ZK Application Landscape

Lakshman Sankar - Personae Labs

Yi Sun - AXIOM

What is the goal of this talk?

‘ZK’ is becoming more of an opaque buzzword every day

We hope to make sense of the ZK application landscape today and in the near future

In the process, introduce some more nuanced language for talking about applications

Succinctness vs. Privacy requirements seem like the right lens for understanding the application landscape today

Succinctness vs. Privacy

	Not Succinct	Succinct
Private	Off-chain	On-chain but HARD
Not Private	On-chain	

Succinctness vs. Privacy

	Not Succinct	Succinct
Private	zkML (zKonduit) semaphore unirep heyanon zk-email	ZCash Tornado Cash
Not Private	zkRollups dYdX Axiom	

Today’s Capabilities

Succinct but not Private

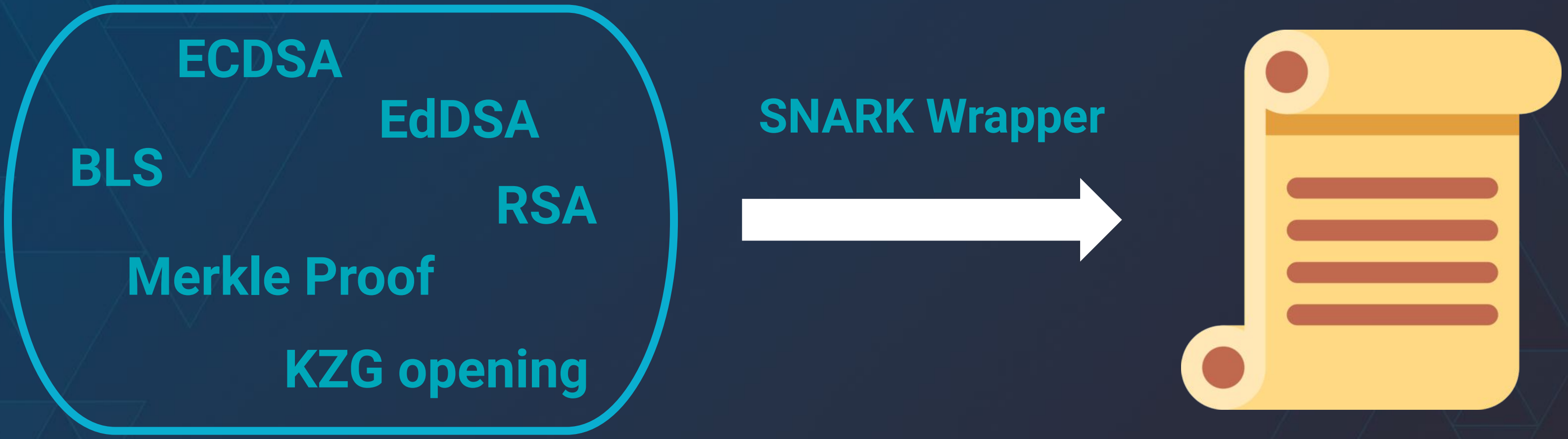
	Not Succinct	Succinct
Private	semaphore zkML (zKonduit) unirep heyanon zk-email	ZCash Tornado Cash
Not Private	zkRollups dYdX Axiom	

ZK scales trustless off-chain compute

~100K Full Nodes
Validate Computation
High Duplication

One Prover Generates
Validity Proof
High Overhead

ZK enables cryptographic interoperability



ECDSA

EdDSA

BLS

RSA

Merkle Proof

KZG opening

SNARK Wrapper

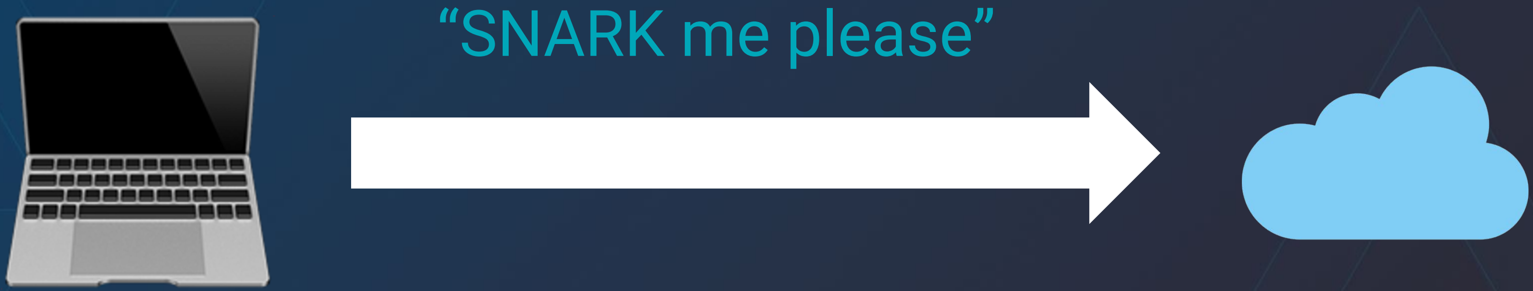
Single Purpose Crypto Primitive

Custom Aggregation / Composition

SNARK Proof

Arbitrarily Composable

ZK for on-chain Infrastructure: Scaling Proving

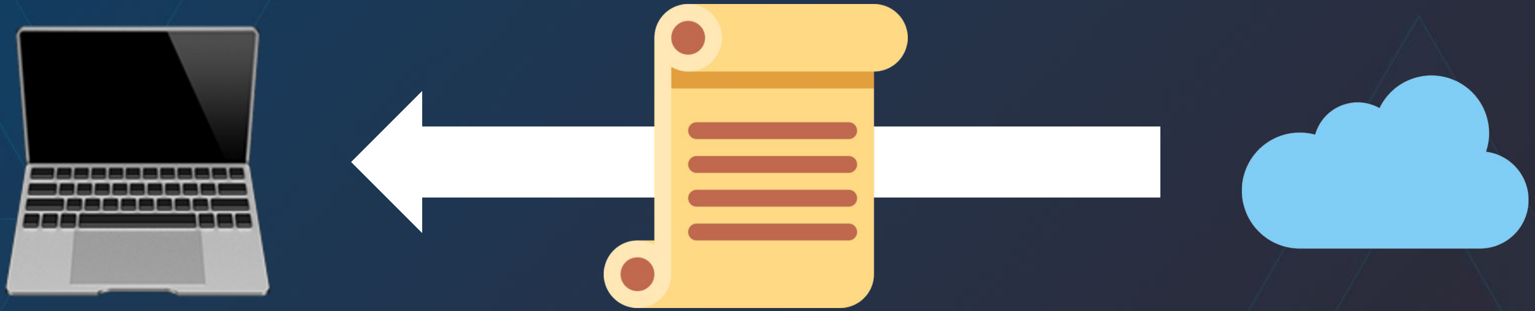


“SNARK me please”

Bare metal proving

5-10x faster than browser

ZK for on-chain Infrastructure: Scaling Proving



Cloud Proving

Large server / GPU / FPGA / ASIC

Another **5-10x** speedup

ZK for on-chain Infrastructure: On-chain Verification

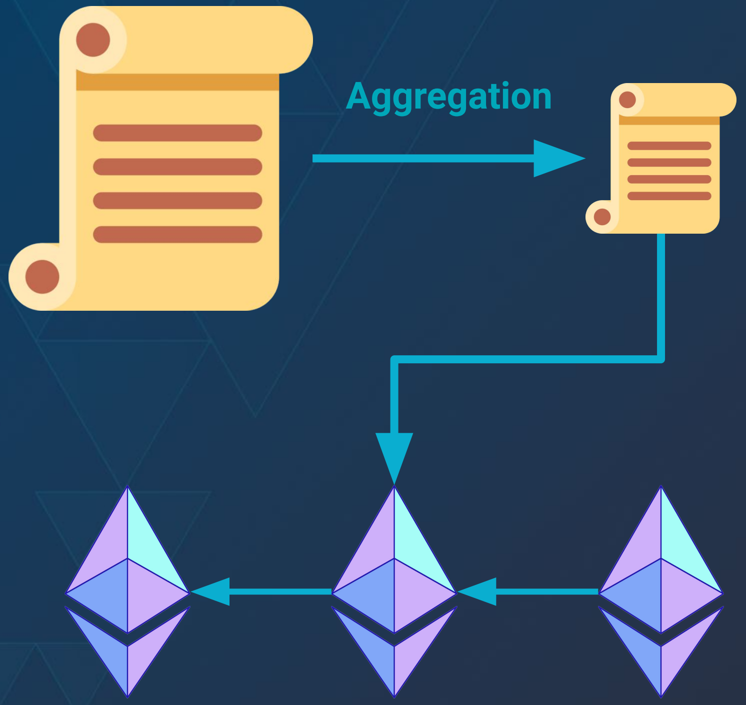
Gas cost **differs** from CPU cost! Depends on:

- Choice of proving system
- Choice of curve
- Proving-system specific choices

Choice of curve is restrictive:

- **Precompiles** make BN254 operations much cheaper
- Other curves are prohibitive in EVM

ZK for on-chain Infrastructure: Aggregation



For SNARK **A** not natively compatible with EVM:

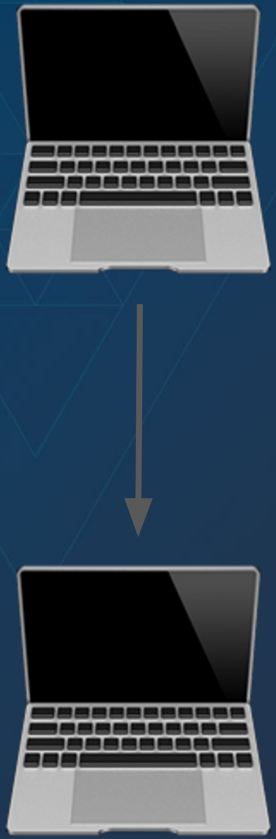
- Verify **A** inside another SNARK **B**
- This means **B** proves:

"I know a SNARK A which verifies against the verification key for my statement."

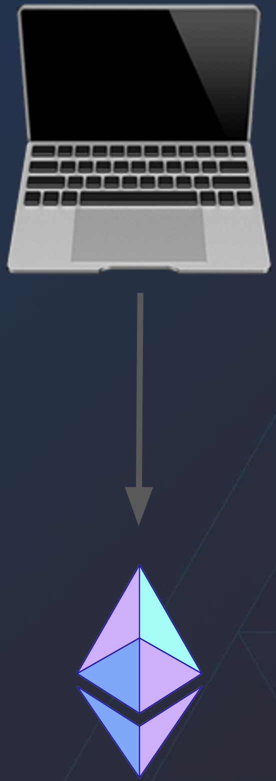
- For any **A**, can choose **B** to be a cheap-to-verify SNARK.
- Incurs **recursion overhead**

Private but not Succinct

	Not Succinct	Succinct
Private	semaphore zkML (zKonduit) unirep heyanon zk-email	ZCash Tornado Cash
Not Private	zkRollups dYdX Axiom	



vs.



human ‘consumption’ vs. chain ‘consumption’

Humans	Chains
higher velocity	composable
ephemeral (i.e. social)	canonical

ZKPs for enriching existing content

+
SOUNDCLOUD

Different requirements relative to succinct-zk

1. verification complexity < proving complexity

2. ‘consumer device’ proving friendliness

3. respect for sensitive user information

The Challenges Ahead

ZK for Privacy

1. performance in resource constrained environments

2. deterministic, non-privkey nullifiers for consistent pseudonyms

3. more cryptosystems representable in SNARKs
    - I.e. anywhere interesting identity is forming

ZK for Infrastructure: Optimizing Aggregation and Recursion

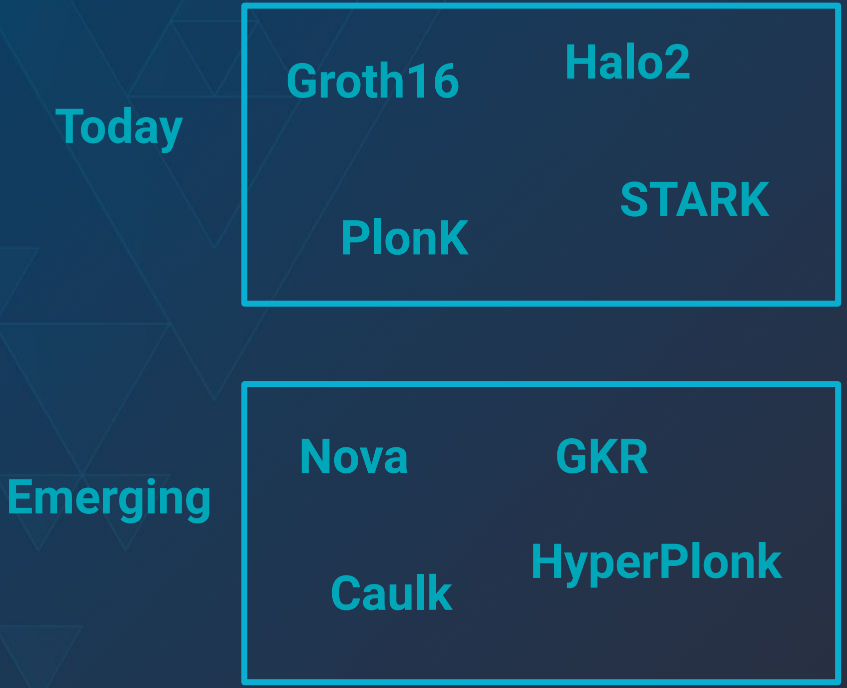
Richer applications need proofs for **bigger circuits**:

- Maximize **prover-verifier** tradeoff (arithmetization design)
- Use **multiple aggregation layers**
- Optimize **non-native arithmetic** and **elliptic curve operations**

The most interesting statements will require **multiple circuits**:

- Divide up a big computation with **recursive verification**
- Allows **virtual machine** operation (zkRollups are just the beginning)

ZK for Infrastructure: Exploring New Proof Systems



Today

Groth16

Halo2

PlonK

STARK

Emerging

Nova

GKR

Caulk

HyperPlonk

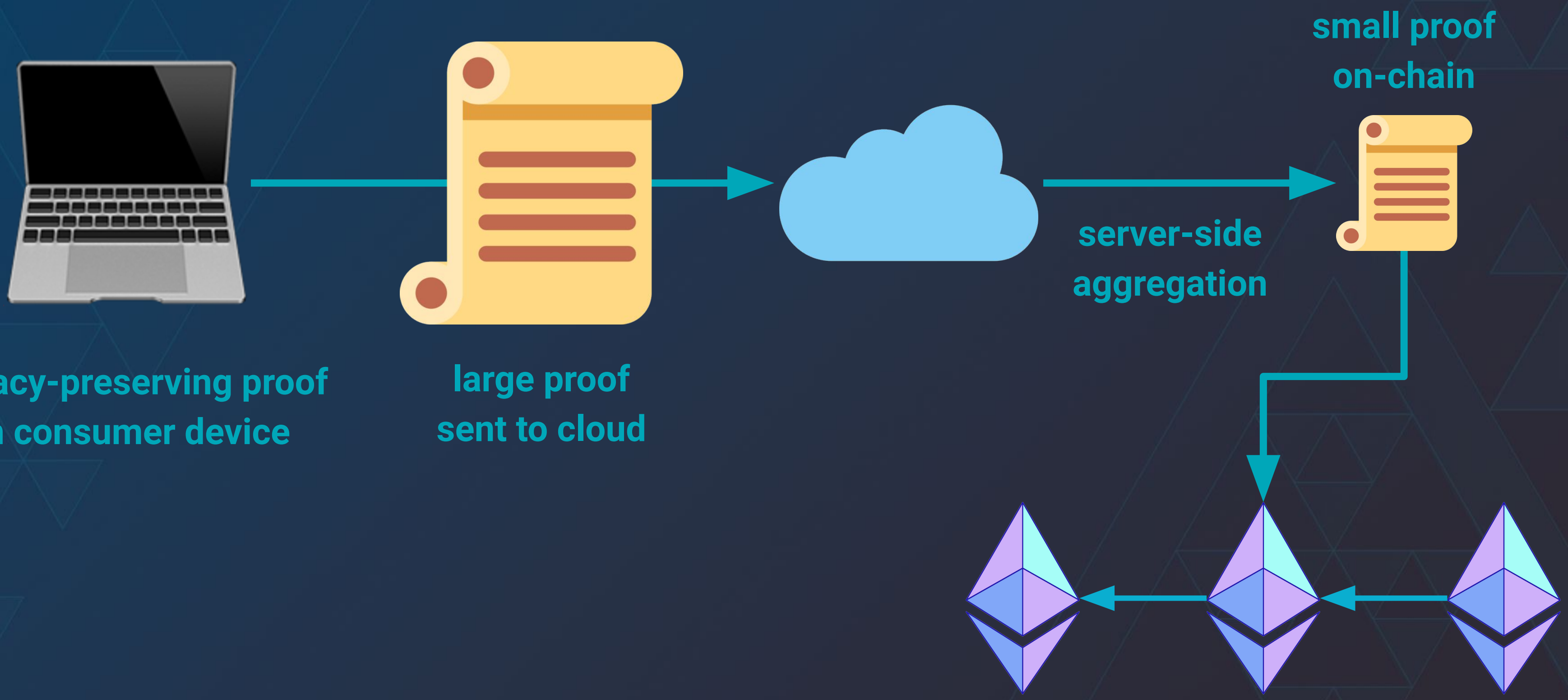
Proof systems have advanced massively in the last 5 years.

- Added **custom gates, lookups**
- Removed **some trusted setups**

New advances are coming fast

- More efficient **accumulation**
- Fast and large proofs
- More efficient lookups

Recursion will bring us together



Privacy-preserving proof on consumer device

large proof sent to cloud

server-side aggregation

small proof on-chain

Thank you!

Lakshman Sankar
Personae Labs
@lakshmansankar

Yi Sun
AXIOM
@theyisun