Project Ideas

<https://discord.com/channels/942318442340560917/944981401432915978/961650613509292043>

Some ideas on final projects for the infra stream:

\* Cloning https://github.com/nomad-xyz/nomad-monorepo and integrating other chains

\* Cloning https://github.com/harmony-one/ethhmy-bridge.sdk and integrating other chains

\* Integrating harmony spv bridge to other proof of work networks

\* Changing plumo's circuit to work on harmony's consensus (or another blockchain's consensus)

\* Developing some cryptographic pre-compiles (example described here https://github.com/celo-org/celo-proposals/issues/113. Don't do something that's already done here so dyor). Pre-compiles are implementations in solidity that have been pre-compiled into assembly (solidity is not the best assembly generator so you probably will need to edit some code in the pre-compile in order to make it efficient)

\* You can look for more ideas on improvement proposals for blockchain protocols like https://eips.ethereum.org/core https://github.com/celo-org/celo-proposals and <https://github.com/harmony-one/bounties/>

# ZK Message Board

Fully-decentralized message boards (i.e. a Reddit analog) that give mainstream users privacy and power over their data.

**ZK Mechanic**

Users can post messages anonymously, while using zkSNARKs to signal that they are credible (they have a certain reputation score, or they are a member of a certain group, etc.)

**One level deeper**

zkSNARKs allow us to theoretically build message boards with strong privacy guarantees, censorship-resistance, and expressive / granular reputation and credibility systems.

Using these constructions, anonymous whistleblowers can signal credibility ("This message is signed by me; I am a US Senator, but I won't reveal which US Senator I am" or "I am a user with at least 10m Twitter followers") without putting exact identity at risk.

In a message board with an associated upvote/downvote system, users can prove statements like "I am signing this message as someone whose posts have achieved at least X karma in the past, but I won't reveal who I am or which posts contribute to that score."

This enables online communities to separate signal from noise and to verify reputation or credibility, without requiring that a centralized party to store underlying user data.

**Progress**

* The Ethereum Foundation's applied ZK team has produced [Semaphore](https://semaphore.appliedzkp.org/), a set of primitives for anonymous signaling.
* Aayush Gupta and Nick Ulven from ETHUniversity have and [proof-of-concept demo](https://github.com/nulven/zk-polling) of a "ZK Confessions" application, similar in spirit to Semaphore. Writeup [here](https://docs.google.com/document/d/1rQqmqMJTe8eRO9hRMt79CvApJXvIv62ufwbU1LUNflk/edit).

**Open questions**

* UX: Current constructions require users to make multiple back-and-forth steps just to join a system or to post messages/proofs. This is a potentially unacceptable amount of friction for a social app.
* Execution environment: It is unclear if such a network should be completely on-chain—can we sacrifice censorship resistance or data availability for ease of use? For example, by building on a some network of broadcaster nodes in a p2p network, rather than a robustly-incentivized blockchain.
* Constructions: We don't yet have complete ZK constructions for some of the above primitives!