This is the mind map of the current plan to explore all possibilities with something like this.

It'll be powered by Intel's SGX or AMD's SEV, an encryption standard to encrypt User Data, IPFS for encrypted data storage and decryption key gen, management and reconstruction using Shamir secret sharing to ensure confidentiality and distributed access.

Brief overview : In house KYC implementation (which can be scaled up massively) with the priority of keeping sensitive user data safe. We first encrypt the data provided by the user for KYC, upload the encrypted data onto IPFS or similar decentralised file storage solutions.

Then we use SSS to split up the decryption key into secret shares which are to then distributed among the Off chain SGX or SEV nodes.

To retrieve the data, you need a clear mandate from (first among ?) equals and only after getting enough votes can you reconstruct the decryption keys to access the encrypted data stored on IPFS [inFavour >> Threshold]

## Here's how the process works : Basic Architecture

A high level overview of the system || At the User Level which happens all on the Backend

[

# 1

1024×1024 56.7 KB

](https://global.discourse-cdn.com/apecoin/original/2X/1/1c559bea5c6c2b3e04c132911954d7341b67c94b.png)

Same but with Extra Steps

|| Describes entire process

[

# 4

1024×1024 63.5 KB

](https://global.discourse-cdn.com/apecoin/original/2X/0/08ac7452bed86658ab5ba4611dbcaa127bfff5e4.png)

Secret Management, retrieval and Reconstruction

[

# 2

1024×1024 111 KB

](https://global.discourse-cdn.com/apecoin/original/2X/5/58374862c7cfc31ac20629094690abdebb143db0.png)

Just a dash of Terminology

[

# 3

1024×1024 35.5 KB

](https://global.discourse-cdn.com/apecoin/original/2X/d/d5d9155675019418358 54b967b2dbdf7454dd0a0.png)

Advantages :

Shamir secret sharing makes it Quantum resistant, Security W

At no point is sensitive info revealed in the process, Privacy W

With the introduction of clusters it can be scaled up massively to inc more communities, Scaling W

My confidence in the system : I’m tempted to store all of my personal information on here.

Scope for Improvement :

Although the way this system deals with privacy and consensus to achieve a majority mandate for data retrieval is a okay, There’s still significant room for improvement in the way the identity is verified.

And for that the most important thing will be familiarisation with the current KYC process. After taking inputs from that, we can ensure our stack will be rock solid

.

Show me the Incentive and I'll show you the outcome

Incentive is a very powerful tool which helps us shape human behaviour. Such is the case with disincentives. Disincentives can help us combat undesirable behaviour.

Disincentive → inaccurate Data gets you disqualified to participate in a role which requires KYC

Closing Statement :

While this tech has the ability to be re purposed for a variety of use cases, it still lacks in maturity in its current form (My proposal and not SGX, SEV or SSS).

For it to be all encompassing, It’ll need significant time and effort from across the DAO. It might or might not help us in the original solution (if for some reason it becomes impractical) but I’m sure this will help us pivot our approach and that tech could be repurposed.

It is too important to be left behind, without giving it a try.

There’s also Multi Party Computation which is a way to verify information in a trustless system which can be used as an alternative, Although I need to read up on this more.

If you found it interesting, or want to share your unfiltered feedback just drop me a message below.

Will keep this under discussion for some time until I clear my AIP backlog (Launching MVPs ahead of voting on AIP - 233)