Comparing Enshroud with Aztec
21 April, 2025

The Enshroud dev team has been asked to what extent Aztec (the ZK-rollup project) represents competition for Enshroud. This is doubtless a fair question in view of Aztec's completed Series B fundraising round back in December 2022, in which they raised $100M for further development.

Our flip, knee-jerk answer would be to note that nothing repels a privacy user and advocate more than seeing phrases like "backed by a16z" and "update to our privacy policy." But the question does deserve a more substantive response, so here goes.

First we should note that regardless of how impressively Aztec is funded, that doesn't directly change the extent to which Aztec is competition for Enshroud (or competition for any other privacy project). The claim that they're building "an encrypted Ethereum" (as frequently stated in the media) is a wee bit disingenuous, in that nothing they're doing is adding any encryption to the Ethereum network *per se*. (For an example of a proposal for adding privacy to Ethereum at the protocol level, see this.) Instead Aztec is building an encrypted sidechain alongside Ethereum and providing API tools to bridge back and forth to/from mainnet.

There's some good info in their FAQ here:

https://docs.aztec.network/how-aztec-works/faq

which describes what they really do. Note also their Limitations page which describes where they really are at present (perhaps less impressive than expected given their funding level 3 years ago).

Theirs is a conceptually valid but significantly different approach from ours. Enshroud allows users to encrypt transactions on (unencrypted) Ethereum itself, without a true sidechain. Here's a bullet list of the top 10 competitive advantages re Aztec we think we'll have going forward:

1. **Decentralization**

   Aztec presently has only one transaction validator, run by Aztec. They claim other validators will be allowed in future, and *at that point* it will become decentralized. The plan called for decentralized *testnets* in 2024. But for now it appears to be completely centralized. Which is presumably how they can implement all of their value caps and IP tracking.

   Enshroud will be decentralized from release, in that we'll have multiple Layer 2 MVOs (Metadata Validator Oracles) run by different parties, as well as welcoming new independent MVO providers through our staking program.

2. **Chain Support**

   Aztec currently supports Ethereum only. They claim additional chains will be supported once "Aztec3" is eventually launched. (Whenever that occurs.)

   Enshroud will support as many EVM-compatible chains as there's demand for, beginning with Ethereum mainnet. We will of course prioritize our deployments in a sensible way. We are

currently (since Q1 ‘24) on testnet deployment on Sepolia, with Mainnet deployment imminent as soon as we can organize all the required logistics.

3. **Asset Support**

   Aztec initially supported zkETH, zkDAI, and zkstETH2 assets. No doubt they can add more in future. Note staked ETH2 does not appear to be spendable on their network, merely stakeable.

   Enshroud will support as many ERC20-compatible assets as there's demand for, and indeed will delegate to its users the ability to choose which tokens to deposit.

4. **User Compliance Tooling**

   Aztec provides "viewing keys" which allow read-only access to all (!) of an account's transactions. Since these keys correspond to the wallet keypair, this mechanism is evidently all-or-nothing. Give your viewing key to someone and they can forever see all your past, present, and future transactions. Therefore so could anyone else with whom that party might share your viewing key. How long until you must register your viewing key in order to use Aztec in certain contexts, such as spending to a hosted wallet?

   Enshroud provides encrypted receipts on a per-transaction basis, one for the payer and one for the payee. Users can choose to decrypt certain receipts upon demand for compliance purposes, thus providing certified details of a transaction. (Receipt details are attested to by the signature of the generating MVO as a neutral third party.) However, users can also delete their receipts at any time, just like throwing away a receipt for a purchase made with physical cash. There is simply no mechanism for revealing the set of all account transactions, short of the account owner producing every relevant historical receipt.

5. **Balance Confidentiality**

   Presumably, Aztec always knows your real account balance of every zk- asset type. It’s difficult to see how their value cap limitations would work otherwise.

   Enshroud (i.e. its MVOs, smart contracts, and Auditors) has no way to determine a current balance in any asset type, since your balance is simply the sum of a set of eNFTs (encrypted NFTs), which only you can decrypt.

6. **Ephermeral Keys**

   Aztec uses the same wallet keypair for all of your transactions. (This is how viewing keys can work.) This practice puts all of your privacy eggs into one basket.

   Enshroud generates unique AES keys for each eNFT and receipt, and these keys eventually get purged once the eNFTs have been burned, or the receipts are deleted by their owner. (Note too that input eNFTs are always burned in every transaction, much like UXTOs.) The wallet's private key is used only for signing requests involving the eNFTs and receipts that it owns.

7. **Naive Receiver Protection**

In Aztec's system, if you spend say zkDAI to a naive wallet (one which isn't registered with Aztec, i.e. has no account created on their sidechain), the payee receives DAI on Ethereum, with the sender being Aztec. So an unregistered payee gets an open, normal payment with no clear provenance. No encryption; and how is the recipient to know who sent this DAI?

In Enshroud's system, there is no concept of account registration. The payee user's wallet simply receives a normal (ERC-1155) eNFT. No one can see what that eNFT is for, DAI or otherwise. However the user can see who sent it to them by examining their receipt. (Or by performing some more complex tasks on Etherscan.) The sender can even provide a memo line in the encrypted data of the eNFT describing the payment. (Memo is also shown in the receipt.)

8. **Compliance Requirements**

Aztec operates as a mixing service, something like Tornado Cash. You deposit assets, wait until a reasonable anonymity set has accumulated, and then spend to other accounts. If you withdraw in clear to a naive account, best to use amounts that are non-unique and do not match your deposit. Withdrawals originate from the smart contract, breaking the on-chain link between sending and receiving accounts. This puts Aztec in a difficult spot re regulatory enforcement, and forces them to implement a bunch of limit caps and to track IP addresses, as described here:

https://docs.aztec.network/compliance

Enshroud is **not** a mixing service which breaks the on-chain links between sending and receiving accounts. It is therefore natively unsuitable for use by money launderers or other criminal actors. Enshroud is an anti-surveillance tool. While withdrawals do come from the smart contract's asset pool, you can only redeem (burn) eNFTs which you yourself already own. Accordingly Enshroud does not implement any amount limits, and does not track IP addresses. (In fact IP addresses are concealed from MVOs by HTTP proxies.)

9. **Revenue Model**

Aztec's revenue model appears mysterious. Fees charged are currently used to subsidize zk-rollup gas costs. It isn't clear where Aztec will make money. But once it is, it's a good bet that its revenue will flow to the VCs who provided the $100M in its latest funding round, plus its earlier $17M seed round funders. Users will pay fees and presumably earn nothing.

Enshroud's revenue model is clearly defined. Fees charged (on deposits and withdrawals, but not on spends) will be 95% remitted to users who stake $ENSHROUD. MVO operators also receive incentives. Post-launch crowdsale contract revenues go into the DAO Treasury, allocated to a specific list of disclosed uses. There is no liability or debt to VC investors because there are no VC investors. The idea for Enshroud is that system revenue flows to users and vendors who support privacy by using and supporting the protocol.

10. **Admin Vulnerabilities**

The Aztec protocol is governed by a centralized corporate structure. It can be sued, subpoenaed, served with search orders, required to obtain licenses, etc. Its large VC backing

and Series equity registrations guarantee that Aztec will always be a state-facing and fully compliant organization, and public statements made by their corporate officers always confirm this. It is therefore not only possible (due to the ZK-proof architecture) but highly likely (due to the corporate architecture) that a set of "superuser" admin keys exist which can de-anonymize any and all accounts and transactions on the Aztec network, upon any legally binding demand.

In any event, there's literally no reason to suppose that Aztec administrators will not have access to a copy of all the "viewing keys" created by users. For anyone serious about unconditional privacy, this factor alone should be sufficient to steer them away from Aztec's technology, no matter how many consulting math professors opine (probably for a donative) that ZK algorithms are oh-so-cool. They *are* cool, but usage context is everything.

The Enshroud protocol is governed by a decentralized DAO, not registered anywhere, and ultimately controlled (after an initial period of effective insider control) by a majority of $ENSHROUD token holders. There is thus no incentive to adopt policies which undermine or detract from the system's privacy guarantees. It is not possible for global admin keys to exist which can decrypt transactions or perform forensic analyses, because unique AES-256 keys are generated for each eNFT and receipt; and as noted above those keys are ephemeral.

Finally, we should note that these systems can also be synergistic. For example one could withdraw DAI from Aztec and deposit it into Enshroud, or vice-versa.

Thanks for reading!

– The Enshroud Dev Team