CASE STUDY | umbra

Umbra: Building the Bank Account of Crypto

How Umbra chose to become the self-custody bank account of crypto, built V2 and its own infrastructure around that position, and had its busiest month on record.

The Startup Blacksmith · 16 November 2026

UMBRA V2, THE FIRST MONTH

196 → 749	**$1.4M → $4.0M**	**+116%**
depositors, Sep to Oct V2 live 19 days of Oct	volume, Sep to Oct V2 live 19 days of Oct	TVL shielded 13 Oct launch to 12 Nov

Source: Umbra stats

> **The Startup Blacksmith**
>
> The Startup Blacksmith is a specialist strategy firm for crypto companies. With our clients, we build the strategy that accelerates their growth, so that they win in their market. This case study sets out Umbra Privacy's path to its V2, the decisions behind it, and the outcomes to date. Umbra developed the strategy behind V2 as a client of The Startup Blacksmith.

Summary

Umbra began as a hackathon project in 2025. Later that year its raise on MetaDAO drew $154.9M of commitments against a $3M cap. Its first product proved that people want private balances on a public chain.

In mid-2026 Umbra had to choose what to become. It chose a position we know of no other privacy product taking, the self-custody bank account of crypto, a private place to hold and transact from where the user keeps control of their assets, and built a new product and its own infrastructure around it.

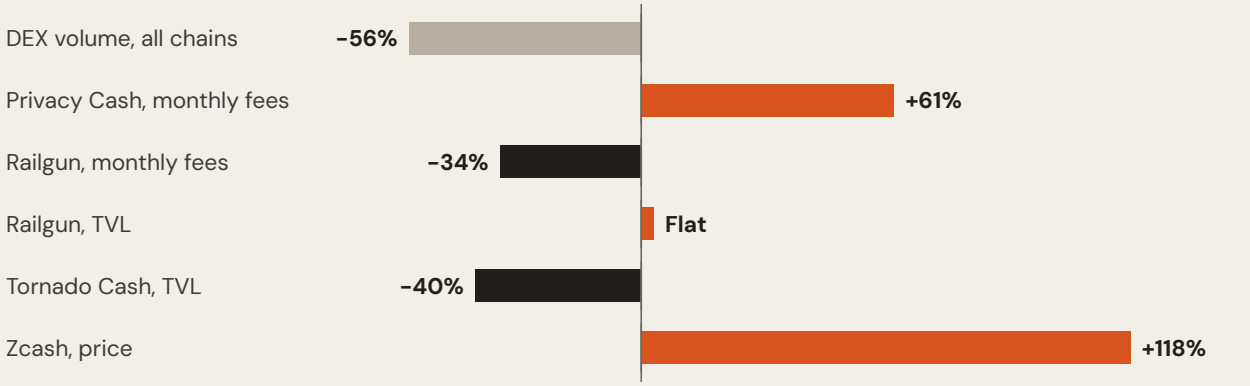
V2 launched on 13 October 2026, and October was Umbra's busiest month on record.

The privacy market, and what it has not yet built

Everything on a public chain is visible. Anyone a wallet has paid can read its whole history, what it holds, what it has invested in and who else it pays, in perpetuity. With individuals and companies now holding real wealth on chain, the problem is growing. CZ wrote in February 2026 that a lack of privacy "may [be] the missing link for crypto payments adoption", citing a company whose on-chain payroll shows what everyone is paid. An identifiable wallet is also a target. Chainalysis found that thefts from personal wallets rose from 7% of all crypto stolen in 2022 to 44% in 2024.

The market has noticed. Over the last twelve months trading volume on DEXs fell by more than half, while the winners in privacy grew. The products that lost ground were older ones, outcompeted in our view by newer products built for what users now need. Zcash, the largest privacy asset by market cap, more than doubled, and the first ETF to hold it passed $500M in assets within two weeks of launch.

Privacy's winners grew while the wider market halved



Measure	October 2025	October 2026	Change
DEX volume, all chains	$588B	$258B	Down 56%
Privacy Cash, monthly fees	$68,000	$109,000	Up 61%
Railgun, monthly fees	$523,000	$345,000	Down 34%
Railgun, TVL	$104M	$107M	Flat
Tornado Cash, TVL	$1.23B	$736M	Down 40%
Zama, TVL	None	$108M	New
Zcash, price	$523	$1,142	Up 118%

Sources: DefiLlama and CoinGecko. TVL and the Zcash price are 10 November figures in each year

Three kinds of product serve this demand, and each asks its users to give something up.

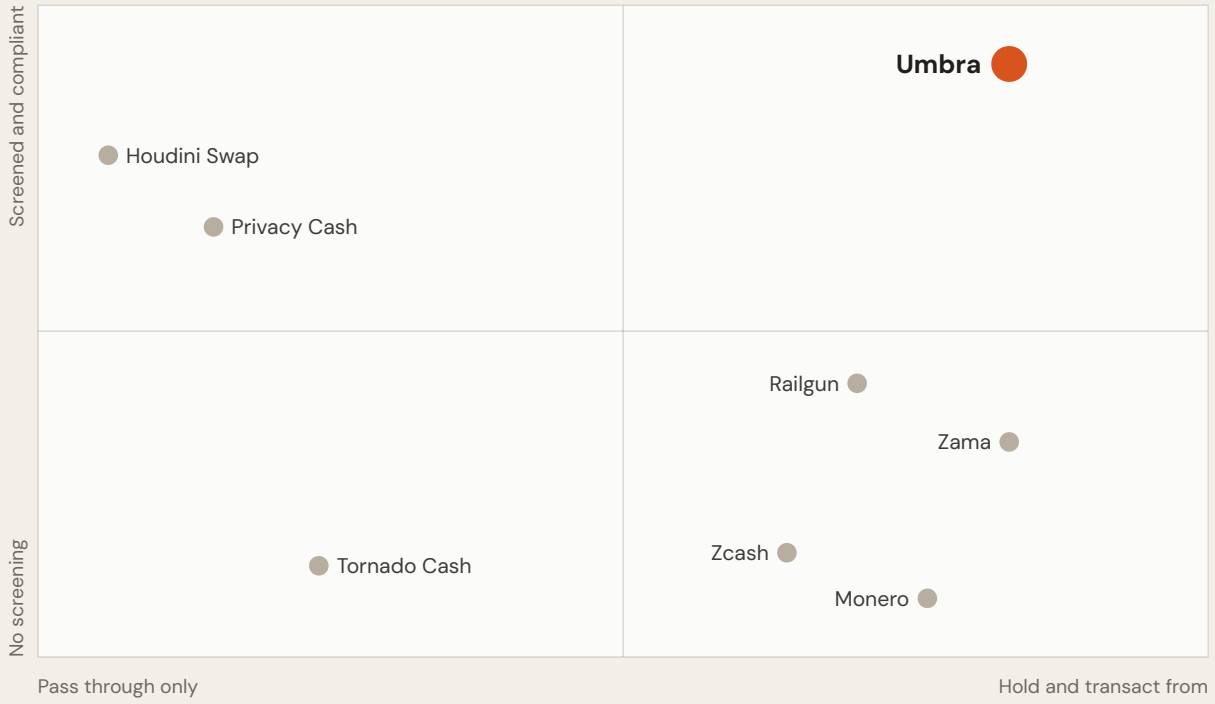
- **Privacy coins:** Zcash and Monero each keep one coin private. Everything else a holder uses sits on other chains, so using a privacy chain means bridging for every transaction. People bridge to move assets somewhere they mean to keep them, as traders do on Hyperliquid, and not each time they pay.
- **Pass-through tools:** Tornado Cash, Houdini Swap and Privacy Cash break the link between sender and receiver. Users arrive, transact and leave, and decide again each time who can see what.
- **Shielded balances on public chains:** Railgun and Zama let users hold privately on the chains where assets already sit, but in our view both carry friction for the user. Railgun needs a separate third-party wallet and holds every new deposit for an hour, and in practice is used mostly to transact. Zama wraps assets into new tokens that the rest of the market must then support.

Two lessons stand out. The first is that convenience wins. Houdini Swap, the market leader in compliant private swap, which our founder Josh Rogers led until early 2026, was expensive and slow compared with its peers, with a private swap taking 10 to 50 minutes. It still passed $3B in cumulative volume. Our founder's experience there, supported by users we have spoken to since, was that users stayed because the product was simple to use.

The second is that legitimacy is a deciding factor. Tornado Cash, the best-known mixer, does not screen its users, so its tokens carry that risk wherever they go next. While it was under sanctions, exchanges including OKX and dYdX blocked accounts that used it, and dYdX blocked users who had only received tokens that once passed through it. Its TVL has fallen 40% in a year.

What nobody had built was the everyday thing people use in traditional finance, the bank account. A bank account is one private, secure place to keep money and operate all of your finances from. That convenience is why almost everyone, everywhere, uses one. The trade-off is custody, because you must trust the bank with your money. Crypto had nothing with that convenience and functionality which was also self-custody.

The position nobody had taken



Privacy products by what they are built for and how they treat compliance. Placements are The Startup Blacksmith's judgement, not a measurement

Background to Umbra

Umbra was born out of the Solana Breakout hackathon, run online by Colosseum with the Solana Foundation from 14 April to 16 May 2025. More than 1,400 projects were submitted.

In October 2025 the team raised its funding through MetaDAO, where the treasury is governed by futarchy. About 10,500 investors committed $154.9M against a cap of $3M, about 50 times oversubscribed. The rest was returned.

The first product was built on Arcium, a third-party MPC network. In February 2026 Umbra became the first application live on Arcium's mainnet, opening to 100 new users a week. The public wallet followed on 27 March with shielded transfers, encrypted swaps and compliance screening.

The team then shipped quickly. Mobile apps, a browser extension and an SDK arrived in April, and more than 100 teams built on the SDK during Colosseum's next hackathon. In May Umbra launched private token vesting with Streamflow, and released a payroll tool as a beta to test the market.

By mid-2026 Umbra had proved the demand was real. People wanted private balances on Solana and developers wanted to build on them. It had also learned the limits of building on another company's network, since it could move only as fast, and offer only as much, as that network allowed. The team concluded that to scale it needed to own its infrastructure. What that infrastructure should be, and what it should be built to do, was still open.

The strategic question

Umbra had no shortage of options, and each was reasonable.

- A faster private transfer, since much of V1's activity was people moving funds through the pool and Umbra could build the quickest and cheapest way to do that.
- A payroll and payments product for crypto companies.
- An infrastructure company, selling privacy to wallets, exchanges and applications through its SDK.
- A consumer wallet for private holders.

Umbra had shipped something towards each. Going into July the team had four directions and no agreed way to choose between them. It saw its users' job as mostly transacting, and every feature it had built as important.

The choice mattered because an architecture decision depended on it. The four options need different systems. A faster transfer is built for speed through the pool. Payroll has to pay many people at once and give a company records it can audit. An infrastructure business means Umbra never sees the user. A place to hold assets needs a guarantee that funds can always be withdrawn. An architecture can only be judged against the position it serves, so choosing the architecture first would have chosen the position by default.

Umbra worked through that choice in July 2026, in a week with The Startup Blacksmith. The whole team took part, most of them in one room together for the first time.

We brought two things. The first was the discovery, our analysis before the team arrived of what worked in V1 and what did not, the architecture options Umbra could build, and the competitive market. That study of the market showed the position nobody had taken. Nothing in privacy offered the convenience and functionality of a bank account with self-custody of the user's assets.

The second was a process, built over Josh Rogers's 23 years as a CEO of high-growth technology companies, for taking a team from evidence to decisions in the right order. Define the job being done for the user, then the position it wins, then the architecture that delivers it. Everything else in the business is then built around those decisions, and together they form the strategy.

The team tested the bank account position, challenged it and made the decisions. By the end of the week Umbra had its position, its first user, the specification for its infrastructure, a decision on every feature and a roadmap to V2.

The first question answered was what Umbra's users are trying to get done.

Privacy is the means

People do not seek privacy for its own sake. Privacy has a job to do. The job the team arrived at is "manage my assets on chain, my own or my company's, with my identity, balances, counterparties and amounts kept private, and without the tool I use making me look suspect."

That last condition carries the tension that defines this market. The people with most to protect need privacy to protect their financial data yet are wary of privacy tools due to compliance concerns. A product that gives privacy and raises suspicion solves half the problem. The job is privacy that leaves its user knowing they are legitimate, and others knowing the same.

Managing, and not only transacting

The team first described the job as transacting privately. Through the work it widened. Managing assets privately includes holding them as well as moving them. That change of one verb is the centre of the strategy. The pass-through tools are built around the transfer, and nobody had built a convenient place for the transfer to start from.

The position

Umbra chose to become the self-custody bank account of crypto. The strategy statement, published on 6 August 2026, captures it. “Umbra is the sovereign safe haven for private wealth: a compliant, secure place to hold and transact where people’s critical financial data is always protected — and so earns the right to become the embedded privacy layer for internet capital markets.”

A position is defined as much by what it gives up as by what it claims. Umbra made four trade-offs.

- **Bank-level privacy, ahead of absolute anonymity:** A bank customer’s affairs are private from the public, competitors and colleagues, but not beyond the reach of a court. Umbra chose the same standard, leaving the argument about perfect anonymity to others.
- **Legitimate by design:** Umbra does not serve people hiding from lawful process. Every transaction is screened, and a user can prove where their funds came from. This costs Umbra the users who seek no record at all and gains the far larger group, legitimate users who wish to avoid any taint of illicit activity.
- **Holding as well as transacting:** The product is designed and priced for people who keep assets in it as well as transact. A tool built for the fastest single transfer would make different choices.
- **Self-custody:** Users keep control of their own assets. Umbra never holds them, which rules out the shortcuts a custodian could take.

In our view these trade-offs make the position hard to copy. A pass-through tool cannot become a safe haven by adding a feature, and a privacy coin cannot add compliance without losing the people who chose it for having none.

The position also reaches the user the market has served least. Someone holding significant assets on chain has had no good option, since privacy coins cannot hold the assets that person owns and pass-through tools protect a transaction and nothing after it.

Last, the position answers the problem every privacy pool has at the start. Privacy in a pool comes from the crowd inside it, and a pool that people only pass through stays thin however much volume it carries. Assets that stay deepen it for everyone, so a user who keeps a balance improves the pool for the next. The position and the economics point the same way.

The decisions, and how V2 delivers them

With the position chosen, each open question could be settled against it. Umbra announced V2 on 6 August 2026 and launched it on 13 October, on Nimbus, a zero-knowledge privacy network the team built itself.

> **"We were building on a network that was designed to do everything. Privacy for money needs infrastructure built for exactly that, so we built our own."**
>
> Kru Shah, CEO, Umbra

The first user

The team decided on the individual who holds enough to care. Someone holding $50,000 to $500,000, who knows crypto well and understands what a public ledger exposes, feels the problem every time they transact. Earning that user's trust takes properly built infrastructure, systems and processes. They were also the user Umbra could reach at launch, and the team expected them to point the way to those who would follow.

Three things that must be true

The team identified the three conditions its target users set before moving their assets anywhere, and they became the specification for the infrastructure.

1. **Self-custody:** A user can always withdraw their assets, whatever happens to Umbra. Funds move only with a proof generated in the user's own browser, and six independent signers approve each transaction without being able to take funds. If the network is unavailable, an escape hatch lets a user withdraw with their proof alone after a 48-hour delay.
2. **The system is compliant:** A transaction does not settle unless it has been screened, and each carries an encrypted record of its sender, with the keys split across three guardian nodes so that no single operator can read them. A user can prove their funds are clean to an exchange, an auditor or an authority, and lawful authorities can pursue bad actors.
3. **A user's tokens do not taint another's:** Screening at the door is the first protection. Zones, due before the end of 2026, are the second, isolating a holder's assets inside the pool under its own disclosure rules. This matters most to companies, treasuries and regulated organisations, the users expected to follow the first.

One pool that Umbra owns

With those decisions made, the architecture could be selected. The team tested its preferred design against the alternatives and settled on a single shielded pool that Umbra owns and runs. V1 gave each token its own pool. In V2 every deposit, transfer and withdrawal takes the same form on chain, so each user adds to everyone's privacy, and owning the pool gives Umbra control of its speed, fees and roadmap. Nimbus shields the tokens people already hold, and nothing is wrapped into a new version the market must adopt.

Swaps inside the pool take this further. A user who deposits 100 $USDC, swaps inside the pool and later withdraws $80 of $SOL leaves neither the same token nor the same amount to match. The protection has a limit while the pool is small. A deposit and a withdrawal that are both larger than the rest of the pool would be easy to pair. Privacy strengthens as deposits and transactions grow, so the limit fades as Umbra scales.

Convenience as the test

The product had to be simple enough that using it built trust. A deposit in V1 took 13 separate approvals, and in V2 it takes one. Umbra reports transfers settling in a few seconds and swaps in about 15 seconds.

Security

Notes use post-quantum encryption. Umbra has published more than 1,500 machine-checked proofs about its circuits, with its trust assumptions and known risks.

Focus

Umbra had built a multi-featured product in five months. The team went through every feature and confronted which to keep, bench or kill, by asking which created the most value for the first user. The private core stayed, which meant transfers, swaps, the web app, compliance and yield. The cross-chain bridge, the Android apps and the SDK were shut down, and the browser extension, the iOS app, referrals and rewards were put on hold. The most significant decision was to stop building on Arcium. As Kru Shah, Umbra's CEO, put it, "Never build a startup on top of another startup."

The position called for a new brand. V1's identity was playful, which suited a product born at a hackathon. It did not convey the technical depth of what Umbra was building, or the seriousness people expect from the place they keep their money. The team decided on a full rebrand, which went live on 6 October, so that Umbra would look like the company it had chosen to be.

Transact first, hold later

The team expected new users to transact before they left money in the pool. Trust is consistency over time, and nobody has it on the first day, so the plan was to earn deposits as that trust built.

Who would come next

The team expected crypto companies to follow individuals. Payroll looked like the clearest need, because no company wants staff seeing each other's pay, so it stayed in the product as a beta, a test of whether such companies would arrive. Beyond that, the same infrastructure could serve other products as the privacy layer beneath them.

What changed between V1 and V2

	V1, March 2026	V2, October 2026
Infrastructure	Built on a third-party network	Nimbus, Umbra's own network
Pools	One per token	One shared pool for every asset
Assets	Three at launch, six by June	More than 100 on Solana, about 80 on Robinhood Chain
Deposit	13 approvals	One approval
Compliance	Voluntary disclosure, screening in the app	Screening required for settlement, encrypted record in every transaction
Exit if the network stops	Depended on the network	Escape hatch with the user's proof alone
Fee	0.35%	0.1% on withdrawals, 0.05% on internal transfers, from 5 November
Chains	Solana	Solana and Robinhood Chain

Sources: Umbra and Nimbus documentation, Umbra's website, and Umbra's statements at launch

What V2 has shown

More people are depositing

Umbra's public statistics show October as its busiest month since V1 opened in March, with 749 depositors against 196 in September and a previous high of 577 in June. Monthly volume rose from $1.4M to $4.0M and transactions from about 8,000 to about 12,700. In the first month after launch, to 12 November, users shielded $1.91M and unshielded $1.66M in 11,719 transactions, a net inflow of about $250,000. Value shielded (TVL) stood at about $483,000 on 12 November, up 116% since launch, after a high of about $630,000.

Early signs match the first user the team decided on

Kru describes today's users as individuals holding about $50,000 to $1M. That is the user the team identified, with a higher ceiling.

Validators arrived

The companies that showed up first were not who the team had expected. Validators are coming to Umbra to receive and distribute their staking rewards. The tool first built for payroll now pays out their rewards.

Validators suit Umbra unusually well. Their rewards arrive as small amounts over a long period, so a later large transfer is very difficult to link back to those deposits. The same is true of anyone whose income arrives gradually, including stakers, yield earners and teams whose tokens vest over time.

Going cross-chain

Umbra went live on Robinhood Chain on 30 October, bringing privacy to tokenised stocks. Robinhood Chain is an EVM chain, and Umbra's cross-chain architecture was built so that it can be deployed to further EVM chains. That lets Umbra move quickly onto the other large chains that matter to a privacy user. Kru expects Elysium to go live very shortly, followed by Tron and Ethereum mainnet, with Hyperliquid under discussion for Q1 2027.

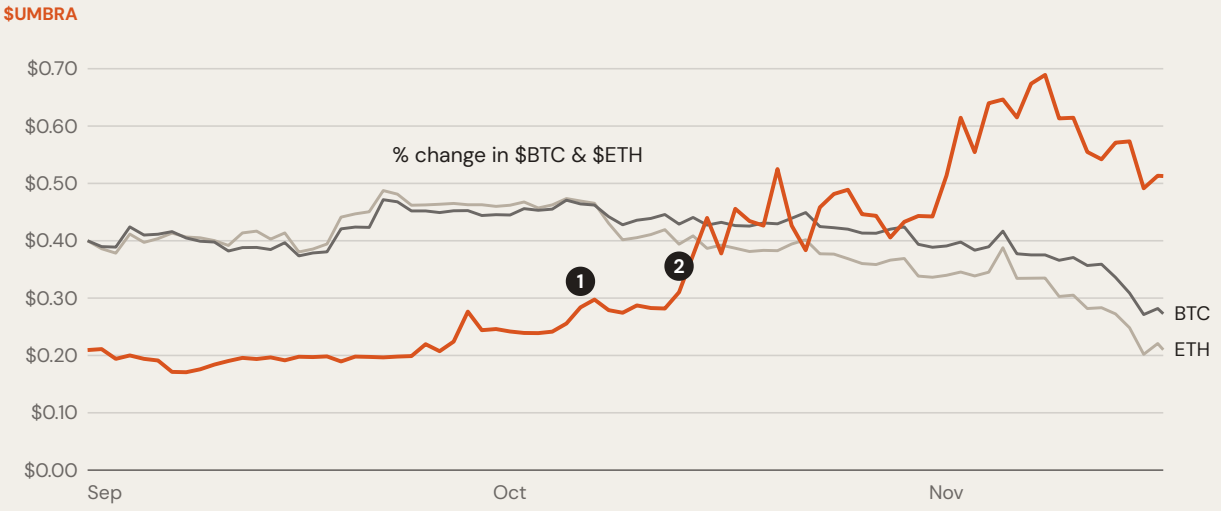
Lower fees

On 5 November Umbra cut its fees to 0.1% on withdrawals and 0.05% on transfers inside the pool. Moving within Umbra costs very little, which rewards those who stay.

The market's response

$UMBRA traded at about $0.17 in early September 2026. It began to rise after the team announced V2's impending launch, and again when the V2 waitlist opened on 6 October. By 16 November it stood at $0.51, three times its September low. Over the same weeks BTC fell 18% and ETH 27%.

$UMBRA up 3x from its September low while $BTC and $ETH fell



1 V2 waitlist opens, 6 Oct

2 V2 launches, 13 Oct

$UMBRA $USD. $BTC and $ETH % change in price. 1 Sep to 16 Nov 2026. Source: CoinGecko

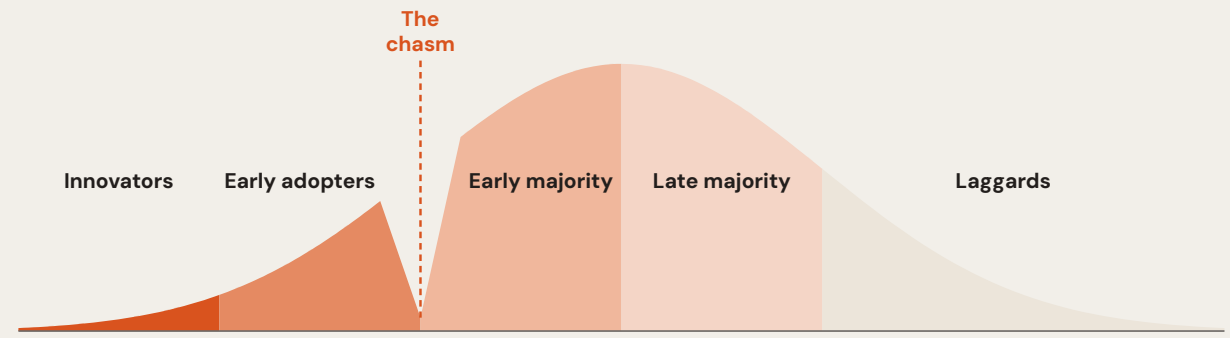
What one month does not show

Users are transacting through Umbra, with holding initially building slowly. TVL peaked at about $630,000, a small share of what its depositors own, and close to half of it is held in the UMBRA token. This early pattern is what the team expected. The metric to watch is TVL, the balances that stay. The audits and zones under way should build trust with validators and the companies that follow them, and support growth in TVL. As Kru put it, “In just one month, people have shown they want this. Now we’re focused on what comes next, helping their balances stay and grow with Umbra.”

What comes next

Umbra’s path follows the adoption curve, the pattern by which a new type of product spreads. Innovators come first and influence the early adopters, who give the early majority the confidence to try it. For Umbra the innovators were the individuals who understood the need, and validators and stakers look like the early adopters. The early majority is crypto companies and treasuries, and after them come institutions.

Who adopts Umbra, and in what order



Innovators	Individuals who understood the need
Early adopters	Validators and stakers
Early majority	Crypto companies and treasuries
Late majority	Institutions

Adapted from Rogers, *Diffusion of Innovations* (1962), and Moore, *Crossing the Chasm* (1991)

The work done and under way supports that path.

- **Zones:** Due before the end of 2026, zones let a company or a large holder keep its assets apart within the pool. They matter most to the firms and treasuries who come next.
- **Yield inside the pool:** Umbra has launched a private yield-bearing stablecoin, and holders will be able to earn without leaving. Private lending through existing lending markets is next, and Umbra is inviting more lending protocols to talk.
- **EVM deployment:** Live, so that Umbra is present where its users’ assets already sit.

- **Independent audits:** Audits of Nimbus, which Umbra's documentation describes as in progress.

We know of no other privacy product that makes holding as convenient as transacting. Kru describes Nimbus as the only privacy network that works across multiple chains and executes on the chain itself, with any DeFi primitive and with compliance built in.

What the position makes possible

Three things now work in Umbra's favour, and few projects have all of them.

The first is the position. Market leaders Aave, Uniswap and Jupiter are all non-custodial, each serves a very large market, and each won it through convenience and user trust. Umbra holds the equivalent position in privacy, and we know of no other product that has taken it.

The second is the sector. Privacy is one of the few parts of crypto growing while trading falls, and that demand is coming from people already on chain.

The third is the wider market. Umbra starts with a narrow first user, but its addressable market widens as the product builds out, potentially to everyone who holds crypto. As the on-chain economy grows, Umbra should grow with it.

A position is not a result. One month of V2 shows the first users arriving as the team expected. The team has built quickly to reach new users, with the move onto an EVM chain one example. These are first steps, and what follows depends on execution. We look forward to watching Umbra bring the opportunities its strategy affords to fruition.

In Umbra's words

Umbra wrote on 10 August 2026 that it was "the highest-leverage week in Umbra's history". Kru has said that the team learned that week the difference between a plan and a strategy, and that until that week it had been working from "just a plan".

> **"We came into the week with four products and a team that couldn't agree on which one mattered. Josh pushed us to find the one position nobody else in privacy had claimed and that we could genuinely own. By Friday, everyone on the team could explain Umbra in a single sentence, and we'd decided what to launch, what to drop, and in what order. That clarity would have taken us months on our own. It took a week."**
>
> Kru Shah, CEO, Umbra

Sources

Umbra, "Umbra V2: The Sovereign Chapter Begins", 6 August 2026, and "Private, and provably clean", 5 November 2026 (X).

Umbra, article on X, 10 August 2026.

Umbra public statistics, stats.umbraprivacy.com, read 10 and 12 November 2026.

Nimbus documentation, docs.nimbusprivacy.xyz, read 10 November 2026.

Interview with Kru Shah, Umbra CEO, 3 November 2026, and his written comments on this case study, 12 November 2026.

Colosseum, "Announcing the Winners of the Solana Breakout Hackathon", 2 July 2025.

The Block, coverage of Umbra's MetaDAO sale (10 October 2025), Arcium mainnet launch (2 February 2026), public wallet (27 March 2026) and Streamflow vesting (26 May 2026).

DefiLlama, protocol and exchange volume data, read 10 November 2026.

CoinGecko, $UMBRA, $SOL and $ZEC prices, read 10 November 2026.

Novora, "Umbra: The First Principles Approach to Privacy", 28 October 2026, for the Zcash figures.

SOL Strategies, results and updates on Houdini Swap, June to September 2026, and Houdini Swap analytics.

Step Data, "Privacy Cash: Over $121M in Private Transfers During Its First 100 Days".

Venable and Steptoe, notes on the Tornado Cash sanctions, 2025.

The Block, "Crypto hacks hit $3.4 billion in 2025, attacks on individual wallets rise: Chainalysis", 18 December 2025.

Grayscale, "The Zcash ETF (Ticker: ZCSH) Grows AUM to More Than $500 Million Following NYSE Arca Debut", 8 September 2026.

The Block, "OKX CEO reiterates accounts interacting with sanctioned entities will be blocked", August 2024, and CoinDesk, "Crypto Exchange dYdX Blocked Accounts That Received Even Small Amounts From Tornado Cash", 11 August 2022.

Infinex, "Private sends" support article, and Solana Compass, Houdini Swap profile, for private swap routing and timing.

CZ, post on X, 15 February 2026.

Ownership, "Ownership Report #14: Umbra V2, Private Payroll and the Next Era of On-chain Privacy", 8 August 2026.

Railgun documentation, "Getting Started", "Private Proofs of Innocence" and "RAILGUN Deductions", docs.railgun.org, read 12 November 2026.

DefiLlama, Railgun fees and TVL, read 12 November 2026.

Umbra V1 documentation, "Arcium MPC", read 10 November 2026.

Solana Compass, "How MetaDAO Became Solana's Breakout Token Launchpad", for MetaDAO's futarchy governance.

S&P Global, "The Engine of DeFi: Inside the Aave Crypto Lending Protocol", 13 October 2026.

Coinperps, "Uniswap Statistics and What the Fee Switch Changed", figures to 25 October 2026.

Crypto Briefing, "Jupiter holds top DEX aggregator spot for eighth straight quarter in Q3 2026".

The Startup Blacksmith is run by Josh Rogers, a CEO of high-growth technology companies for 23 years, who led Houdini Swap before founding the firm. An engagement begins with discovery and centres on one week in person with the client's whole team, followed by support with implementation. startupblacksmith.com