

High-performance decentralized applications (dApps), such as games, often require a mixture of high-security/low interactivity with low-security/high interactivity.

For instance, during a game round, players may frequently interact with others (low-security, high-interactivity), leading to the minting of an NFT as a result (high security/low interactivity).

Posting all user low security low value game actions to the ZK rollup may slow down the game and affect its interactivity.

We propose a hybrid decentralized ZK sequencer,

which is a modular distributed ledger incorporating two chain IDs

- a Layer 2 ZK EVM chain rolled into ETH Main net
- a lower-security, high-speed fast chain (e.g., a Layer 3 chain).

The ledger will feature intermingled blocks from both chains while maintaining a global order of events.

Users will typically store their assets on the ZK chain but engage in complex interactions on the fast chain. With both chains running on the same ledger, quick transfers between chains are possible.

In case the fast chain is compromised, all users will lose is the value of assets currently transferred to the fast chains. In many cases this value can be close to zero, since the fast chain may need only proofs of ownership of the assets, instead of actual assets

Example: a game

- A user possesses an NFT that grants authentication access to the game.
- The NFT is stored on the ZK chain.
- The user will generate an ownership proof for the NFT and submit it to the fast chain, where all game interactions take place.
- After the game concludes, the user will send a game report to the ZK chain. This can result in minting of a new NFT based on this report. The new NFT can then be traded on a DeFi market hosted on the ZK chain.

Note in the example above, if the fast chain is compromised maximum what the user will lose is the gain made in the current round. The ZK chain can effectively limit damage done if the fast chain is compromised in a single game round by assigning a limit on NFTs minted in a particular game round.

By separating assets and high-activity tasks, users can benefit from high interactivity for low-security transactions while ensuring the security of assets and high-security tasks.