P R E S S R E L E A S E

EMBARGO UNTIL 28TH MARCH 2023, 12 NOON UTC

ZeroSync Association launches to bring zero-knowledge proofs to Bitcoin, allowing the world to verify Bitcoin's chain state without having to download the blockchain. Furthermore, a new generation of Bitcoin applications is enabled with a toolkit for developers to apply proof systems to their individual use case.

Zug, Switzerland — 28th March 2023

Introducing the ZeroSync Association

The ZeroSync Association launches today in Zug, Switzerland, in a new initiative to bring zero-knowledge proofs to Bitcoin. For the very first time, Bitcoin users will be able to validate the state of the network without having to download the blockchain or trusting a third party.

Based in Zug, Switzerland, the ZeroSync Association is a new *Verein* established to develop and maintain open-source software enabling succinct zero-knowledge proofs (ZKPs) on the Bitcoin blockchain.

The work of Robin Linus Woll and his team has captured the excitement of all corners of the blockchain community:

> *"This is extremely exciting. We've shown the power of STARKs on Ethereum. Seeing them now deploying to Bitcoin is a logical next step. This could have a profound effect on how Bitcoin users interact with the network."*
>
> **— Uri Kolodny**, CEO and Co-Founder at StarkWare Industries

> *"ZeroSync is first of its kind in the Bitcoin space, compressing the chain and producing proofs about processing its state in a light client manner today and as a full node in the future, enabling new ways to interact with Bitcoin. It's an ambitious project which is led by a motivated and smart team that I had the luck to see take it from an idea that seemed extremely hard to a reality."*
>
> **— Kobi Gurkan**, Head of Research at Geometry

> *“ZeroSync is an amazing project tackling this design space.”*
>
> **— Olaoluwa Osuntokun**, CTO and Co-Founder at Lightning Labs

Zero-Knowledge Proofs

ZKPs promise a paradigm shift in blockchain scalability and privacy, allowing almost-fixed-size proofs to verify unboundedly large computations.

For the one-off cost of creating the proofs for each section of Bitcoin’s block history, anyone at any time in the future can check the validity of the state of Bitcoin they are looking at, without trusting third parties. This dramatically improves the decentralisation guarantees of the Bitcoin network.

Bringing ZKPs to Bitcoin for the First Time

While considerable engineering effort is underway in the Ethereum community to apply this technology, no similar investment has yet been made for the Bitcoin network.

Bitcoin’s relative simplicity and UTXO model present unique value propositions for recursive proofs. Most importantly, these features do not require consensus changes, nor do they introduce any additional trust assumptions.

ZeroSync is bringing this technology to Bitcoin for the first time, to strengthen its decentralisation guarantees for the future.

For Developers: The ZeroSync SDK

To give the world’s developers easy access to these proofs, ZeroSync is developing an SDK that allows developers with minimal domain expertise to generate custom validity proofs for their individual use case.

To kickstart this effort, ZeroSync is building a client for fast initial block download (IBD), and implementing the first full proof of Bitcoin consensus. This client can be used to sync a full node without making any code changes to Bitcoin Core.

Furthermore, the ZeroSync toolkit can be applied, for example, to compress the transaction histories of client-side validation protocols such as Taro or RGB, improving significantly both their scalability and privacy. Other ideas are to use the toolkit to improve the privacy of routing in the Lightning Network, or for Bitcoin exchanges and custodians to provide a proof of solvency.

ZeroSync are using the Cairo language to develop the first version of this software, as it remains best-in-class in terms of developer tooling and security for applications of this complexity. As developer tooling for other proving systems matures, they eventually plan to build out parallel implementations for different constructions.

The Technology Today

Significant progress has already been made by the ZeroSync team on making fast IBD a reality since the project was started in August 2022:

- ZeroSync can prove the validity of individual assumed valid blocks, which verify all Bitcoin rules except for the Scripts
- ZeroSync has implemented a recursive STARK verifier in Cairo, which allows to incrementally extend a chain proof with a next block proof
- The team has a working in-browser verifier for STARK proofs, demoing block proofs

This existing prototype is a strong proof of the technical feasibility. Now the project’s main focus becomes to enhance the system’s performance and then harden it for security.

The Roadmap

Moving forward: the team maintains a detailed roadmap for the project.

ZeroSync as a Public Good

The ZeroSync Association believes that its software stack should exist as a public good, without interference from incentives that could distort its core mission.

As such, ZeroSync is establishing a non-profit entity to steward its development and maintenance, and is assembling a diverse group of stakeholders within the Bitcoin community to help with this effort.

The project has so far been supported and funded by Geometry and StarkWare.

The Association Board & Core Contributors

The ZeroSync Association will be governed by a diverse board of individuals with a strong reputation in the field of Bitcoin research or proof systems.

Core contributors are:

- Robin Linus
- Tino Steffens
- Lukas George
- Max Gillett

Contributing partners:

- Lightning Labs: Develops Bitcoin's most popular Lightning client and, on top, the *Taro* protocol. To solve Taro's scalability, they intend to use ZeroSync to turn it into *zkTaro* with compressed transaction history proofs. Furthermore, they are planning to integrate ZeroSync into btcd, which is the second most used Bitcoin client next to Bitcoin Core.
- LambdaClass: Develops cairo-rs, a Cairo runner in Rust.
- Andrew Milson: Creator of *MiniSTARK*, a GPU-accelerated prover. This is key for generating proofs on consumer devices for use cases like zkTaro.

Advisory partners:

- StarkWare Industries
- Geometry

How to Support ZeroSync

You can contribute to ZeroSync in many ways:

- Code contributions
- Donations to the association
- Helping to manage our community
- Helping take our message to a wider audience

If you would like to be involved in the ZeroSync project in any capacity, please reach out at hello@zerosync.org.

Other Links

- ZeroSync website
- Geometry Notebook: Introduction to ZeroSync
- The ZeroSync GitHub repository
- Presentation about STARKs on Bitcoin at Starkware Sessions 2023
- Andrew Milson's talk on "Provers for Consumers" at StarkWare Sessions 2023
- Upcoming presentation at MIT Bitcoin Expo 2023