Zeko: Fractal scaling of ZK applications using a Shared Sequencer L2 Stack

Robert Kornacki
rob@milkomeda.com

Nicolas Arqueros
nico@milkomeda.com

Sebastien Guillemot
seba@milkomeda.com

Brandon Kase
bkase@o1labs.org

Florian Kluge
florian.kluge@o1labs.org

October 5, 2023

1 Introduction

With the latest innovations in the blockchain space pushing towards a rollup-dominant future, Mina has found itself to be positioned in an ideal place to capitalize on all of its upfront ZK work, but now in a new direction. At this point in time ZK Rollups have reached significant mind-share in the blockchain industry as the ideal scaling solution, yet due to the inherent complexity at play, are up till now a nascent and burgeoning field with no clear winner.

A ZK Rollup on top of Mina unlocks the best of what Mina's model has to offer while maintaining a competitive edge with the likes of Ethereum and other leading chains with growing L2 ecosystems. Furthermore, this project seeks to strengthen Mina's strong points by fulfilling the following goals:

- Increasing the throughput of Mina L1
- Unlocking new possibilities for dApps by offering a DA Layer as a part of the L2
- Implementing reusable rollup architecture that can be expanded upon by future innovative Rollups (both onto Mina and in the future to Ethereum as well)
- Improve UX by supporting faster block times at the L2 level

2 Motivation

Mina Protocol is a layer one blockchain that aims to be the privacy and security layer for web3 through utilization of zero knowledge proofs. Mina itself is powered by a multi-tiered recursive zkSNARK proof that in a small, constant, size (succinctness) stands in for the full blockchain. Developers write smart contracts on top of Mina by tapping into this proof layer: The zkApps protocol extends the potential of zero-knowledge cryptography by enabling the following characteristics while preserving the succinctness of Mina:

- **General programmability** - able to execute and settle arbitrary programs, not constrained to a particular VM model, but instead is flexibly designed to support any number of execution models, VM-like or otherwise
- **Programmable privacy** - the privacy of inputs to smart contracts and their state can be programmed by their developers
- **Constant verification time** - individual transactions are executed, or more accurately "proven", asynchronously off-chain and verified on-chain in time proportional to the account updates, independent of computational complexity of any individual proof inside of each account update.

Mina's recursive layer, Pickles, on top of its proof system, Kimchi, supports arbitrary infinite recursion with no trusted setup. This is the key to unlocking an isomorphic Mina L2 ZK Rollup as this paper describes. Moreover, recursion allows private computation to be broken up into pieces, even ones that