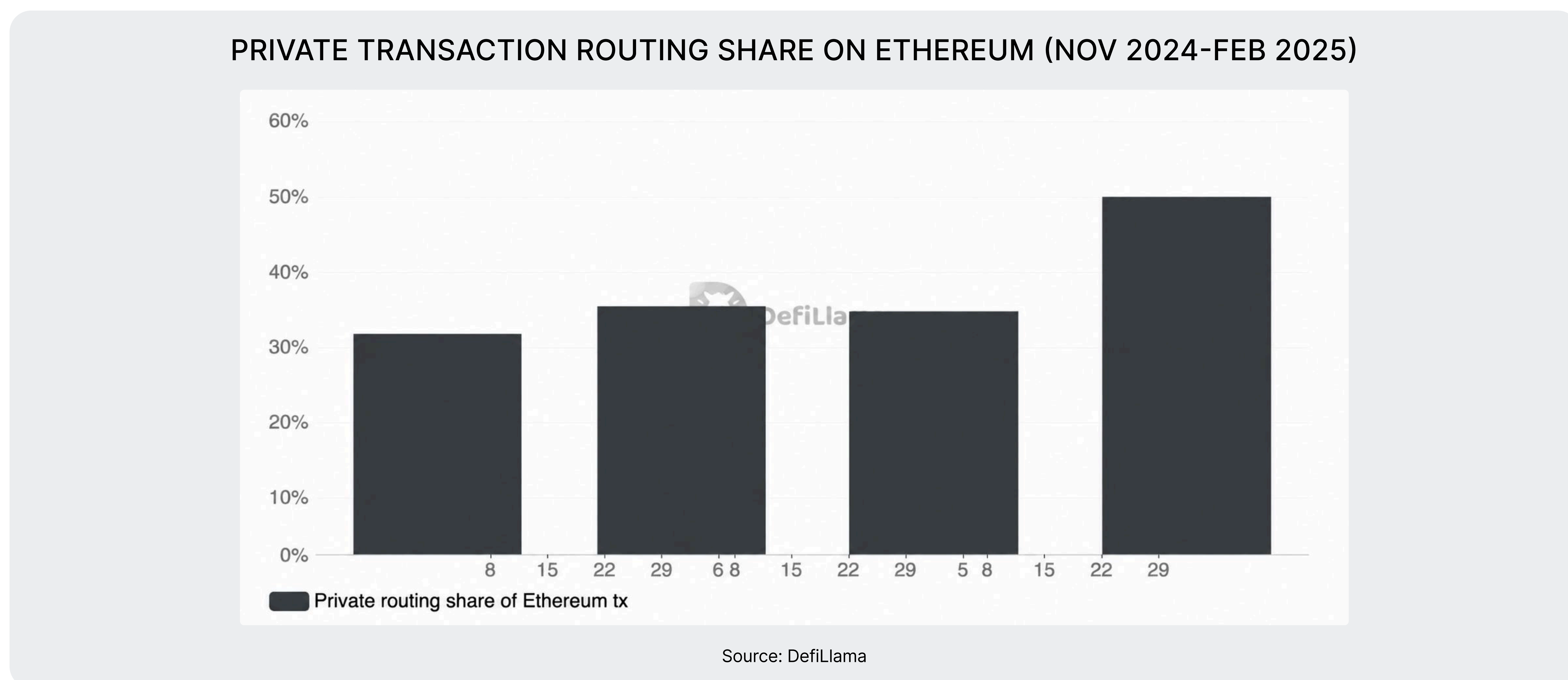
In November and December 2024 alone, the "Sandwiched and Silent" study recorded:

- 2,932 sandwich attacks through private channels, hitting 3,126 transactions
- \$409,237 lost by victims
- \$293,786 earned by attackers

One bot was behind about 65% of these attacks; So the "private" route institutions are moving to is not truly private - It is a concentrated venue that a few players can still exploit.

Despite this, adoption keeps growing - private routing went from 31.8% of all Ethereum transactions in November 2024 to 50.1% by February 2025, and passed the halfway mark in just four months.

Demand for privacy is clearly here — not only because current defenses against exploitation are weak, but because capital efficiency and entirely new onchain use cases depend on solving the deeper legibility problem, and the current tools don't deliver it.



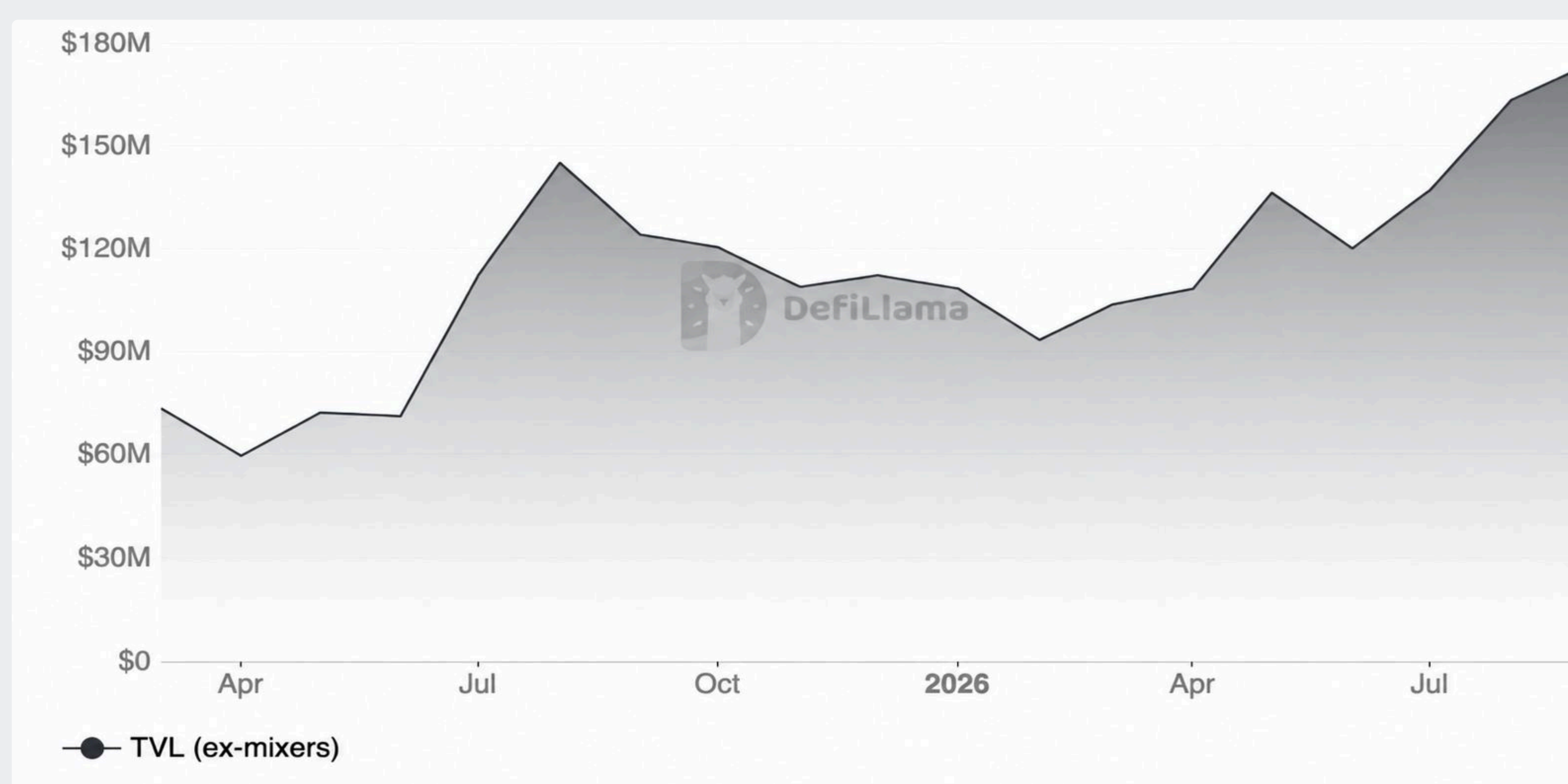
This is the real "why now." Institutions are already switching to private routing - showcasing demand for it; Yet, routing only hides the path to a trade. It can't make the trade itself confidential.

What does make the trade itself confidential is building privacy into the settlement layer, into the point where trades are finalised onchain. Now, instead of hiding how a transaction gets there, you encrypt the balance itself - and the market is slowly moving this way.

Excluding mixers, which are built for anonymity, DefiLlama's privacy category has grown from \$73.3M in March 2025 to \$197.6M today. That is a rise of about 170% in 18 months.

However, this growth has been lumpy - the category fell 18.7% month-on-month in April 2025, then jumped 58.3% that July. As of September 2026, it has grown for three months in a row and is at its highest level in 18 months.

CONFIDENTIAL DEFI CATEGORY TVL, EXCLUDING MIXERS (18-MONTH TREND)



Source: DefiLlama

Market Opportunity

The appetite is clearly there, yet today, confidential DeFi's footprint is tiny. But therein lies the opportunity.

The category's \$197.6M in tracked TVL (excluding mixers) is a rounding error against the broader markets it's positioned to serve. It's just 0.21% of total DeFi TVL (\$96.2B), 0.06% of total stablecoin supply (\$310.4B), and 0.06% of the \$350.0B already tokenized onchain as real-world assets — three separate pools of capital, all live today, that confidential rails could eventually touch.

The forward-looking numbers are what make the gap interesting rather than discouraging. Apex Group, which services \$3.2 trillion in assets globally, has committed to placing \$100 billion in tokenized assets on the T-REX Ledger by June 2027 with Zama as its confidentiality layer — a single partner commitment now approaching total current DeFi TVL, and equal to 28.6% of all RWA value currently tokenized onchain. McKinsey's 2030 forecast puts the total addressable RWA market at \$4T — nearly 11.4x today's entire tokenized-RWA market.

Early production data points the same way. Zama's first confidential vault, the Steakhouse Confidential Prime USDC vault on Morpho, reached roughly \$40M in TVL within seven weeks of its June 2026 launch. In September 2026 it was expanded into a 16-vault suite across five institutional curators (Steakhouse Financial, Armitage by Wintermute, Flowdesk, RockawayX and Bitwise).

T-REX enables confidential RWA issuance & trading

T-REX is the leading RWA protocol and permissioned token standard, with over \$32B tokenized, 20K users, and over 200 token issuers, service providers, and applications in its ecosystem. T-REX chose Zama to be its confidentiality protocol for its upcoming canonical chain.

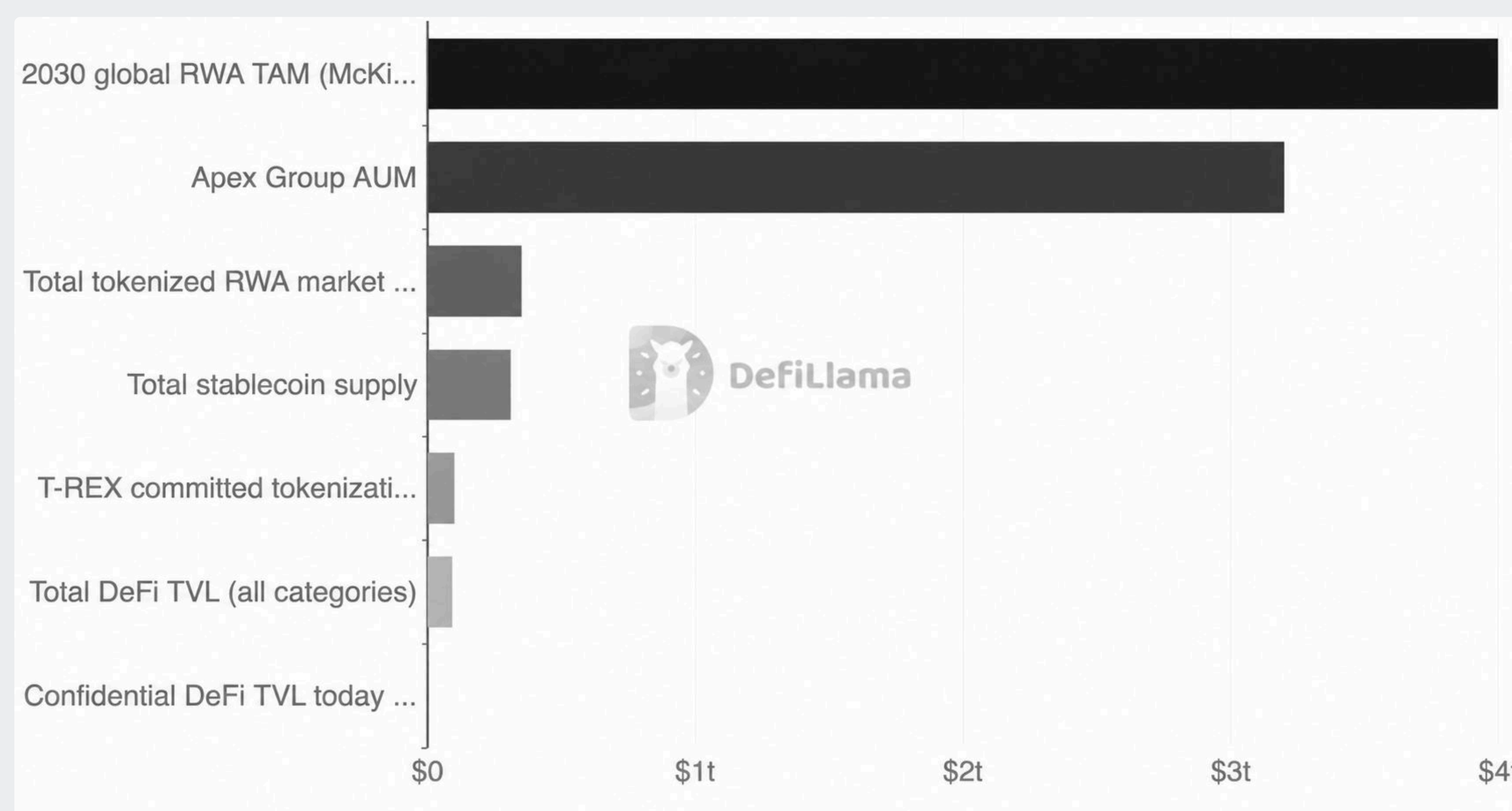
T-REX is backed by APEX Group – a global asset manager with over \$3.2T in assets under management – which already committed to tokenize \$100B in assets by June 2027, which is four times the size of the current Ethereum RWA market. Shielding only 2% of this TVL would be enough to make Zama the largest privacy protocol by TVS, ahead of Zcash.



Committed TVL	2030 RWA TAM *	APEX AUM
\$100B	\$4T	\$3.2T

*McKinsey RWA market forecast

CONFIDENTIAL DEFI'S ADDRESSABLE MARKET: TODAY VS. THE INSTITUTIONAL OPPORTUNITY



Source: DefiLlama

Even a small fraction of that pipeline actually shielded would dwarf the category's current size: Zama's report notes that shielding just 2% of T-REX's committed TVL would make it the largest privacy protocol by value shielded, ahead of Zcash. The gap between the leftmost and rightmost bars above is the thesis: confidential DeFi isn't competing for today's onchain TVL — it's the precondition for institutional AUM, measured in trillions, to touch public chains at all. There is room for different privacy protocols. For example, Zcash can be perceived as a great protocol for encrypted store of value, but for onchain finance to go private, it requires new privacy primitives, like compliance and composability. That's what unlocks Confidential DeFi at scale.



ZAMA

The Establishment of Confidential DeFi — A New Category

RESEARCH REPORT 2026

The Establishment of Confidential DeFi — A New Category

3a. Origins: Five Approaches, One Convergent Problem

Confidential DeFi didn't arrive as a single invention — it's the convergence of five separate cryptographic lineages, each solving "hide the data, keep it verifiable" in a different way, and each with their own solution for it.

ZK (Zero-Knowledge) Proofs

ZK Proofs got here first and remains the category's largest bucket by TVL. ZK Proofs lets you prove something is true without revealing the underlying data — for example, proving you have enough funds without showing your balance.

Zcash pioneered ZK-shielded transactions at the protocol level; the approach later powered general-purpose mixers and, more recently, compliance-oriented shielded pools (Railgun, Privacy Pools). Zcash itself now carries a \$24.6B market cap — evidence the underlying cryptography has real staying power, even though it took Zcash roughly 1,580 days to reach \$100M in shielded value, against Railgun's 1,185 days. Not every ZK experiment survives: Aztec Connect, once a leading ZK-rollup-based confidential DeFi implementation, now sits at \$0 TVL, down 100% year-over-year — a reminder that ZK Proofs are just an approach, not a guarantee of product durability.

TEE (Trusted Execution Environments)

TEE takes a hardware route: computation runs inside a sealed chip that even the machine's operator can't see into. Oasis Sapphire is the clearest live example, but its \$179.2K in TVL is down 96.0% year-over-year, and Secret Network's chain TVL (\$890.9K, down 86.2% YoY) tells a similar story. They have not had much success for adoption, and while TEEs are still used by institutions for custody and off-chain compute, neither has turned into lasting onchain confidential-DeFi TVL.

MPC (Multi-Party Computation)

MPCs never built a base-settlement layer at all in this category — it shows up instead inside custody and wallet infrastructure (Bron combines MPC with native confidential-token support). Hence, there's no MPC-based protocol carrying its own DeFi TVL in DefiLlama's privacy category today.

Private chains

Choosing private chains for institutional DeFi protects sensitive financial data through strict access perimeters, but it forces institutions to sacrifice global liquidity and composability by trapping assets in isolated "walled gardens." While these permissioned networks offer turnkey compliance and absolute control over data residency, they introduce centralized infrastructure risks due to a small validator base and create long-term technological debt by severing ties with the rapid innovation occurring on public networks. Ultimately, institutions trade the core economic benefits of public DeFi - massive network effects, interoperability, and continuous uptime - for a controlled, highly restricted environment that mirrors legacy financial silos.

FHE (Fully Homomorphic Encryption)

FHE is the newest entrant and the fastest-growing: Zama reached \$100M in shielded value in just 25 days after the mainnet launch — against 860 days for Monero, 1,185 for Railgun, and 1,580 for Zcash. Zama's growth has been incredible - with over \$120M in USDT shielded within three days after the auction's opening, it makes Zama the fastest privacy protocol to cross the \$100M Shielded TVL mark.

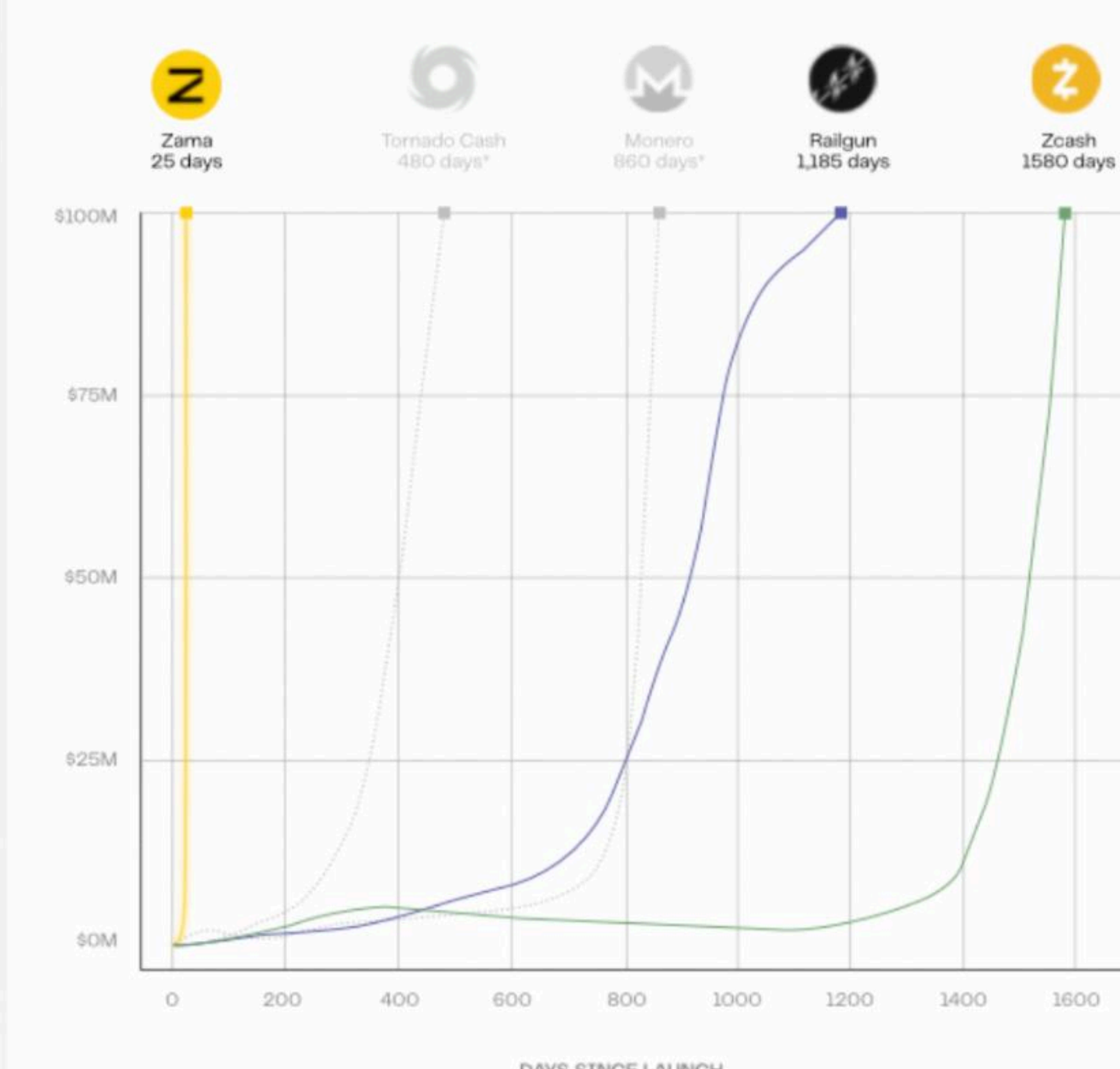
FHE enables computation on encrypted data, so encrypted state can be shared across contracts, which makes it composable and compatible with existing public blockchains and DeFi infrastructure.

Zama is the fastest privacy protocol to reach \$100m TVS

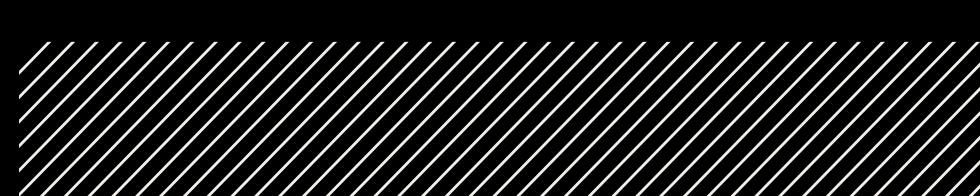
During the ZAMA public sale — the first application deployed on the protocol — over \$120M in USDT was shielded within three days, making Zama the fastest privacy protocol to cross the \$100M TVS mark.

Total Value Shielded (TVS) – a metric that represents the dollar value of onchain assets shielded (encrypted) using the Zama Protocol. TVS is equivalent to TVL for public chains. It measures network health, adoption, liquidity, and trust.

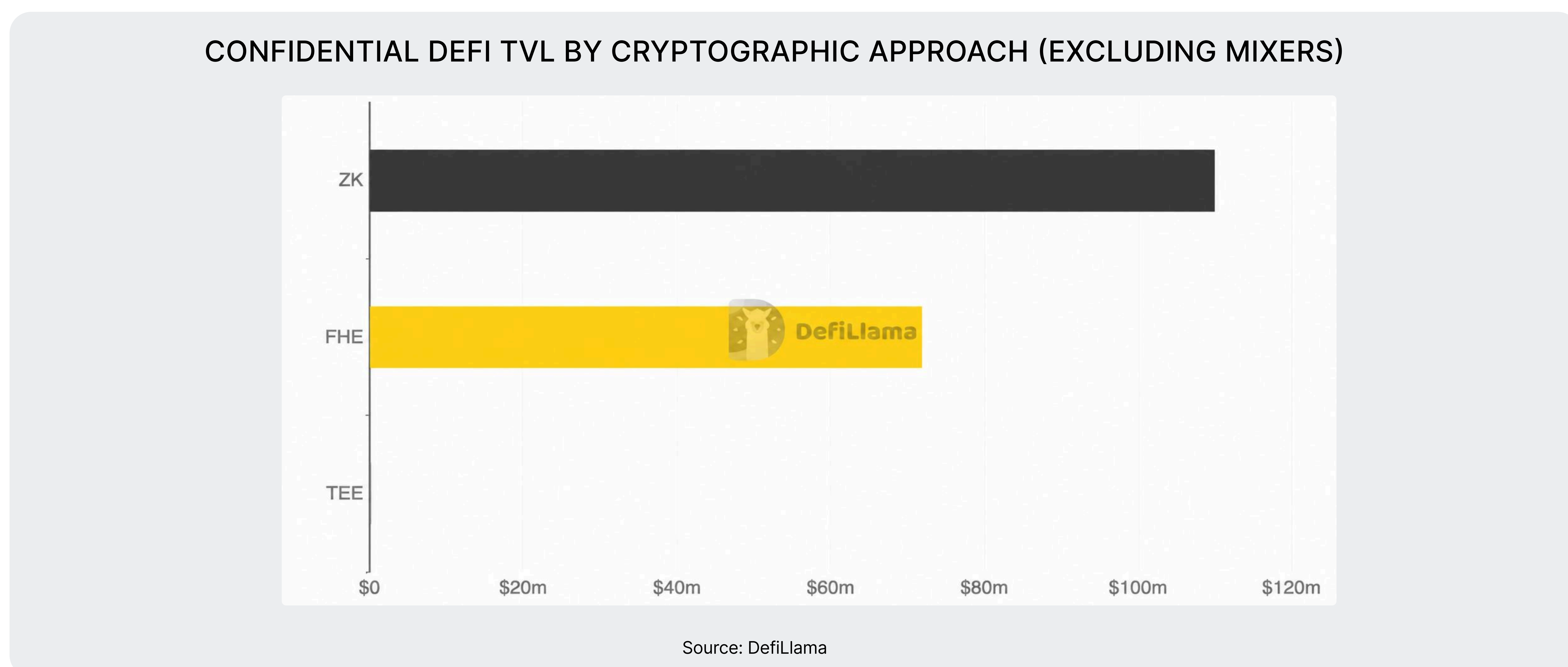
TVS serves as a growth proxy for the emerging ecosystem of confidential onchain finance. The larger the pool of shielded assets, the more attractive it becomes for financial services to target. Zama is one of only 5 protocols to cross \$100M TVS.



Notes:
* Tornado Cash and Monero are excluded from most institutional frameworks due to regulatory status.
** If a privacy protocol is not shown here, it means it never reached \$100m TVS.



Today, on DefiLlama's live tracking, the balance of TVL among the surviving approaches looks like this (excluding mixers):



ZK-based protocols carry \$115.5M across Railgun and the long tail of shielded pools/mixers; Zama's FHE deployment alone carries \$83.1M — a single FHE protocol, two years younger than the ZK cohort as a category, already holds 41.7% of all excluding mixers confidential-DeFi TVL against a ZK field with a decade's head start.

3b. The Standardization Moment (Merged with Standards & Distribution)

This part is about who set the rules everyone now builds on. ERC-7984, the confidential token standard, was developed jointly by Zama and OpenZeppelin — defining how confidential tokens are wrapped, unwrapped, and transferred on public blockchains, and remaining compatible with existing ERC-20 infrastructure so confidential assets can be shielded and unshielded back and forth on the same chain.

This is the category's genuine "constitutional" moment: rather than each approach building incompatible token formats, the standard gives FHE-based confidential tokens (and, per its design, other approaches building on the same interface) a common wrapper. The standard now sits at the center of the Confidential Token Association (CTA) — an industry group whose stated mission is "a common framework for encryption-based onchain confidentiality," co-founded by three organizations: Zama, OpenZeppelin, and Inco.

That three-party founding is the establishment event itself — a standard is a proposal until a second and third organization commit to it, and the CTA is exactly that commitment being formalized. Adoption evidence beyond the standard's authorship:

- The standard is already integrated into OpenZeppelin's Contracts library — the most widely used smart-contract toolkit in Ethereum development. This is the single highest-leverage distribution point in the ecosystem: any developer starting a new confidential-token project inherits ERC-7984 support by default.
- Dfns, enterprise wallet infrastructure, integrated the confidential token standard natively in Q2 2026.
- The Zama SDK — a TypeScript & React toolkit — has over 10,000 weekly downloads and is trending up, described by Zama as "by far the easiest way to integrate confidential financial primitives into your front end applications". This is the practical, day-to-day evidence that ERC-7984 isn't just a paper standard.
- Distribution beyond Zama's own app: Zerion, Utila, Yield.xyz as access points, plus Pendle and Merkl as incentive layers — meaning the standard is being built with third-party distribution from the outset, not as a single-app product.

However - it's worth flagging that ERC-7984 is one proposal among several possible confidential-token designs, and its long-run dominance across the whole category (not just Zama's own ecosystem) isn't assured yet.

3c. Category-Wide Traction

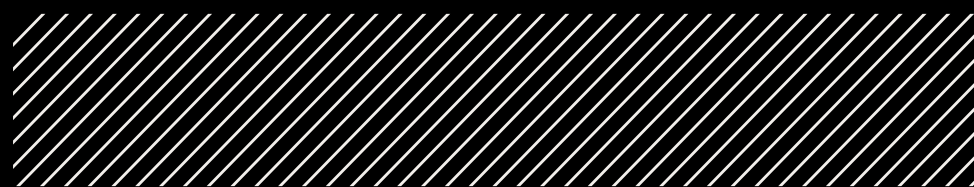
The category isn't just growing in TVL — it's widening. The number of tracked privacy protocols rose from 18 to 39 over 18 months (+117%), and that growth is accelerating, not flattening: September 2026 alone added 5 new protocols (+15.2% month-on-month) — the single largest monthly jump in the whole window, more than double the average monthly addition rate. Growth wasn't perfectly smooth (one month, March 2026, saw a small net decline of 1 protocol, and 6 of the 19 months were flat), but the category is currently on its strongest run in the dataset, sitting at an all-time high in both protocol count and TVL simultaneously.

The more revealing trend is who's taking share within that growth. From that first tracked month, FHE's share of excluding mixers category TVL has risen monotonically, without a single monthly dip: from 23.1% in May 2026 to 41.7% today — a +18.6 percentage-point gain in five months, entirely at ZK's expense (ZK's share fell from 76.9% to 58.3% over the same window). FHE has not yet overtaken ZK in share, but the trajectory, if it continued at the same pace, would cross 50% within roughly the next two months — flagged here as a trend read, not a forecast.

Below, we have the Approach-by-Approach Scorecard:

APPROACH-BY-APPROACH SCORECARD						
Approach	Leading example	TVL today	90d Δ	Chains (live)	Tracked since	Use case / partner ecosystem
FHE	ZAMA	\$83.1M	+262.9%	Ethereum (1 chain)	2026-05-04	Institutional confidential yield (Steakhouse/Morpho vaults); OTC settlement (GSR), payroll/custody (Bron)
ZK	Railgun	\$101.5M	+29.1%	Arbitrum, BSC, Ethereum, Polygon (4 chains)	2022-01-28 (our window start — Railgun predates this)	Private DeFi interactions, wallet-level shielded balances
ZK	Privacy Pools	\$9.4M	+23.7%	Arbitrum, Ethereum, Optimism (3 chains)	2025-03-31	Compliance-oriented shielded pools (association-set proofs)
ZK (other shielded pools — long tail)	27 smaller protocols (zkBob, Privacy Cash, Umbra, Nocturne, Hinkal, etc.)	\$5.0M	+121.4%	Multiple (Ethereum, Solana, others)	Varies (2025-03 onward)	Long tail of smaller ZK-based shielded pools/mixers making up the balance of the compliant ZK cohort
ZK (wound down)	Aztec Connect	\$0.0M (n/a — already at \$0 across the full 90d window)	n/a	Ethereum (1 chain)	n/a — now inactive	Formerly a ZK-rollup-based confidential DeFi implementation; now inactive
ZK (mixer, excluded from compliant cohort)	Tornado Cash	\$790.2M	+80.8%	Arbitrum, BSC, Ethereum, Ethereum Classic, Gnosis, Optimism, Polygon (8 chains)	2019-12-17	General-purpose anonymity mixer — excluded from institutional compliance frameworks and from this report's category figures
TEE	Oasis Sapphire	\$189.4K	+7.9% (90d — see note)	Confidential EVM chain	—	Hardware-isolated confidential compute; weak onchain DeFi traction to date
MPC	Bron	Not TVL-tracked	—	—	—	Custody/wallet infrastructure (MPC + native confidential-token support), not base-layer settlement

Figures: DefiLlama privacy-category and chain TVL as of Sept 23, 2026. "Time to \$100M" comparison and standardization narrative are Zama-reported (Q1 2026 Shielded Report), labeled as such throughout.





ZAMA

Technology Deep Dive: Inside the Zama Protocol

RESEARCH REPORT 2026

Technology Deep Dive: Inside the Zama Protocol

The Architecture: A Full-Stack Confidentiality Protocol

Zama's protocol is built in layers, each with a distinct role. At the base sits The Zama Confidential Blockchain Protocol — general-purpose confidentiality infrastructure deployable across chains (Ethereum, other EVMs and Solana are named in the roadmap).

Above it sits a set of core confidential financial primitives — confidential transfers, swaps, and lending — directly into the protocol layer rather than leaving them to individual applications to reimplement. At the top of the stack, the Zama App and SDK sit side by side: the App is the consumer-facing gateway for shielding, transferring, earning, and swapping; the SDK gives institutions and third-party developers the same primitives to build custom confidential flows into their own products.

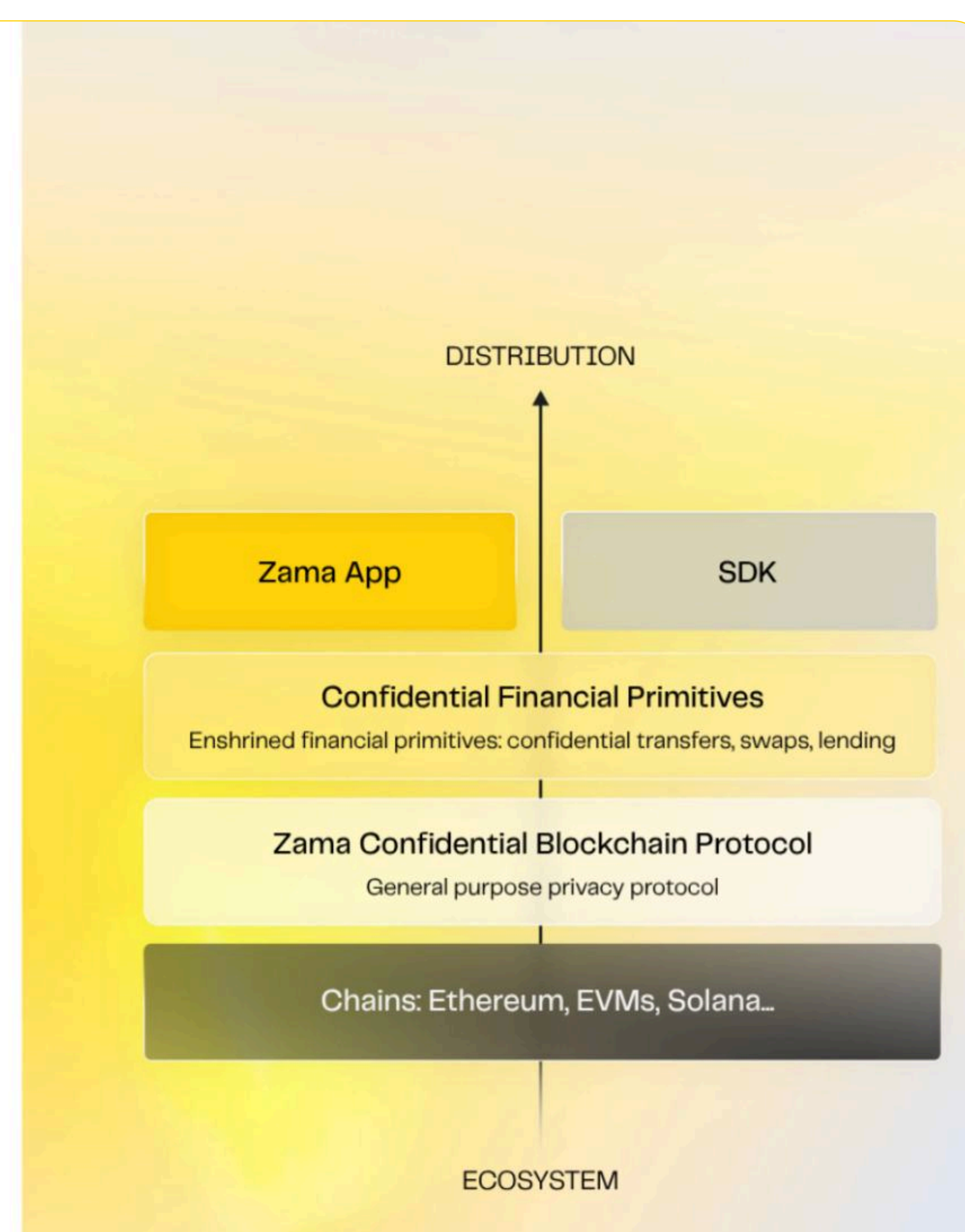
The design intent is explicit: Zama solved the underlying cryptography and shipped the general-purpose protocol first, and is now building the application and distribution layer on top of it, with every third-party SDK integration functioning as an additional distribution point for the base protocol.

Zama is a full-stack confidentiality protocol for onchain finance

Zama built the cryptography that underpins our protocol enabling privacy and compliance on top of existing public blockchains. We're extending the general purpose capabilities of the protocol with financial primitives and applications derived from these primitives that make using confidential tokens as seamless as regular ERC-20s.

The Zama App serves as a gateway for investors looking to access onchain finance confidentially: shield/unshield, transfer, earn and swap. We're also taking these primitives and building tailored solutions for institutions looking to access onchain finance. The SDK enshrines these primitives and offers the modularity institutions need to create custom confidential flows within their product stack.

Zama solved the core cryptography and deployed the general purpose protocol. Now, we're building solutions to own the full stack for confidential onchain finance.



The Cryptography: FHE and Quantum Resistance

Fully Homomorphic Encryption computes directly on encrypted data without ever decrypting it — the property that lets a balance, a trade size, or a lending position remain encrypted onchain while still being verifiably valid and composable with public infrastructure. Zama's implementation rests on lattice-based cryptography, which the protocol's own reporting positions as inherently resistant to attack by future quantum computers, in contrast to cryptographic approaches (including most ZK and TEE implementations) that do not carry the same guarantee.

Zama cites NIST's recognition of lattice-based schemes as the strongest available post-quantum option, and frames data encrypted onchain today as safe against decryption by quantum hardware in the future — a relevant distinction given public estimates that quantum computers could break ECDSA, the signature scheme underlying Bitcoin and Ethereum, within the next several years.

On audit posture, Zama reports an ongoing ISO-track audit program for the protocol's underlying scheme, NIST recognition of FHE as post-quantum secure, and a Trail of Bits engagement described as the most heavily audited protocol in its history, backed by a stated \$1M/year budget for new audits.

FHE is already quantum resistant

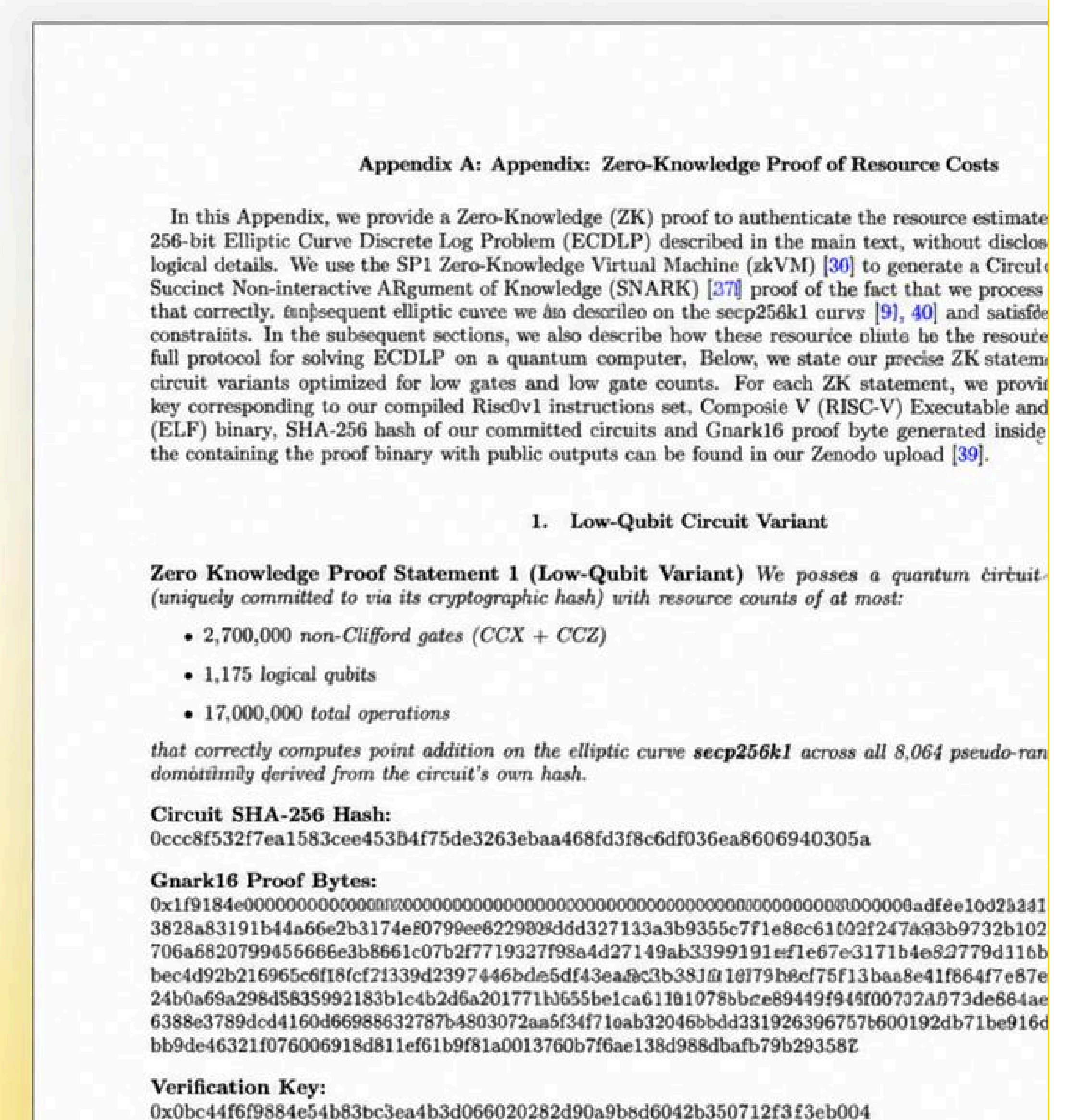
Google predicts quantum computers will break ECDSA (used by Bitcoin and Ethereum) by 2029, making this a critical threat to blockchain security.

Zama's FHE technology is based on lattice cryptography, which is **already quantum-resistant** and recognized by NIST as the strongest post-quantum option available.

Data encrypted with Zama today is safe even against future quantum computers.

Prof. Nigel Smart, Zama's Chief Academic Officer, talks about it [here](#).

 Ongoing for Zama Protocol underlying scheme	 FHE is post-quantum	 Most audited protocol in history, \$1M/year budget for new audits
--	--	--



Performance: From Theoretical to Production-Scale

The clearest real-world stress test of the protocol's throughput came from its own token launch. The ZAMA public sale ran as a sealed-bid Dutch auction over four days in January 2026 — the first FHE-powered auction conducted on a public blockchain, and a deliberate production test of the protocol alongside its role as a token distribution event.

At peak throughput, the auction became the most-used application on Ethereum by transaction volume, ahead of USDT and USDC transfers, processing 14,600 encrypted bids from 7,653 unique participants over four days without incident. The protocol used roughly 1% of co-processor capacity on average and peaked near 4%, while filling 30% of Ethereum's available blockspace — evidence, per Zama, that the protocol has scaling headroom well beyond what a fully confidential production deployment would require.

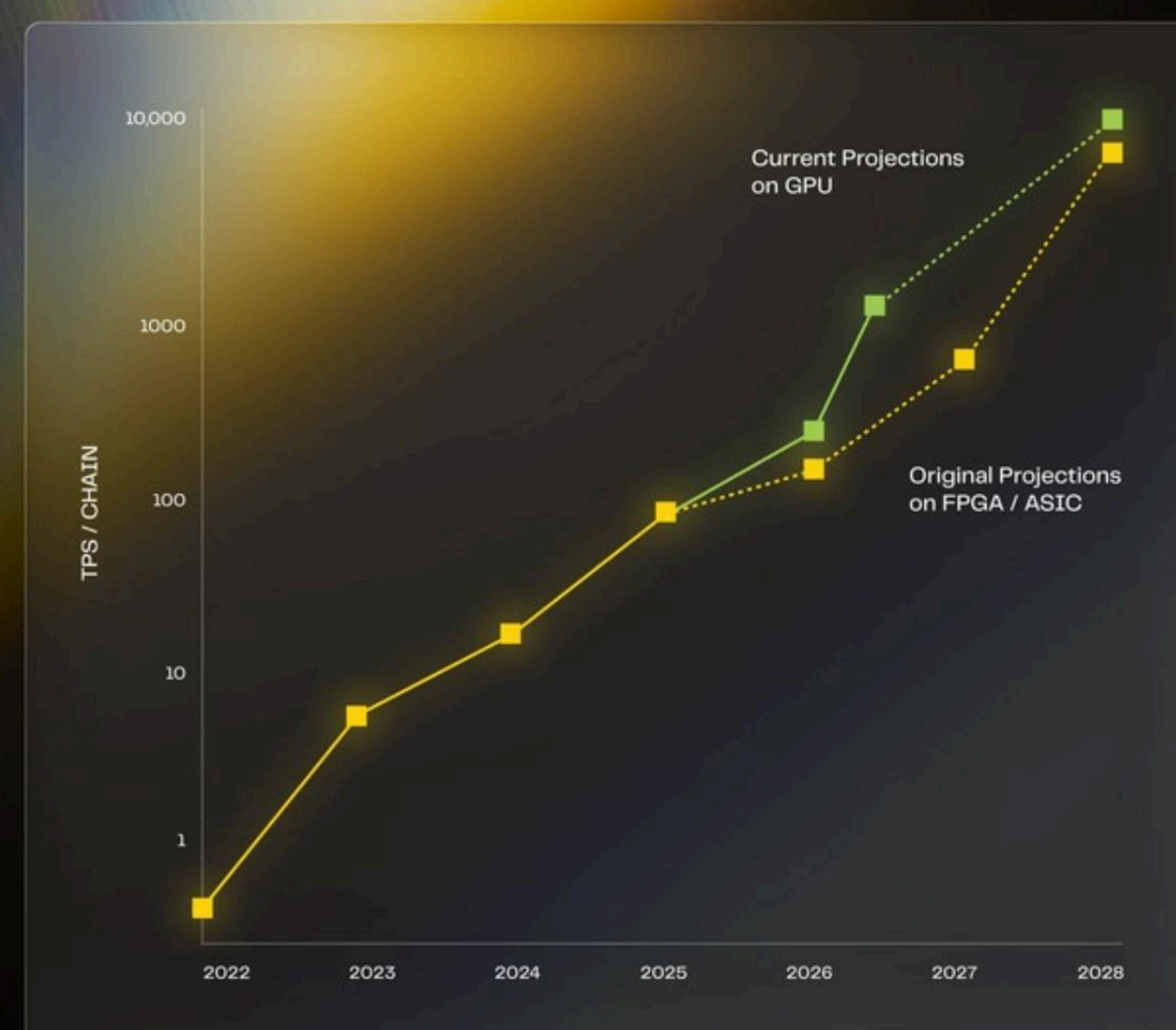
That headroom became a stated milestone by Q2 2026: Zama's engineering team reports reaching 1,000 confidential transfers per second on standard GPUs, arriving roughly a year ahead of the protocol's internal roadmap and without requiring custom hardware. At that throughput, Zama reports the cost of a single confidential token transfer falls below \$0.00005. The protocol's own performance trajectory is framed as outpacing Moore's Law — roughly a 10x throughput improvement every 18–24 months — with 10,000 TPS targeted by 2028 and 100,000 TPS by 2030.

Zama now has the capacity to reach 1,000 TPS per chain

The Zama engineering and cryptography teams have achieved a major milestone: 1,000 confidential transfers per second (TPS)! This came a year earlier than anticipated, using standard GPUs rather than custom hardware.

1,000 TPS is not just symbolic, it's also the throughput required for scaling onchain finance use cases and dramatically lowers the cost of a transaction. Taking into account all the nodes running the Zama Protocol, the cost of a confidential token transfer is now less than \$0.00005.

FHE outpaces Moore's law: performance improves roughly by an order of magnitude (10x) every 18–24 months, meaning we can expect to get to 10,000 TPS by 2028 and 100,000 TPS by 2030, enough to power global human and agentic finance.

[Read more ↗](#)


Multichain Roadmap

Zama's 2026–2027 deployment plan starts with Ethereum mainnet in H1 2026, followed by GPU-based scaling in H2 2026 alongside expansion to two additional EVM chains, with Solana deployment targeted for 2027 — extending the protocol beyond its current single-chain (Ethereum) footprint.





ZAMA

Ecosystem & Use Cases

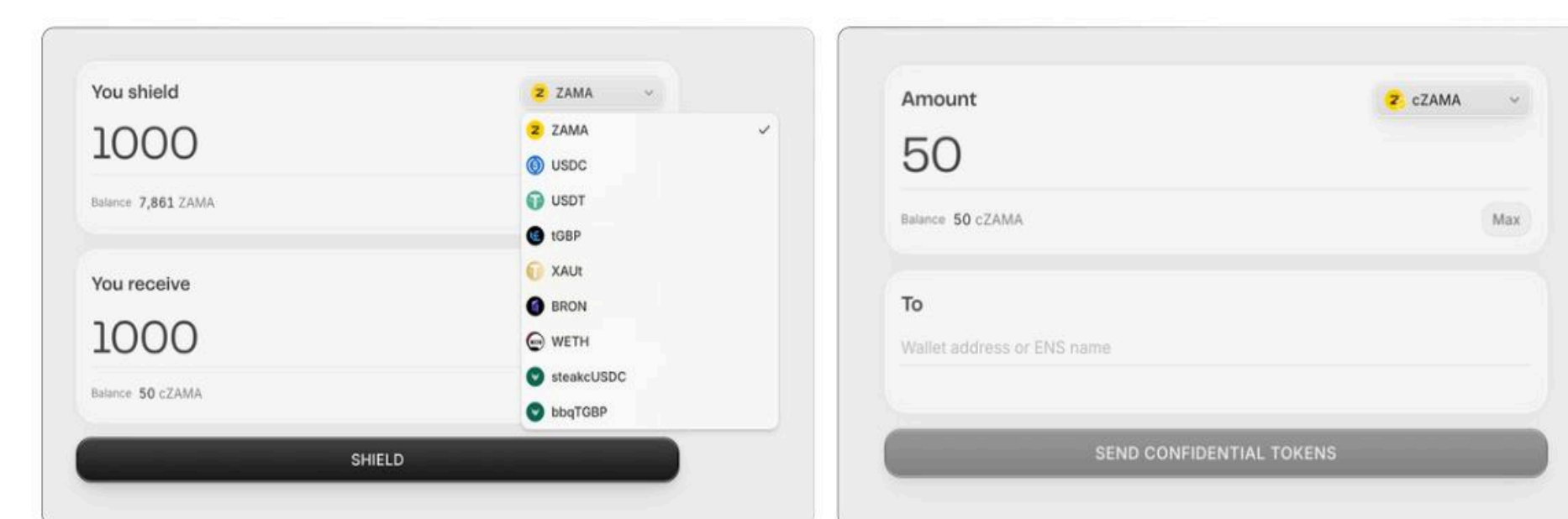
RESEARCH REPORT 2026

Ecosystem & Use Cases

The Zama App enables investors to confidentially shield, transfer, earn and swap digital assets

We've packaged the first confidential financial primitives into a user-friendly, front-end application for anyone to use by simply connecting their existing wallet. The same primitives used to design confidential flows within our partner ecosystems are available to any user in the Zama App.

The Zama App is fundamental to on-ramping users into the cToken ecosystem and developing a meaningful base of shielded TVL. It serves as a universal entry point for confidential tokens and is fully extensible for institutional partners to adapt and distribute within their own ecosystems and applications.

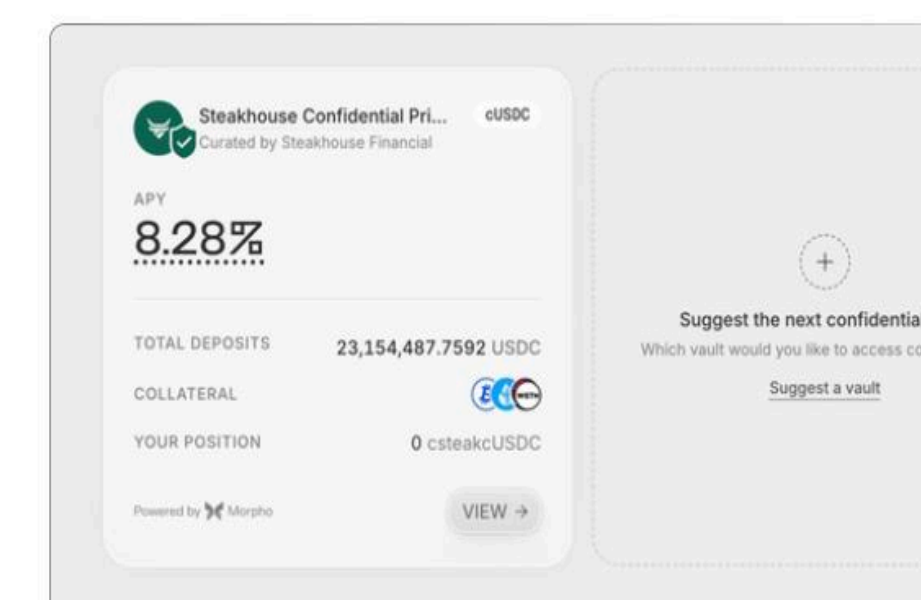


Shield Tokens

Select USDC, USDT, or any supported asset. Shield it in one click.

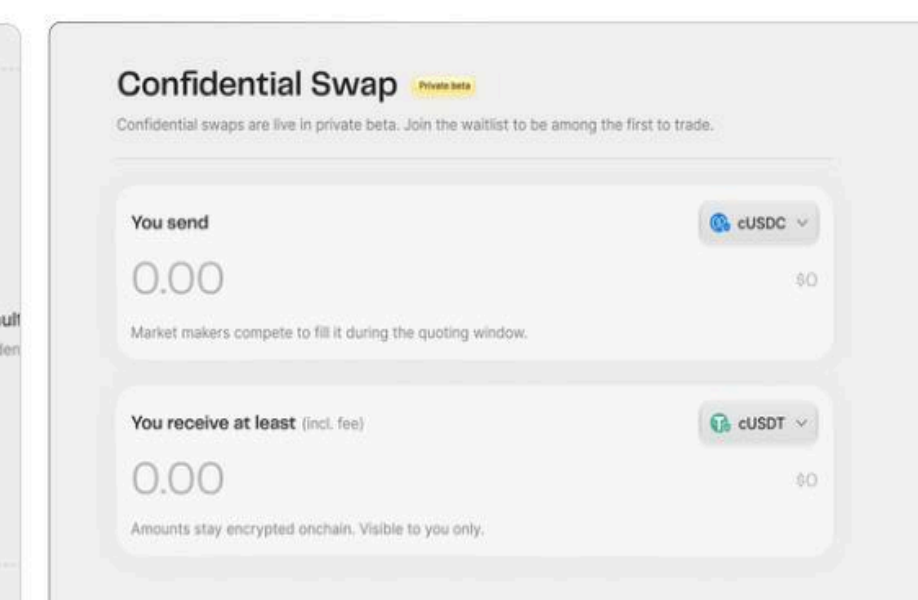
Send Confidentially

Transfer to any address. Amount visibly only to sender and recipient.



Earn yield on your shielded assets

Earn yield on confidential tokens without exposing your position.



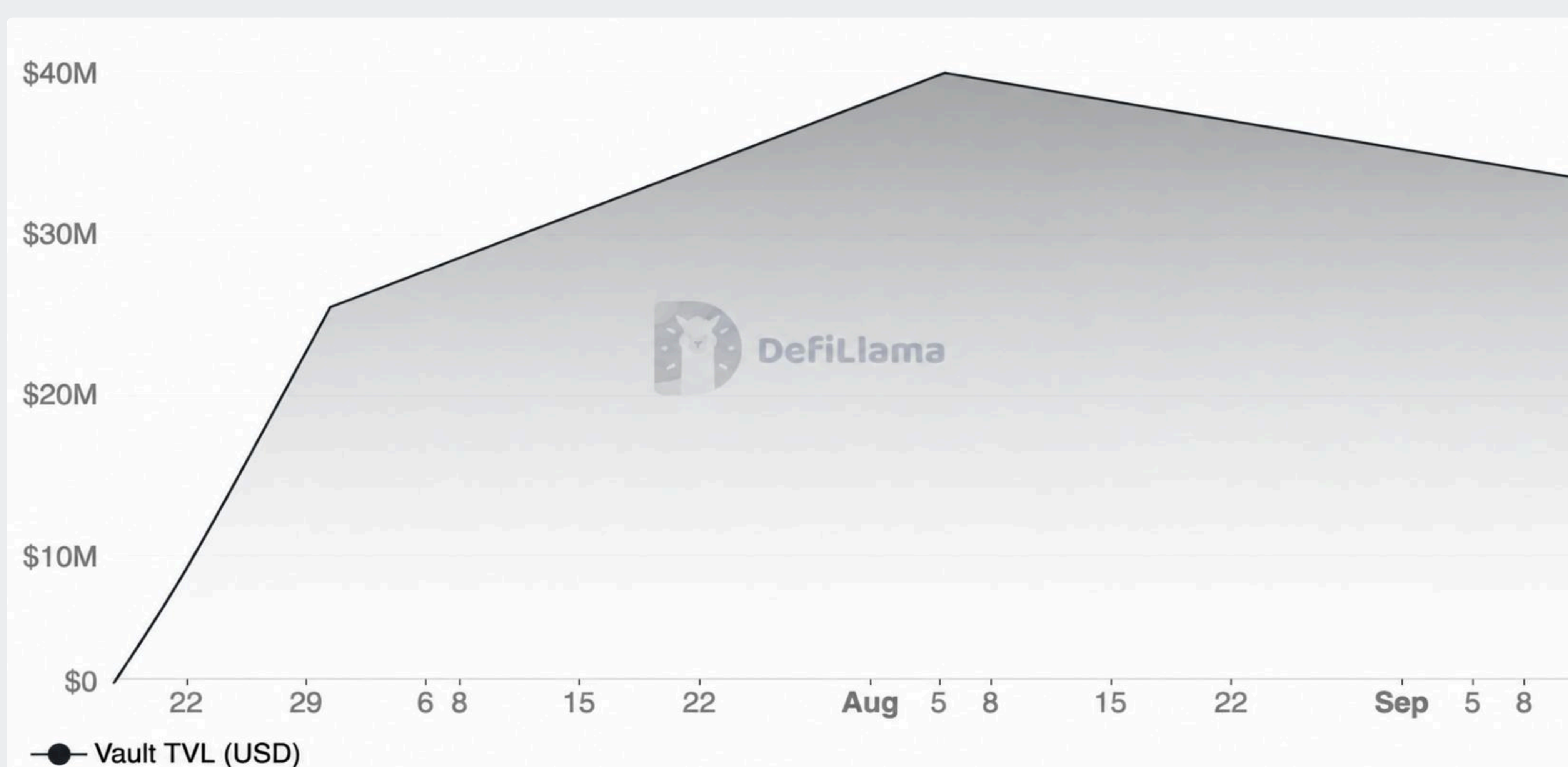
Swap between assets confidentially

Trade confidentially with market makers without revealing size, direction or asset.

Institutional Yield: From One Vault to a 16-Vault Suite

Confidential DeFi's institutional proof point started with a single vault. The Steakhouse Confidential Prime USDC vault, launched with Morpho in June 2026, grew from zero to \$25.5M in TVL by month's end — enough to place it among the top-10 USDC vaults on Morpho — before peaking near \$40M roughly seven weeks after launch, tracking the front-loaded structure of its 12-week incentive program. By September 11, 2026, the vault held \$33.5M in TVL at a 7.2% base APY, a pullback consistent with the incentive program's tapering phases rather than a loss of depositor confidence.

STEAKHOUSE CONFIDENTIAL PRIME USDC VAULT: TVL TRAJECTORY



Source: DefiLlama

On September 15, 2026, Zama, Morpho, and five institutional curators expanded that single proof point into a full product line: 16 confidential vaults across 5 asset classes (USDC, USDT, WBTC, AUDS, tGBP), split into two structures:

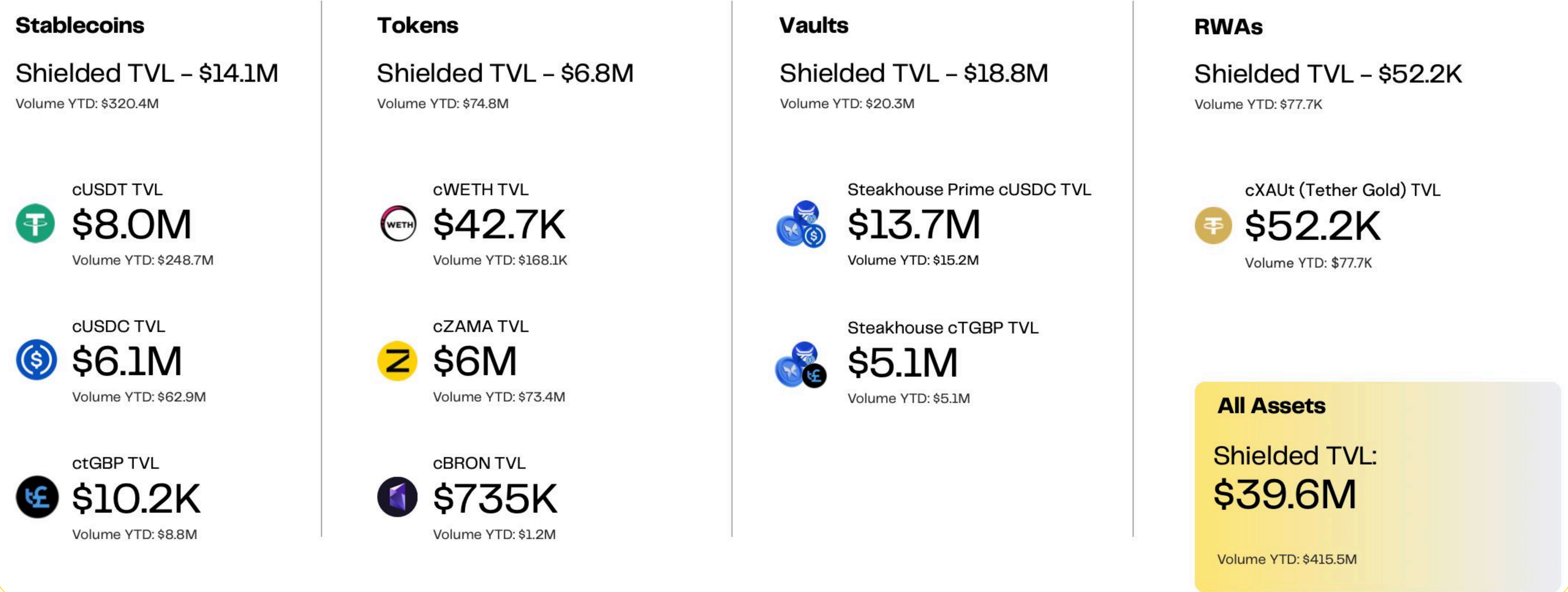
- **12 Hybrid vaults** — confidential entry into existing curated vaults (including a new Steakhouse Prime USDT vault), with the same strategy, liquidity, and risk profile as the underlying public vault, differing only in confidential deposit and position.
- **4 Exclusive vaults** — net-new, confidential-only vaults with no public equivalent, including Wintermute's Confidential WBTC vault (armcWBTC).

All 16 vaults are live on Morpho through the Zama App, with Utila, Zerion, and Yield.xyz distribution rolling out in the following weeks. The curator roster now spans five firms with materially different mandates:

- **Steakhouse Financial (\$4.5B+ TVL)** — the original vault partner, now extending into a five-vault suite. Co-founder Sébastien Derivaux: "The natural next step was to extend that access to a five-vault suite across USDC, USDT, and TGBP. Depositors now have more choice in how they use stablecoins across Morpho, while keeping their positions private."
- **Armitage by Wintermute** — Wintermute's onchain vault curation arm, distinct from the stablecoin curators in that it executes its own liquidations across every supported market, broadening the collateral types (including WBTC) it can accept.
- **Flowdesk** — bringing an AUDS RWA Strategy Vault into confidential access. Co-founder and CEO Guilhem Chaumont: "Confidentiality is the condition onchain capital markets have to satisfy before they can carry institutional-scale volume."
- **RockawayX** — \$2B+ AUM, applying institutional-grade credit underwriting with a stated zero-default record across CeFi and DeFi lending since 2022.
- **Bitwise** — a \$11B+ crypto asset manager serving 5,000+ financial advisors and institutions, the largest traditional-asset-management name in the curator set.

Morpho co-founder Merlin Egalite framed the expansion as scaling infrastructure rather than changing it: "Adding these confidential vaults on Morpho was an important step for us. It'll scale confidential DeFi efficiently and open new possibilities for allocators onchain, without changing the strategy, the liquidity, or the risk profile." On DefiLlama's live tracking, Morpho itself carries \$11.0B in TVL, up 16.6% over the past 30 days, and Steakhouse Financial curates \$3.1B across its vault suite — meaning even the 16-vault expansion still represents a small fraction of either platform's total activity, the same scale dynamic the original single-vault launch showed.

Confidential tokens now cover most major asset classes



The Confidential Swap Protocol

Launched alongside the vault suite, the Zama Swap Protocol closes the deposit-earn-swap loop entirely inside a confidential envelope — letting depositors swap between confidential assets, including vault share positions without exposing intent or size. This is a net-new product with no prior-quarter data; its usage will be a metric to establish in future updates rather than one available today.

RWA Tokenization: T-REX and Apex Group

Beyond yield, Zama's confidentiality layer extends into real-world-asset tokenization. T-REX — described in Zama's Q1 2026 report as the leading RWA protocol and permissioned token standard, with over \$32B already tokenized, 20,000 users, and 200+ token issuers and service providers — chose Zama as the confidentiality layer for its upcoming canonical chain. T-REX is backed by Apex Group, a global asset manager with \$3.2T in AUM, which has committed to tokenize \$100B in assets by June 2027.

Institutional Trading and Custody: GSR and Bron

Two live deployments demonstrate confidential settlement outside the vault-yield use case. GSR, an OTC market maker, executed a trade settled confidentially through Zama's protocol while preserving full compliance — a use case GSR's Global Head of OTC Trading, Spencer Hallarn, tied directly to institutional trading pain points: "Confidential settlement infrastructure addresses one of the largest pain points for institutions trading digital assets." Zama cites 2025 crypto OTC volume at \$15T as the scale of the market this addresses.

Bron, a self-custodial wallet combining MPC with native confidential-token support, executed what Zama describes as the world's first confidential payroll on Ethereum mainnet in December 2025, settling salary payments in confidential USDT with amounts visible only to sender and recipients while remaining publicly verifiable and auditable. Bron reports \$1B+ in assets held in its wallets, averaging \$1M per user.

A third integration extends confidential settlement into wallet infrastructure itself. Dfns, an enterprise wallet platform serving 400+ institutional clients across banking, fintech, custody, RWA, and payments, has natively integrated the confidential token standard into its wallet and transaction stack, making encrypted onchain transactions available to its client base out of the box on Ethereum and EVM chains. The integration targets four use cases directly: settlement and capital markets (encrypted transfer amounts without revealing order sizes), payments (processing institutional flows without exposing counterparties or amounts), banking and custody (managing client positions without making them readable to the market), and RWA distribution (transferring tokenized holdings without revealing ownership, while preserving selective disclosure to regulators or auditors). As with Zama's other institutional integrations, confidentiality here is paired with programmable compliance — designated auditors or regulators can be granted decryption access to specific transactions, mirroring the selective-disclosure model banks already operate under, rather than replacing it.

Payments: Tokenised GBP

tGBP, an FCA-registered GBP stablecoin issued by BCP Technologies and used by exchanges including Coinbase and Kraken, has a confidential counterpart (cTGBP) enabling UK companies to manage operations onchain privately. Per Zama's Q1 2026 report, tGBP carried a \$30M market cap with 17% of supply shielded; the September 2026 expansion adds a dedicated Steakhouse-curated cTGBP vault, and BCP Technologies CEO Benoit Marzouk frames the UK as a "greenfield opportunity" for confidential stablecoin adoption among large institutions.

Security, Compliance, and Infrastructure Partnerships

Beyond the yield, RWA, and payments use cases above, four partnerships extend the Zama Protocol's security and compliance surface directly. OpenZeppelin — already the co-author of the ERC-7984 standard — has been a strategic partner from day one on security as well: its audited smart-contract libraries secure over \$27 trillion in value transferred across Ethereum and other chains, and its Confidential Contracts Library, built on Zama's FHEVM, gives developers production-ready primitives for encrypted tokens, sealed-bid auctions, confidential vesting, private governance, and tokenized RWAs — alongside a customized Contracts Wizard and a new Privacy Relayer for encrypted transaction execution.

Blockscout, the leading open-source block explorer, now natively supports ERC-7984 confidential tokens — recognizing them as a dedicated token type alongside ERC-20, ERC-721, and ERC-1155, indexing confidential transfers with sender, recipient, transaction hash, and block visible while the transfer amount stays marked confidential, and exposing this activity through its API for dashboards and compliance workflows. This closes a real usability gap: without explorer support, confidential token activity would sit onchain but invisible to the tools developers, users, and institutions rely on to verify it.

Two further partnerships bring compliance screening and monitoring directly into the protocol. Elliptic performs wallet-level risk screening before funds enter the protocol — live today on confidential vaults — screening addresses only, with no encrypted balances or transaction amounts ever exposed. Hypernative layers continuous onchain monitoring on top, deployed across Zama's confidential wrappers, host contracts, and DeFi protocol integrations, and is extending its Transaction Guard product with native confidential-token support for pre-execution transaction simulation.

Together, these four partnerships form what Zama calls a "compliance by design" architecture: standardized and audited contracts (OpenZeppelin), visible and indexable activity (Blockscout), pre-transaction screening (Elliptic), and continuous post-deployment monitoring (Hypernative) — directly addressing the auditability and regulatory-uncertainty risks raised later in this report from the infrastructure side.



ZAMA

Metrics: Tracking the Category

RESEARCH REPORT 2026

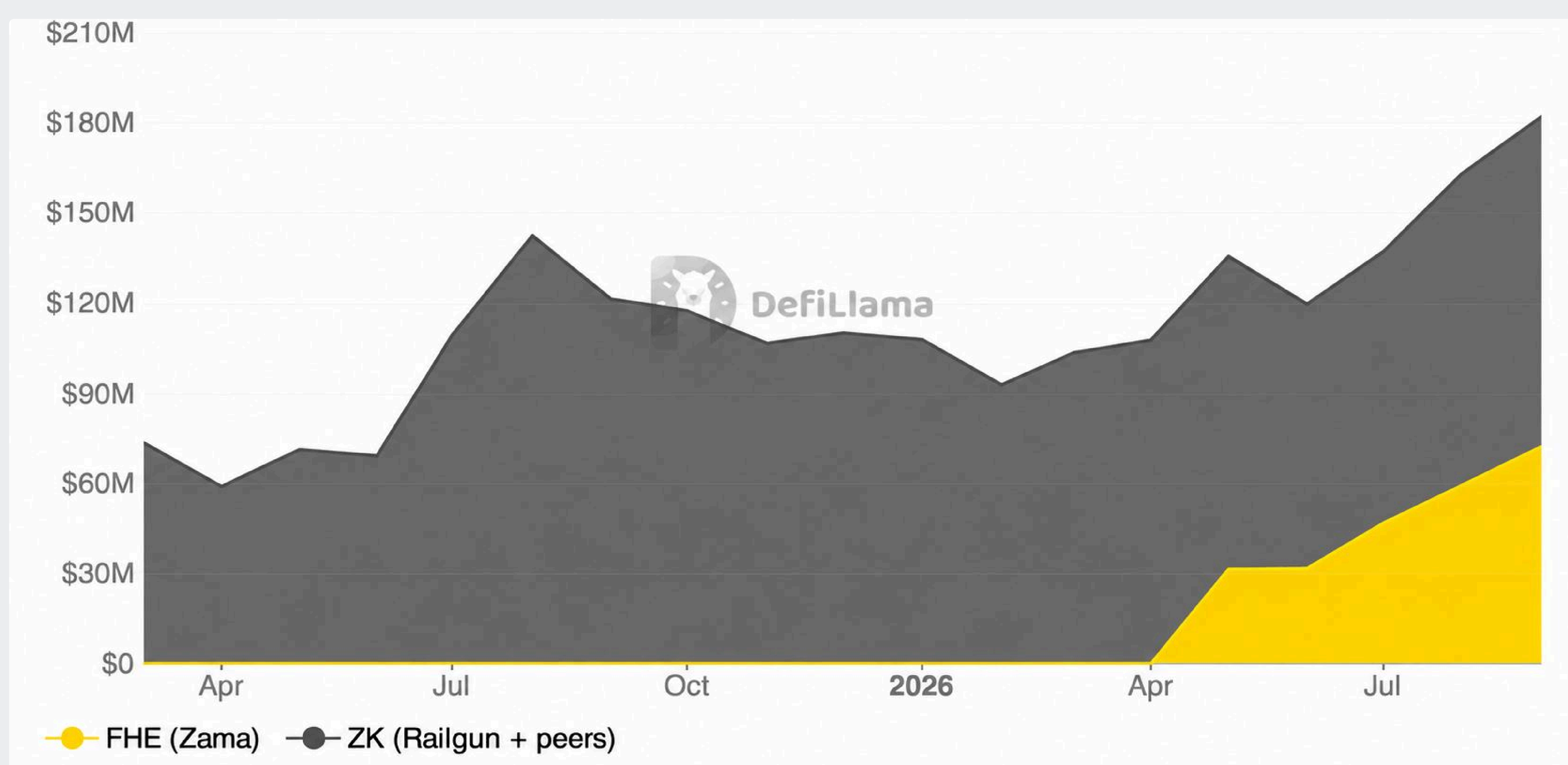
Metrics: Tracking the Category

This report uses two tiers of metrics, deliberately kept separate: DefiLlama's independent, cross-protocol tracking as the category-wide benchmark, and Zama's own reported figures as the detail layer beneath it.

Tier 1: DefiLlama's Privacy Category — The Independent Benchmark

DefiLlama's privacy category is the only cross-protocol benchmark that lets Zama's traction be read against its peers rather than in isolation. As of today, the category carries \$984.2M in total tracked TVL across 39 protocols, or \$197.6M stripped of anonymity mixers. Within that compliant cohort, the FHE/ZK trend already is the clearest single metric for tracking the category's structural shift over time:

CONFIDENTIAL DEFI TVL BY APPROACH: FHE VS. ZK (EXCLUDING MIXERS, 18-MONTH TREND)



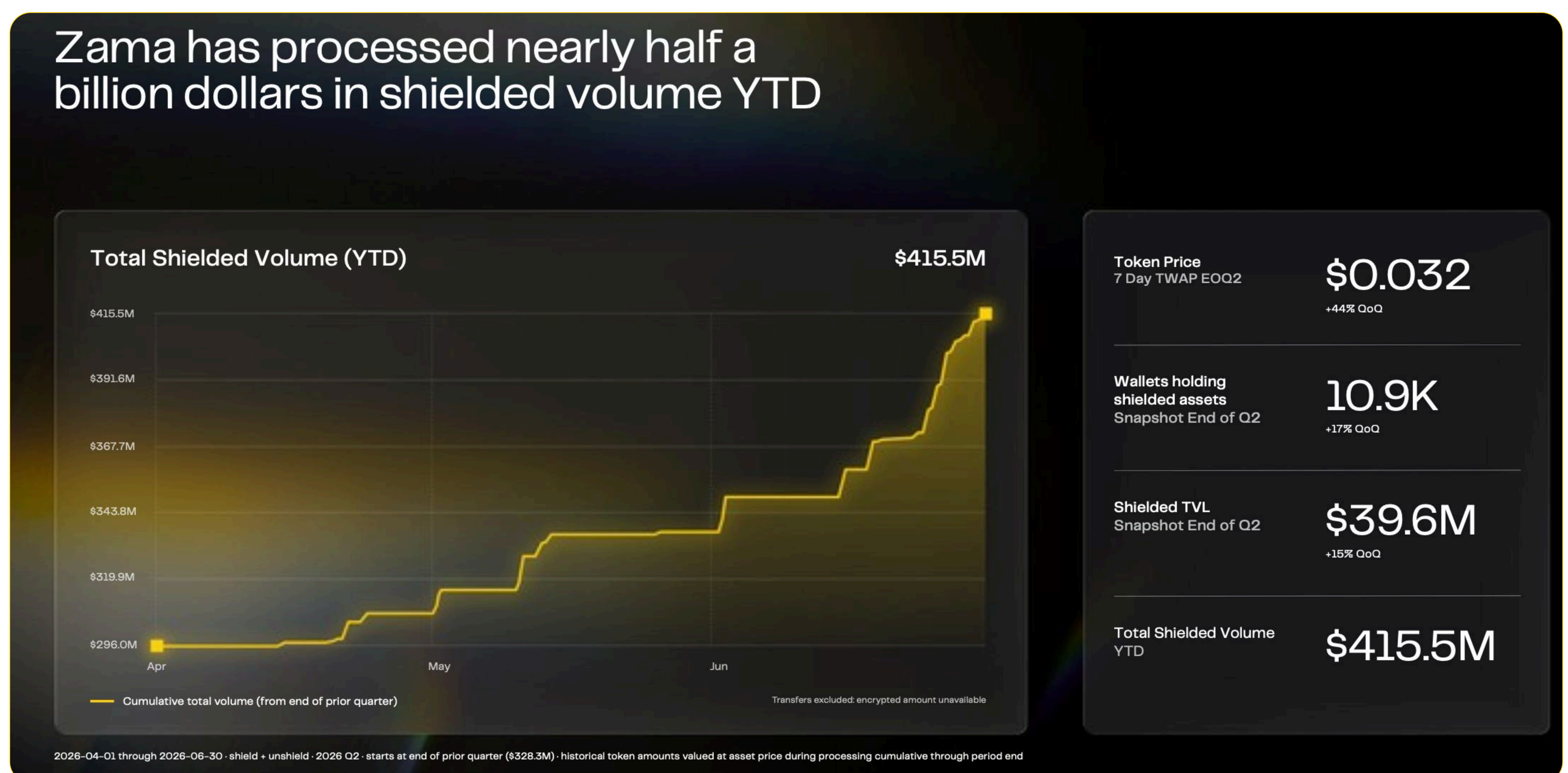
Source: DefiLlama

Zama's own protocol TVL on this independent tracking currently stands at \$82.7M, up 39.0% over 30 days and 3.6x over 90 days — the fastest-growing single line in the category benchmark.

Tier 2: Zama's Self-Reported Metrics — The Detail Layer

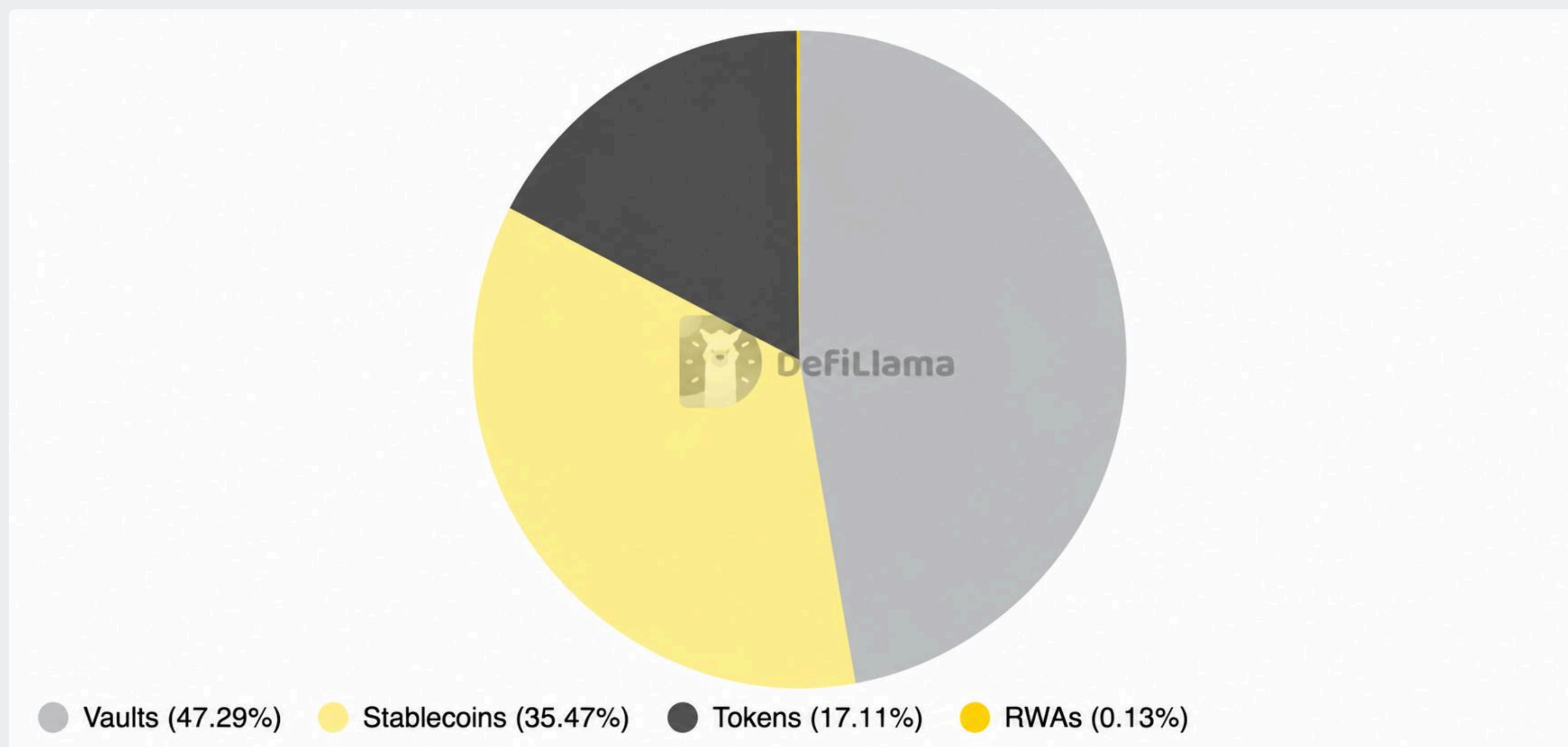
DefiLlama's category TVL captures Zama's onchain footprint but not the metric Zama itself uses internally: Shielded TVL, alongside cumulative shielded volume and unique depositor counts. These come from two sources — Zama's quarterly Shielded Reports (point-in-time snapshots) and its live Dune dashboard, which tracks Shielded TVL, cumulative shield/unshield volume, unique depositors, per-vault Confidential Vaults TVL, and \$ZAMA token metrics on an ongoing basis.

The two quarterly snapshots reported so far show: Shielded TVL peaked at \$123M in Q1 2026, within days of the ZAMA public sale shielding over \$120M in USDT, then settled to a \$39.6M snapshot by June 30, 2026 — still up 15% quarter-on-quarter against Q1's own end-of-quarter level once the auction-driven spike is excluded.



The more durable growth signal sits beneath that snapshot: cumulative shielded volume reached \$415.5M year-to-date by Q2, up 44% quarter-on-quarter, with 10,900 wallets holding shielded assets, up 17% over the same period. Zama's Q2 2026 report also breaks that \$39.6M shielded TVL down by asset class:

ZAMA SHIELDED TVL BY ASSET CLASS (SELF-REPORTED, Q2 2026)



Source: DefiLlama

Vaults (\$18.8M) are the largest single bucket — consistent with the Steakhouse vault being the category's most advanced live product — followed by stablecoins (\$14.1M), tokens (\$6.8M), and RWAs (\$52.2K), summing to \$39.75M total.



ZAMA

Risks & Open Questions

RESEARCH REPORT 2026

Risks & Open Questions

Five structural risks apply to confidential DeFi as a category, regardless of which cryptographic approach ultimately leads.

Fragmentation Across Approaches

FHE, ZK, MPC, and TEE implementations are not interoperable. A confidential balance shielded under one system cannot move to another without first unshielding back to a public asset — meaning liquidity is fragmented across incompatible privacy silos rather than pooled into a single confidential venue. The category's current approach scorecard illustrates the practical version of this: Zama's entire live footprint sits on a single chain (Ethereum), and Railgun spans four — each approach is building its own chain-by-chain distribution independently, with no shared confidential-liquidity layer connecting them.

Zama's own roadmap treats this as a solvable distribution problem rather than a permanent constraint: its 2026–2027 plan moves from Ethereum mainnet in H1 2026 to GPU-based scaling alongside two additional EVM chains in H2 2026, with Solana deployment targeted for 2027. That roadmap addresses fragmentation within Zama's own footprint — more chains for FHE to reach — but does nothing to resolve the deeper structural issue: even a fully multichain Zama deployment would still be unable to move a confidential balance into a ZK-shielded or TEE-based system without unshielding first. Going multichain widens one approach's reach; it does not make the four approaches interoperable with each other.

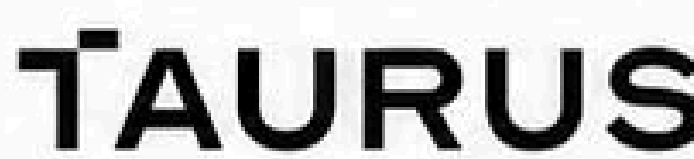
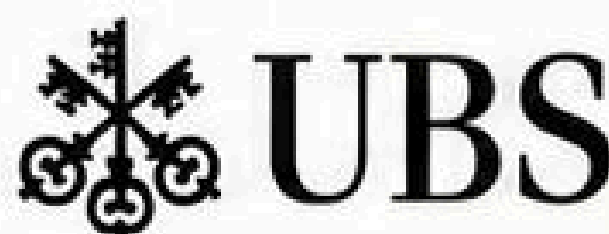
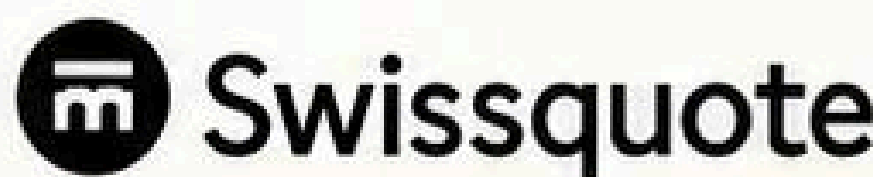
Standards adoption follows the same pattern: Blockscout's native support for ERC-7984 and OpenZeppelin's Confidential Contracts Library make Zama's tooling more accessible across the chains it already reaches, but neither extends interoperability across approaches — a ZK-shielded balance still cannot flow through Blockscout's confidential-token indexing or into an FHE-wrapped position without first unshielding back to a public asset.

Standardization Risk

ERC-7984 is gaining real adoption within Zama's own ecosystem — OpenZeppelin Contracts library integration, Dfns wallet support, Blockscout's native block-explorer support for confidential tokens, and a three-organization founding of the Confidential Token Association — but that adoption is concentrated among Zama, OpenZeppelin, and Inco specifically.

No evidence has emerged of the ZK-based cohort (Railgun, Privacy Pools) or the TEE-based cohort (Oasis Sapphire) building toward the same standard. A standard adopted by one approach's ecosystem is not the same as a category-wide convergence, and ERC-7984's long-run dominance across all four approaches is not assured.

Built on standards issuers already use.

ERC-7984	Confidential token standard. Encrypted balances and transfer amounts via FHE, with programmable disclosure.	    
ERC-3643	Permissioned token standard for RWAs and security tokens. Compliance enforced on-chain through identity verification (ONCHAINID) and transfer rules.	 
CMTAT	Open standard by the Swiss CMTA for tokenized securities (equity, debt, structured products). Built-in issuer controls: pause, freeze, forced transfers. Swiss-law compliant.	   

Regulatory Uncertainty

Programmable, selective-disclosure compliance is a stated design goal across every approach in this category — but no jurisdiction has yet defined a clear regulatory treatment for onchain confidential assets specifically. Institutional adopters are building on infrastructure whose compliance classification could still shift, even where the underlying technology already supports the disclosure controls regulators would likely require.

Partner commentary already implicitly acknowledges this gap: tGBP issuer BCP Technologies frames UK institutional stablecoin adoption as a "greenfield opportunity," and Flowdesk frames confidentiality as "the condition onchain capital markets have to satisfy" — both statements about a compliance bar that has not yet been formally set by regulators.

Zama's own response has been to build compliance infrastructure ahead of that regulatory clarity rather than wait for it: Elliptic performs wallet-level risk screening before funds enter the protocol, and Hypernative provides continuous onchain monitoring across Zama's confidential contracts — together signaling that the category is treating compliance as a design requirement now, not a problem to solve once regulators act.

Auditability

Following a June 2026 vulnerability disclosed in Zcash's Orchard shielded pool, Zama's own reporting argues that once assets are shielded under a pure ZK design, third parties generally cannot independently verify that shielded supply matches underlying deposits. This is a category-wide concern for any pure ZK shielded-pool architecture, not a Zama-specific claim about a competitor — but it is worth noting the claim originates from an FHE vendor assessing a rival approach's cryptography, rather than from an independent security audit of the ZK systems in question.

Concentration Risk (Venue and Chain)

Two concentration points sit underneath the category's current growth story. First, all 16 confidential vaults from the September 2026 expansion are deployed on a single venue, Morpho — the institutional-yield use case has no live proof point outside one lending protocol yet, a gap the report's own Outlook section flags as a trigger to watch. Second, Zama's live protocol TVL sits entirely on Ethereum today, with Solana deployment not targeted until 2027 — meaning the FHE approach's fastest-growing TVL in the category is currently concentrated on one chain, one venue, and a five-curator set that only reached its current size in September 2026.



ZAMA

Outlook & Conclusion

RESEARCH REPORT 2026

Outlook & Conclusion

Three triggers determine whether confidential DeFi moves from an emerging category to a mainstream one: additional institutional entrants beyond the current OTC/custody/curator set, a compliance standard actually converging across jurisdictions rather than merely being proposed, and a second major curator ecosystem — beyond Morpho — adopting confidential vaults at comparable scale.

On the first trigger, the evidence has moved decisively in the category's favor. The expansion from a single Steakhouse vault in June 2026 to 16 vaults across five curators — Armitage by Wintermute, Flowdesk, RockawayX, and Bitwise joining Steakhouse — in September shows that curators beyond the original proof point will adopt confidential rails once one is validated on infrastructure they already trust. This is no longer a single-institution experiment; it is a repeatable onboarding pattern with a \$11B+ asset manager (Bitwise) and a \$2B+ AUM firm (RockawayX) now inside it.

On the second trigger, progress is real but bounded. ERC-7984's integration into OpenZeppelin's Contracts library and the three-organization founding of the Confidential Token Association are genuine standardization steps — but as the Standardization Risk section notes, that convergence sits within Zama's own ecosystem specifically.

The signal to watch is whether a ZK-based or TEE-based project adopts the same standard, which would mark the shift from "Zama's standard" to "the category's standard."

The third trigger remains open. Every one of the 16 vaults sits on Morpho. No second curator ecosystem — a different lending or vault venue entirely — has yet replicated the confidential-vault pattern outside it. This is the single most consequential gap between where the category is now and where "mainstream" would require it to be, and it is also the cleanest trigger to monitor going forward: a confidential vault launching on a lending platform other than Morpho would be a stronger mainstreaming signal than any further expansion within Morpho itself.

Two additional signals sit underneath these three. The category-wide shift already underway — FHE's share of excluding mixers TVL rising from 23.1% to 41.7% over five straight months — suggests institutional capital is actively choosing the newest, most compliance-oriented approach over the incumbent ZK cohort, not simply adding to it.

And the Zama Swap Protocol, live as of September 15, 2026, has no reported volume yet; a full quarter of usage data will be the first real test of whether the deposit-earn-swap loop draws activity comparable to the vault layer it's built alongside.

Readers tracking these signals as they develop can follow Zama's live Dune dashboard (dune.com/zama_fhe/protocol-overview) for ongoing Shielded TVL, vault-level TVL, and volume data, rather than waiting for the next quarterly report.

Appendix

RESEARCH REPORT 2026

Appendix

ZAMA Token

\$ZAMA launched into the market via a sealed-bid Dutch auction in January 2026 — itself a live production stress test of the protocol, processing 14,600 encrypted bids from 7,653 participants and briefly becoming the most-used application on Ethereum by transaction volume. The token traded at a \$0.026 seven-day time-weighted average price through Q1 2026, on \$60M in average daily volume and a \$699.5M peak single-day volume, reaching 6.9K unique holders in its first quarter. It listed across a wide venue set immediately — Binance, Coinbase, Upbit, Bybit, OKX, Kraken, and even Revolut among centralized exchanges, and Uniswap, PancakeSwap, and Hyperliquid among decentralized venues.

By the end of Q2 2026, the token's seven-day TWAP had risen to \$0.032 — up 23.1% quarter-on-quarter. On DefiLlama's live tracking today, \$ZAMA trades at \$0.1003, up 285.6% against its Q1 average price and 213.3% against its Q2 average, with a \$245.1M market cap, \$1.13B fully diluted valuation on 11.3B total supply, and \$71.8M in 24-hour trading volume.

Staking participation has grown alongside price: circulating supply staked rose from 45% in Q1 2026 to 63% by the end of Q2, with total value staked increasing from \$23.1M to \$44.8M as average APY compressed from 47.8% to 33.8% — the expected pattern as more of the circulating supply gets locked into securing the protocol rather than trading freely.

Live data — snapshot September 23, 2026: [Zama's public Dune dashboard](#) shows Shielded TVL at \$81.8M, cumulative shielded volume at \$532.3M, and cumulative total volume (shielded plus unshielded activity) past \$982.8M — more than double the Q2 snapshot's shielded TVL in under three months, against 10,900 wallets holding shielded assets as of the Q2 report. Confidential Vaults TVL, tracked separately on the same dashboard, stands at \$58.5M, with the largest individual holdings sitting in the Steakhouse and RockawayX vault-wrapper tokens. Staking has also continued climbing, with 2.19 billion ZAMA now staked.

\$ZAMA is now listed on every major exchange

CEXs

 BINANCE	coinbase	<i>UPbit</i>	 Gate.io
BYBIT		 bitpanda	LBANK
 kraken	 KUCOIN	 bithumb	 uphold
 MEXC	 Backpack	 Bitget	 bitvavo

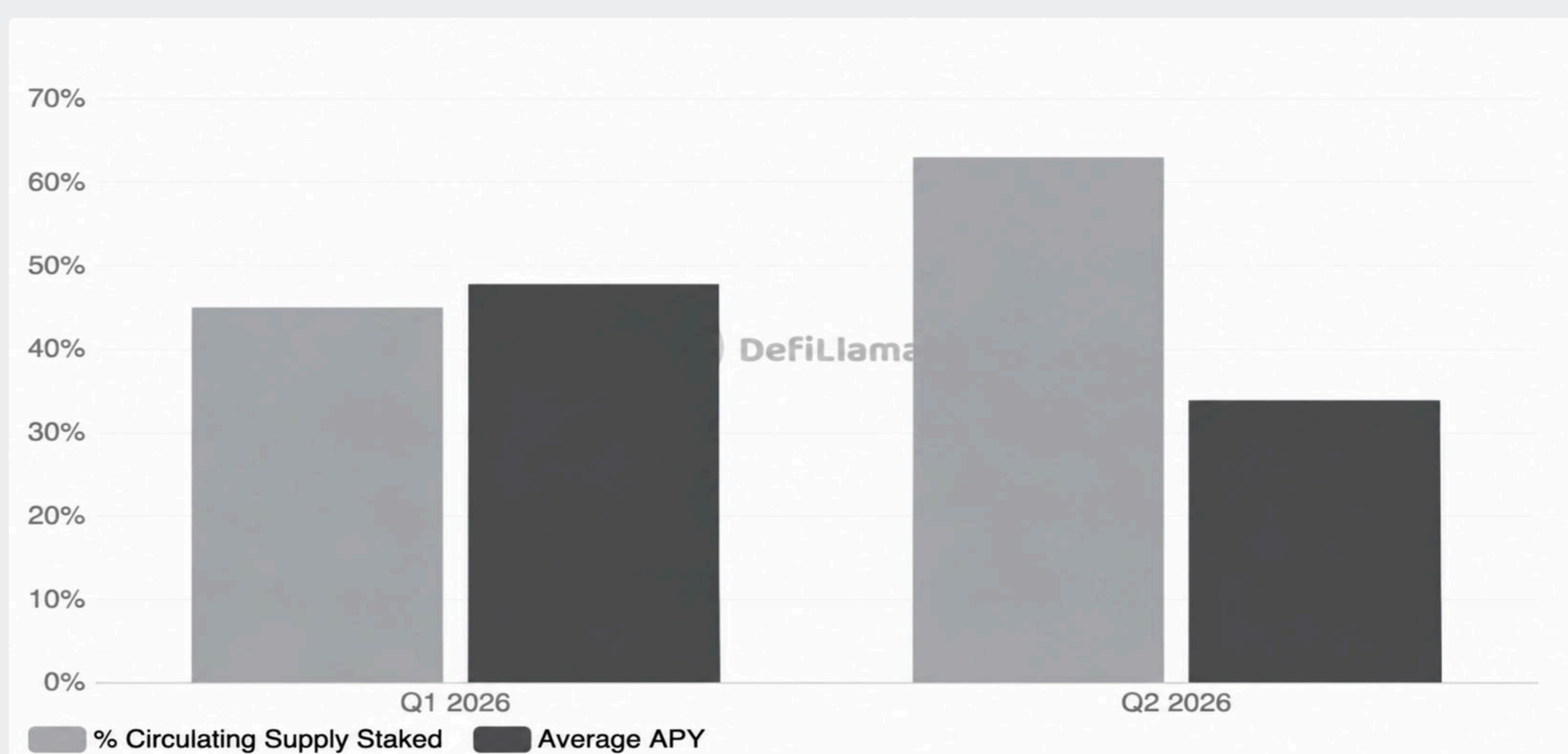
DEXs

 Uniswap	 PancakeSwap
 Hyperliquid	 sunrise
 Meteora	

Token Economics: A Staking Base That Nearly Doubled

Zama's own token, \$ZAMA, currently carries \$82.7M in DefiLlama-tracked TVL, up 39.0% over the past 30 days. Staking participation grew sharply across the two reported quarters: circulating supply staked rose from 45% in Q1 2026 to 63% by the end of Q2, with total staked value increasing from \$23.1M to \$44.8M and average APY declining from 47.8% to 33.8% as the staked base grew.

ZAMA STAKING PARTICIPATION: Q1 TO Q2 2026 (SELF-REPORTED)



Source: DefiLlama

