Zeeka

A Layer 1 Zero-knowledge proof blockchain

2022/06/05

L2 solutions, What's the problem now?

- Layer 2 Blockchain solutions will always be less decentralized and more vulnerable than the underlying Layer 1
- Receivers of transactions may be required to be online.
- Funds are locked in contracts. Those contracts are not free to enter or exit.
- Typically, they require trusting a centralized third party. Users can then prove that the centralized party is cheating, thus guaranteeing the network's security. You must be online to prove that the third party is cheating.
- Strange things can happen if the centralized party goes offline.

What can Zeeka Network bring?

Make zero-knowledge available to all web3 users

Focus on Scalability, speed, efficiency and security, With Zero-Knowledge proofs at its core.

Introduce Zero Contract written in Rank-1 Constraint System, which allows Smart Contracts to be evaluated using Zero-Knowledge proof systems.

The implementation of Zero Knowledge by Zeeka will change the way Blockchain is used in every sector.

Built from the ground up to support Zero Knowledge applications

Faster

- constant sized proofs reduce computation complexity
- enabling enhanced efficiency
- large transactions per second

No Gas

- no gas fees - the verification time of all contract calls is equal
- transaction fees are expected to be much lower

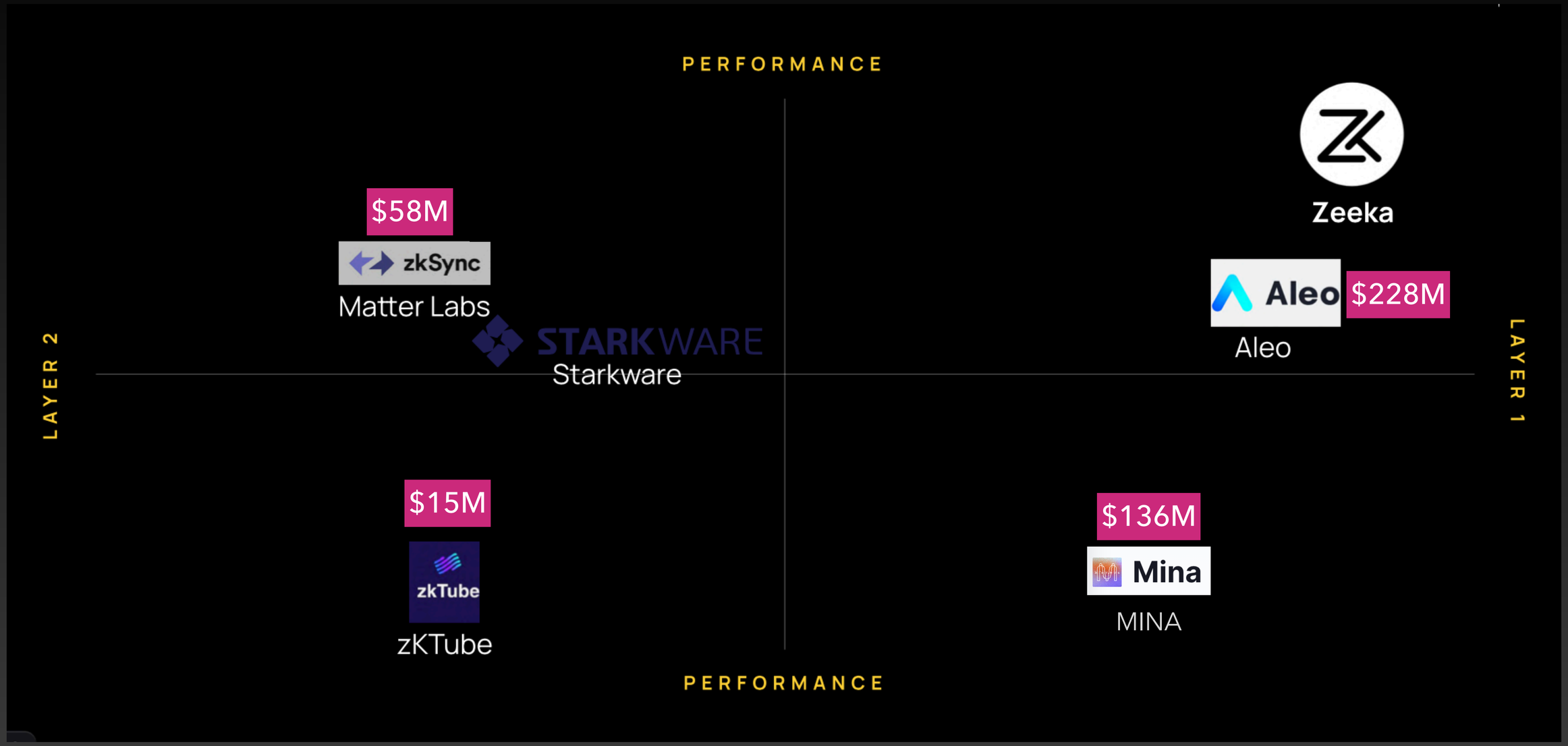
Secure

- data availability issues are eliminated through decentralization

Better solution

- With Zero-Knowledge proofs at its core, Zeeka can process an impressive number of transactions per second without compromising block size.
- Zeeka does not enforce a constant-sized blockchain (like MINA protocol), but it still offers all of the benefits of ZK technology.
- Smart contract execution is moved off-chain bringing scale, transactional and efficiency gains.
- Privacy, scalability, throughput and flexibility are all enhanced on Zeeka with Zero Contracts

Competitors landscape



Zeeka

- Layer 1 network, more decentralized
- Introduce Zero Contract written in Rank-1 Constraint System, can directly process data
- Better security, improved efficiency, higher throughput and lower fees

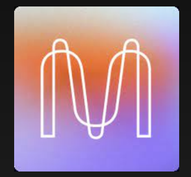
vs

zkRollups

- Only trade and cannot programming
- Invisible to the data of the L1 network
- More centralized

Zeeka

VS



- Zero contract execution is moved off-chain bringing scale, transactional and efficiency gains.
- Current zero-knowledge proof reaches 1500 TPS

- The MINA protocol uses Zero-Knowledge proof recursion to provide a constant-sized blockchain.
- TPS is very low, currently only 22

Zeeka

- Focusing on public applications in which transitions are succinct.
- Decentralized database and verifier of decentralized applications, in which everybody is able to generate proofs for every application.
- Use Python as main dev language, which using a widely known language is much better for our dev community.
- Using more popular and well-tested proof systems (E.g Groth16).

vs

Aleo

- Focusing on private applications
- Aleo is a decentralized verifier of private applications, proved by centralized entities.
- Providing a new tech stack for dev (Leo programming language)
- Focusing on bleeding edge tech which has not been experimented enough yet.

Team

Founder

Peter

Has been deeply involved in blockchain since 2016.
Very passionate about zero-knowledge proof, and has made some achievements in Filecoin mining by optimizing zero-knowledge proof technology.

Core dev

Bastian Götze

Used to be a SDR who work for world class cloud company, like AliCloud, AWS.
Having rich experience about CDN-Network, machine learning and distributed database over 5 years.
Also as a passionate open source developer who made some contribution to ETH, Filecoin.
He has made some achievements in Zero-Knowledge proof technology.
Optimizing performance for many algorithm include PLONK, Groth16 and so on.

Tech advisor

Keyvan

Big fan of Zero-Knowledge proof technology.
At FinalityLabs, he is research on Ethereum L2 scaling solutions and implemented Pinocchio zkSNARK.
Help Filecoin project to make their storage provers faster by accelerating a zkSNARK library called bellman using GPUs.

Roadmap

2022 Q2

- Using Rust and libp2p, implement a minimal Proof-of-Work cryptocurrency. Create a very simple cryptocurrency that supports nothing more than regular payments. Make sure the software is thoroughly tested, to serve as a foundation for further development in the future.
- Implement a Zero Contract development ecosystem (using existing circuit compilers like Circom or Cairo or design a new one). After this stage, platform developers should easily be able to develop zk applications.
- Decide how contracts will be stored on the blockchain, whether as a set of instructions describing the SNARK circuit or a set of verification keys. In addition, determine how the blockchain state will be connected to contract circuits and how they can interact with one another.

Q3

- Develop the Main Payment Network contract using the circuit development kit. The output should be a SNARK circuit, which can handle billions of accounts and takes O(n) time to generate a proof. The circuit should contain a fee, as an incentive, for the one who executes it.
- The PoS cryptocurrency we created earlier will now have the functionality of contract creation and contract updates. We should be able to upload the Main Payment Network contract onto the chain (using the Genesis Block), create contracts through transactions, and update their states using zk-proofs.
- Design an appropriate wallet for the system. Although the wallet should prefer to transact through the Main Payment Network, it should also be able to create regular L1 transactions.

Q4

- Finalize the wallet.
- Support the creation of custom fungible/ non-fungible tokens, and integrate them into the Main Payment Network.
- Develop use cases outside of payments. (Games, exchanges, auctions)

2023

- Launch testnet.
- Improve SNARK prover performance (using GPUs?). Possibly start a SNARK competition for different Executors to compete against each other.
- Start auditing and awarding grants and bug bounties.
- Launch mainnet

Zeeka

Contact

peter@zeeka.io