Authored by @dan_tehrani and @lakshmansankar at @personae_labs

TL;DR:

This post examines the state of scaling non-financial decentralized applications and briefly discusses the consideration for a bespoke scaling solution that embraces such applications.

Although we use the “non-financial applications” to refer to applications that have certain properties, those properties might not strictly be “non-financial”; applications like voting could have properties similar to financial applications (e.g. ordering and nullifying) We will use the term “non-financial” for the sake of simplicity with an acknowledgment of its ambiguity.

Motivation

As in the broader blockchain space, the ethos “don’t trust verify”

should be followed when building non-financial applications

. This is because if we keep relying on centralized parties to uni-directionally present what information is valid and what is not, there will always be a possibility of being misled by manipulated information. For example, in decentralized social networks, users should be able to trustlessly verify that a post was signed by the claimed signer. Furthermore, trustless verification will enable developers to build applications without gaining users’ trust since users can verify the information by themselves, making it easier for developers to participate in serving a large user base.

Therefore, enabling information verification with light clients

for non-financial applications is crucial, as it is in financial applications like wallets.

In summary, the properties we want are:

1. Persistence
2. knowing that signature/proof verifications on the network will be available forever
3. Throughput
4. the rate at which new signatures can be added to the network, particularly important for e.g. social applications
5. Decentralization
6. lack of reliance on a centralized party to know the veracity of signature/proof verifications

Verifying signatures

Most decentralized applications rely on digital signatures to verify user actions. For example, a decentralized blogging platform might require bloggers to sign their blog posts, and a decentralized social network might require users to sign their posts.

However, from the perspective of end users of today’s ecosystem, there isn’t an easy way to know that the signatures are verified.

This is because signatures are not stored on-chain due to high fees, which means verification using light clients is not possible.

Verifying zero-knowledge proofs

There are certain kinds of apps that use zero-knowledge proofs to equip anonymity.

For example, Heyanon allows users to attest credibility to messages anonymously, which makes conversations regarding sensitive topics easier, allows anonymous whistle-blowing, and is likely to be valuable in many other situations as well.

Similar to signatures, zero-knowledge proofs need to be verified. And ideally, the verification should be decentralized (i.e. verifiable with light clients).

Solutions available today

For brevity, we provide examples with signatures, but “signatures” is interchangeable with “zero-knowledge proofs”.

Storing signatures on decentralized storage networks

Storing signatures on decentralized storage like IPFS or Arweave allows anyone to verify the validity of signatures, but such lazy verification is prone to DoS attacks.

Furthermore, in certain kinds of applications like voting or surveys, verifying a large number of signatures is required, making it impractical for end users to verify all information.

Therefore even if the signatures are stored on a decentralized storage network, signatures are usually verified by centralized servers and the end-users only have the option to trust that server, that the signature verification was executed correctly.

Rollups

Rollups relieve users from the high fees of L1s, but for non-financial applications, it is hard to compete with financial applications for block space.

Side chains/Validiums

Side chains and Validiums provide significantly higher scalability compared to rollups by compromising liveness.

In short, we think that side chains or Validiums are the most suitable for non-financial applications.

However, the above is not an exhaustive list of available solutions, so we will continue searching for alternatives that can embrace the requirements of non-financial applications.

Consideration for a bespoke solution

The different requirements of financial applications and non-financial applications

Non-financial applications operate under different assumptions when compared to financial applications. For instance, the followings don't exist in non-financial applications:

there are exceptions (e.g. voting)

- Double spending problem
- Miner-extractable value (MEV)

Given that difference in the underlying assumptions, it is worth considering a design for a scaling solution dedicated to non-financial applications that are credibly neutral and simple relative to designs involving financial transfers.

We will continue with a different post to discuss the possible design of such a system.