SuperNova

is a new recursive proof system for incrementally producing succinct proofs of the correct execution of programs on a stateful machine with a particular instruction set.

These seem to be fantastic features. This article will mainly interpret how these features are implemented.

Content

1. What is folding?
2. Represent computation with R1CS
3. Nova: NIVC for a single instruction
4. SuperNova: NIVC for multiple instructions(ZKVM)
5. Different with other Recursion

For details of this article, check out

Sin7y Tech Review (34): Is SuperNova's Folding Scheme the Endgame for ZK?

If you have any questions about SuperNova's Folding Scheme, please feel free to contact us at <contact@sin7y.org >. Welcome to follow Ola's official Twitter, join our Discord server, and get the latest updates from Ola!

About

This weekly report aims to provide an update on the latest developments and news related to Sin7y — Ola

and zero-knowledge cryptography

, which has the potential to revolutionize the way we approach privacy and security in the digital age. We will continue to monitor and report on the latest developments in this field. Please write to <contact@sin7y.org

if you'd like to join or partner with us.

Stay Tuned

Website | Whitepaper |GitHub | Twitter | Discord | LinkedIn | YouTube | HackMD | Medium | HackerNoon