This post explores some scalability solutions called internal rollups and fractal sidechains.

1) A difficult goal : safe and cheap scalability

Many firms offer high scalability (Visa, Mastercard, banks, GAFAM, …).

They are very centralized, enabling them to offer low fees, but funds and accounts are not very safe, they can be frozen or seized easily. For example, it's common for social networks to ban accounts for any reason.

Cryptocurrencies emerged with Bitcoin, with the promise of keeping funds safer, thanks to decentralization and the blockchain technology, which prevents transaction reversal.

A huge milestone for cryptocurrencies is to increase scalability, while keeping funds relatively safe, and fees very low.

An approach called Validium is to introduce a centralized point to store data. It enables a huge improvement in scalability, but, in fact, funds are unsafe : "validium users can have their funds frozen and withdrawals restricted".

It means Validiums are not better than other centralized solutions. In fact, funds are safer with established firms like Visa, Mastercard, banks, GAFAM, ….

Cryptocurrency projects with excessive centralization meet the same problem, for example projects who rely on a small numbers of validators, which are usually managed by related actors.

To add value compared to centralized solutions, a scalable cryptocurrency project should be relatively decentralized and store data onchain, making it more difficult to seize and freeze funds.

2) Understanding the scalability gap

Centralized multinational corporations like Visa, Mastercard and GAFAM have around 1 or more billion daily users.

A very popular cryptocurrency ecosystem should be able to meet the demand of 200 million daily users, who would process a few daily transactions (utility token, gaming token, fan token, NFT, …). It means such a cryptocurrency ecosystem should be able to handle around 1 billion transactions a day (around 10 000 transactions per second).

Ethereum is currently processing around 1 million transactions per day (around 10 transactions per second).

It means the scalability gap is very huge : x 1 000

And scalability solutions should be very cheap : many centralized corporations like Instagram, Google and Twitter have a free business model : their use is free, but users have to watch an ad from time to time.

To become widely popular, a cryptocurrency ecosystem project should be free for most users. Typical users, especially young users, want to download an app, use it for free, and get an experience they like.

The use of a blockchain can be free only if fees are very low, around a few cents, because such fees can be covered by watching ads.

3) Can rollups reach this goal ?

Rollups are a technical solution to process transactions off-chain, to gather and compress transactions into a batch, and to post them on the main chain.

They enable a huge improvement in term of scalability. "Rollups promise to improve scalability up to 100x"

They are currently many ongoing projects to make rollups more efficient on the Ethereum blockchain.

Yet, they are some points to take care :

- rollups have to post on the main chain, and therefore pay the fees of the L1 chain, which is a barrier to cheap scalability, even if some proposals like EIP-4844 intend to “reduce gas fees on the network, especially for the rollup solutions”

- rollups are often external projects, they need to generate revenue to maintain and develop their infrastructure. As a result, fees are currently not so low

- to connect different rollups, bridges are needed, and are often vulnerable toattacks and exploits

- rollups often integrate some part of centralization, which reduces the safety of funds

Note that ZK rollups are better, because they introduce ZK proofs, which is better in terms of data availability and security.

4) Internal rollups

An interesting option to explore would be to create rollups secured by the same validators as the L1 chain

.

[

architecture2

770×369 40.2 KB

](https://ethresear.ch/uploads/default/original/2X/9/9aa80855866cc2566c18a9a19a85647aceda9d60.jpeg)

For example, there are currently approximately 450 000 Ethereum validators.

They could be used for additional tasks, for example validating not only L1 Ethereum, but also L2 “Official Ethereum Rollups”.

Each of the 450 000 Ethereum validators could be randomly assigned to one L2 Official Ethereum Rollup.

There would be many benefits :

- it would increase the security of bridges between L2 rollups. One major problem of current L2 is that bridges are secured by external validators : “Bridges secured by external validators are typically less secure than bridges that are locally or natively secured by the blockchain’s validators.”

- it would reduce some fees : for example, the cost of development would be shared between all the L2 Official Ethereum Rollups, because it is the same software. And the cost of validation could be very low, because validation on L2 Official Ethereum Rollups would just be a side task, an additional task assigned to Ethereum validators.

Note than rollups have limits : they are essentially an L2 solution, because “Data can be compressed once, but it cannot be compressed again”, so there are limits to rollup scalability. Putting “rollups on top of rollups” for scalability purposes is inefficient.

Therefore, it seems very difficult to fill a x 1 000 scalability gap using rollups, and it would be expensive.

The proposed solutions to fill such a scalability gap using rollups include :

- whether a sharding of the execution layer, for example “having a small number of execution shards” . But with sharding execution comes some risks, for example double spending attempts, looping problems, contradictory instructions …

- whether sharding only the data layer. But it means there will be a lot of pressure on the execution layer of the L1 chain, requiring even more expensive computers. It could be a barrier to achieve cheap scalability.

5) Fractal sidechains

A step further would be to introduce an alternative to rollups.

[

architecture3

807×587 83.4 KB

](https://ethresear.ch/uploads/default/original/2X/8/8257f7c038b9a63c8c56e09ccc4446cbd0434b30.jpeg)

If some L2 sidechains are secured by the same validators as the L1 chain

, it means transactions on L2 sidechains are quite safe. As a result, there is no need to roll-up transactions on the L1 chain

.

Security can be improved by requiring L2 Official sidechains to post Zk proofs on the L1 chain regularly. In this caseone single honest validator would be enough for each L2 Official internal sidechain.

There are currently approximately 450 000 Ethereum validators. In case there are 64 L2 internal sidechains, there would be around 7 000 validators for each L2 internal sidechain.

Finding an honest validator among 7 000 is easy.

This model is safe enough to put an L3 layer on top of the L2 layer, in order to gain another magnitude of scalability.

Each L3 Official internal sidechain could have around 7 000 / 64 = 100 validators.

Only one honest validator among the 100 would be needed to secure the model, because Zk proofs are very scalable : "SNARKs, can scale almost without limit; you really can just keep making "a SNARK of many SNARKs" to scale even more computation down to a single proof."

Once again, due to this security model (internal validators + Zk proofs)

, L3 sidechains don't have to roll-up transactions on L2 sidechains. L3 internal sidechains would just have to post Zk proofs on the L2 sidechains regularly.

The proposed model has further benefits compared to rollups :

- it would be possible to reach another level of scalability, with a gain of 64 x64 = 4 096, which is enough to fill the x 1 000 scalability gap. Even with 32 Official L2 internal sidechains and 32 Official L3 internal sidechains for each L2 sidechain, the scalability gap would be closed, because 32 x 32 = 1 024
- bridges between L2 and L3 sidechains would be processed by the same L1 validators, offeringmaximum security
- the L3 layer of scalability would be pretty cheap to secure, because posting Zk proofs on L2 sidechains isn't expensive
- this scalability level could be reached without putting too much pressure on the execution layer of the L1 chain. The entire model could be sustained by average computers, which makes scalability cheaper and is more in line with the goal of very low transaction fees.