Introduction

Hi all!

I'm Daniel Marin, I work at Nexus Labs and was formerly a cryptography student at Stanford.

We are pleased to introduce Nexus to the Ethereum community, a decentralized cloud computing network designed to scale Ethereum's compute, storage and I/O capabilities. Nexus is an attempt to build a general-purpose platform for verifiable cloud computing, using zero-knowledge proofs, multi-party computation and state-machine-replication.

In particular, we are building:

- Nexus Zero: A decentralized verifiable cloud computing network powered by zero-knowledge proofs and a general-purpose zkVM.
- Nexus: A decentralized verifiable cloud computing network powered by multi-party computation, state-machine-replication and a general-purpose WASM VM.

In the Ethereum context, Nexus essentially functions as a serverless off-chain cloud computing network (similar to Google Cloud / AWS Lambda) that uses MPC/SMR and ZKPs to achieve verifiability. Nexus and Nexus Zero applications can be written in traditional programming languages, with starting support for Rust.

Both Nexus and Nexus Zero's execution layers are based on virtual machines with a traditional von Neumann architecture, which means that programs are executed within an environment that exposes memory, storage and I/O functionality (+ stack and heap) which allows traditional Rust programs to be ported as-is into the networks (except for evident required limitations, like determinism).

Verifiability Protocols

Nexus applications run in dedicated PoS-based decentralized cloud computing networks, which are essentially a form of general-purpose "serverless blockchains" connected directly to Ethereum. As such, Nexus applications do not

inherit Ethereum security, but in exchange achieve much higher computational capabilities (e.g. compute, storage and event-driven I/O) due to their reduced network size. Nexus applications run on a dedicated cloud which reaches internal consensus, and provides a "proof" (not a real

proof) of verifiable compute through network-wide threshold signatures verifiable within Ethereum.

[

Frame 117

1920×977 63.4 KB

](https://ethresear.ch/uploads/default/original/2X/1/1989ead6afce637cb07ebf7ae497b5e93bb34a7d.jpeg)

Nexus Zero applications do

inherit Ethereum security, as they are general-purpose programs accompanied by zero knowledge proofs (this time "real" proofs) which can be verified on-chain on the BN-254 elliptic curve.

[

Nexus Zero

1632×885 65.2 KB

](https://ethresear.ch/uploads/default/original/2X/a/a8b077dbdc431e7cc30b50f956ea4a7f4beb3ff5.png)

Nexus and Nexus Zero applications are compatible with any EVM-compatible execution layer. We expect Ethereum developers who wish to scale their applications with maximum security will use Nexus Zero as a source for off-chain compute, as it inherits Ethereum security, and we expect developers who are willing to sacrifice Ethereum security for increased computational capabilities to use a Nexus Cloud (of arbitrary size) as a source for off-chain compute, which allows them to remain in the Ethereum ecosystem (and not having to use, for instance, an application-specific blockchain like Cosmos).

Further, since Nexus is designed to run any deterministic WASM binary in a replicated setting, we expect that it will be used as a source of liveness / decentralization / fault-tolerance for proof-generating applications, including zk-rollup sequencers, optimistic rollup sequencers and other provers like Nexus Zero's zkVM itself.

TLDR

- We introduce Nexus Labs, a scientific organization dedicated to making Ethereum maximally useful.
- We introduce Nexus, a Decentralized Cloud Computing Network powered by multi-party computation, state-machine-replication and a general-purpose WASM-based VM.
- We introduce Nexus Zero, a decentralized zero-knowledge cloud computing network powered by a general-purpose zkVM.
- Formally, Nexus and Nexus Zero are our attempts at achieving verifiable cloud computing that can scale the computational, storage and I/O capabilities of Ethereum applications.
- Both Nexus and Nexus Zero applications are designed to support traditional programming languages like Rust.

About Us

We're based at Stanford, California and our team has experience building zk-rollups at zkSync, WASM VMs at Polkadot and doing cryptography research at Stanford. We are still in development, and plan to open-source our technology. We welcome feedback from the Ethereum community, and are actively hiring scientists and engineers. Please email us at hello@nexus.xyz if you'd like to learn more, collaborate, have suggestions or are interested in doing research with us.

FAQ

- How does Nexus / Nexus Zero compare to rollups?

Rollups are stateful off-chain scaling solutions which 1) inherit Ethereum's security and 2) "rollup" transactions on an off-chain state tree together. Nexus and Nexus Zero are decentralized application-specific general-purpose verifiable cloud computing networks that connect to any Ethereum-compatible execution layer. Nexus does not inherit Ethereum security (as Nexus Clouds have internal consensus) while Nexus Zero does (as its proofs can be verified on-chain). Both Nexus and Nexus Zero are designed to scale the compute, storage and I/O capabilities of individual Ethereum applications through an event-driven architecture, and not to provide a permissionless transaction-driven blockchain execution layer like rollups.

- Is Nexus stateless?

No, Nexus applications are stateful, whereas Nexus Zero applications are stateless. Nexus networks are essentially a form of externally-aware application-specific "serverless" blockchains, which support any stateful computation which changes state through external (Ethereum) events. Nexus Zero applications are currently just pure computations running on a general-purpose zkVM.

- Can you run an EVM on Nexus?

Theoretically, yes, as one simply needs to run an instance of the EVM that compiles to WASM, similar to NEAR's Aurora. This essentially enables developers to launch their own "serverless" EVM sidechains. However, I personally don't see any use for this if application-specific rollups are more widely adopted as they have superior security guarantees.

- How does Nexus / Nexus Zero compare to other non-rollup scalability solutions?

Truebit can be thought of a stateless verifiable cloud computing platform based on an optimistic (fraud-proof based) mechanism. Nexus Zero is a (currently) stateless verifiable cloud computing platform based on zero-knowledge proofs (validity-proof based). Nexus is a stateful verifiable cloud computing platform based on state-machine-replication and MPC.

- How do specific components work?

Check our research blog for high-level descriptions: https://research.nexus.xyz (more to come).