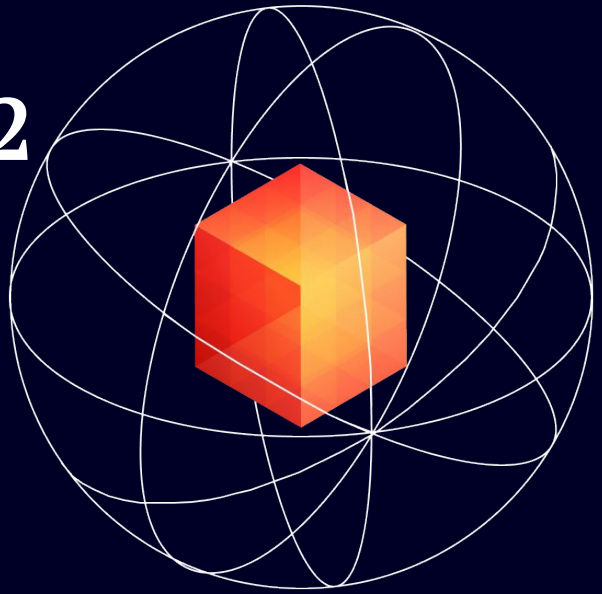
STARKWARE

Building a Future-Proof L2

What should you look for when choosing one?

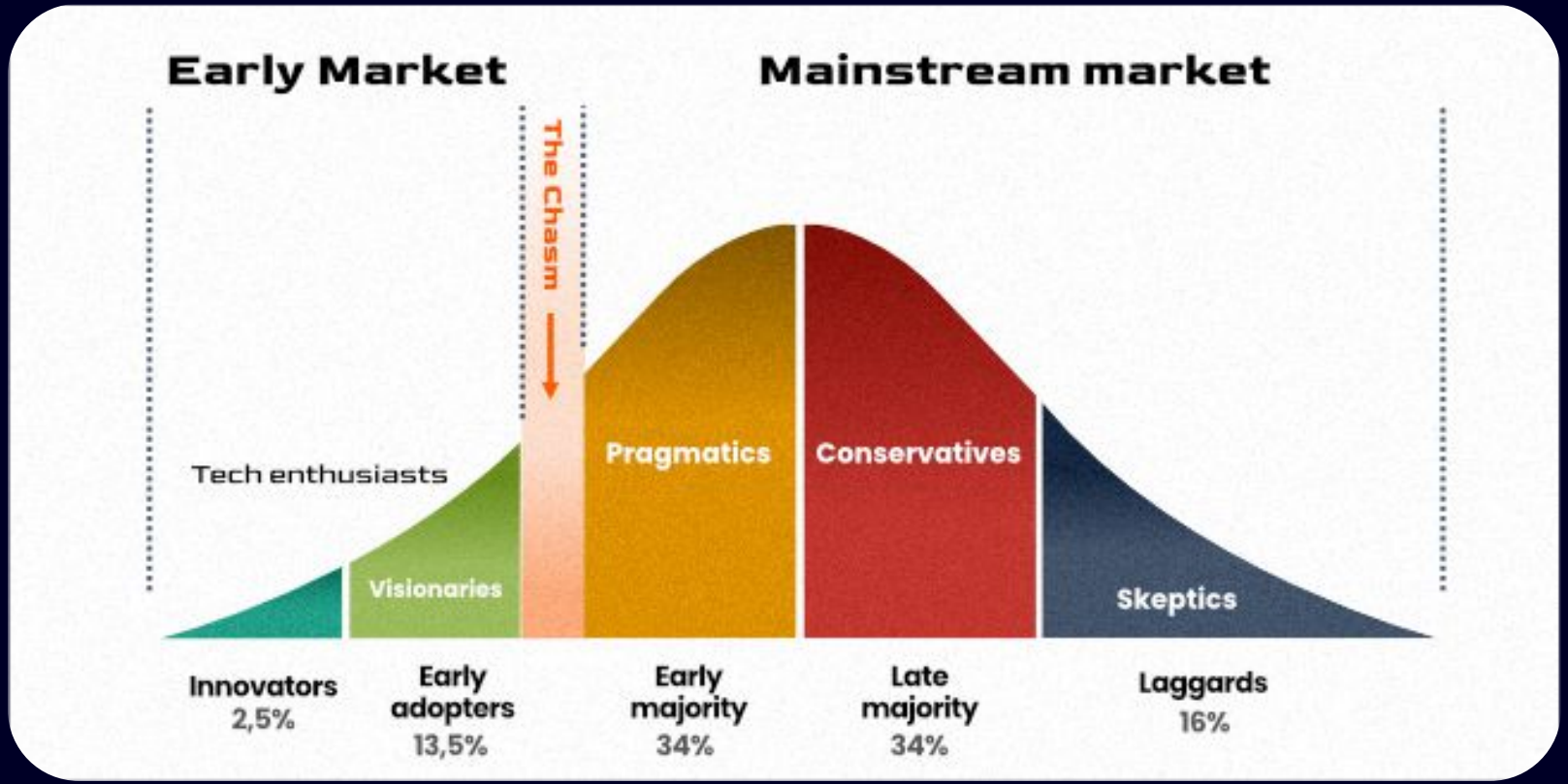


Oren Katz, COO

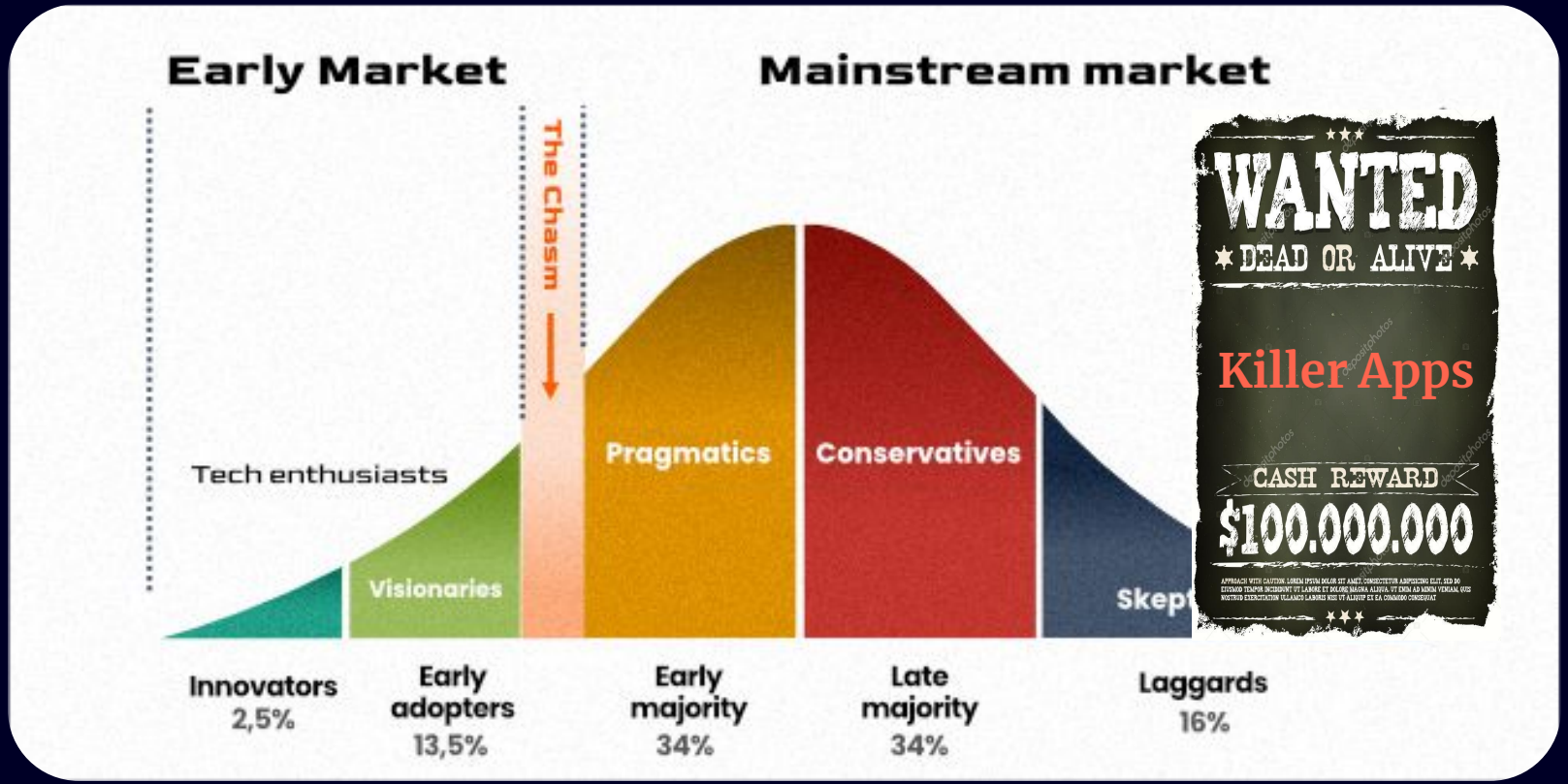
Outline

- Web3 today
- Types of networks
  - L1s, L2s
  - Validity Rollups, Optimistic Rollups
  - Public chains, Appchains
- What’s Important in a chain?
  - Technology & Infrastructure
  - Vision, Values & Community

Where is Web3 Today?



Where is Web3 Today?



L1s vs L2s

L1

Secure

Decentralized, Neutral

Strong networks

L1s vs L2s

L1

Secure

Decentralized, Neutral

Strong networks

Scale

Cost

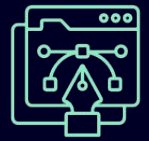
UX

L1s vs L2s

Alt L1

Scale

Cost



UX

L1s vs L2s

Secure

Decentralized, Neutral

Strong networks

Alt L1

Scale

Cost

UX

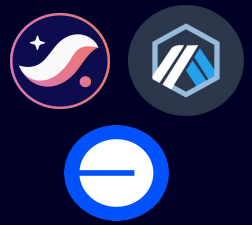
L1s vs L2s

L2

Scale

Cost

UX



L1s vs L2s

L1

Secure

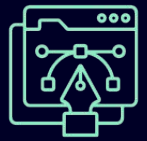
Decentralized, Neutral

Strong networks

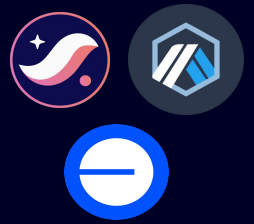
L2

Scale

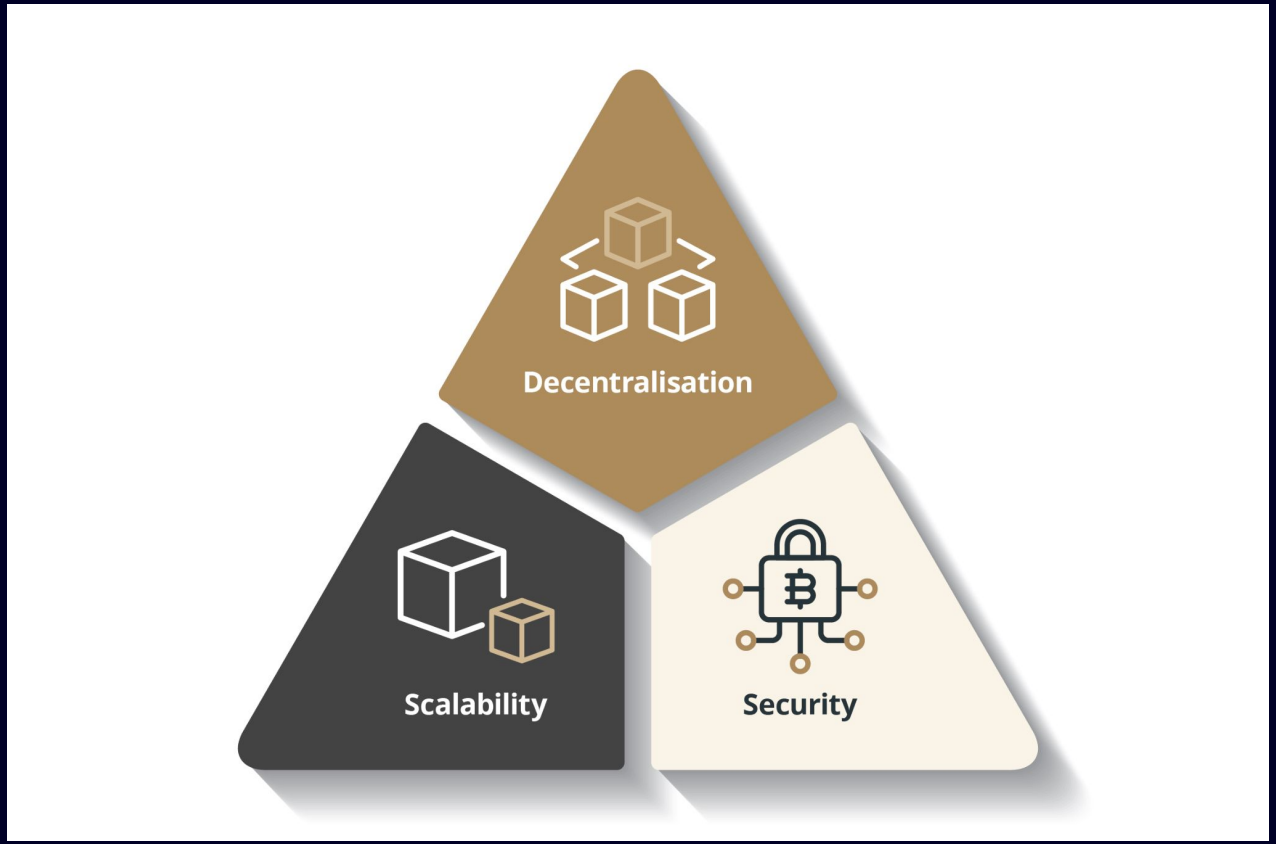
Cost



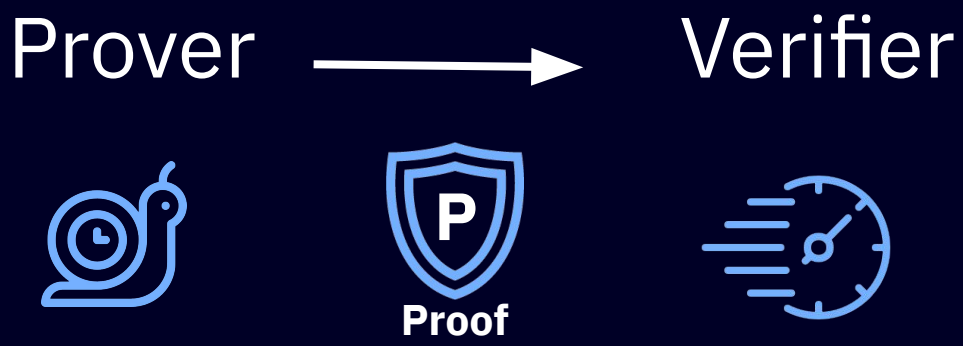
UX



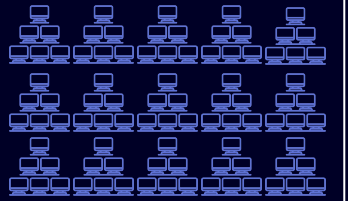
The Blockchain Trilemma



What are Validity (aka ZK) Rollups?



What are Validity (aka ZK) Rollups

	Without Proofs	With Proofs
Sequencer **(miner, validator)** 	Execute all Txs	Execute all Txs Generate Proof
All nodes 	Execute all Txs	Verify Proof

Public Chains vs Appchains

Wen Public Chain?


Composability


Leverage network effects


Lower touch (for the app)

Public Chains vs Appchains

Wen Public Chain?


Composability


Leverage network effects


Lower touch (for the app)

Wen Appchain?


Control

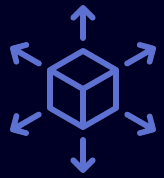

Capturing network revenue


Branding & distribution

What's Important in a Chain - Infra ?

Strong tech

Security



Scalability

Cost

Expressibility

Nobody Cares About Security

Security

And Yet...

Cryptography?

Field-proven?

What damage can the operator(s) do?

Decentralized?

Cost of attack?

Security

And Yet...

- Cryptograph
- Field-prove
- What dam
- Decentra
- Cost of attack?

STARKWARE

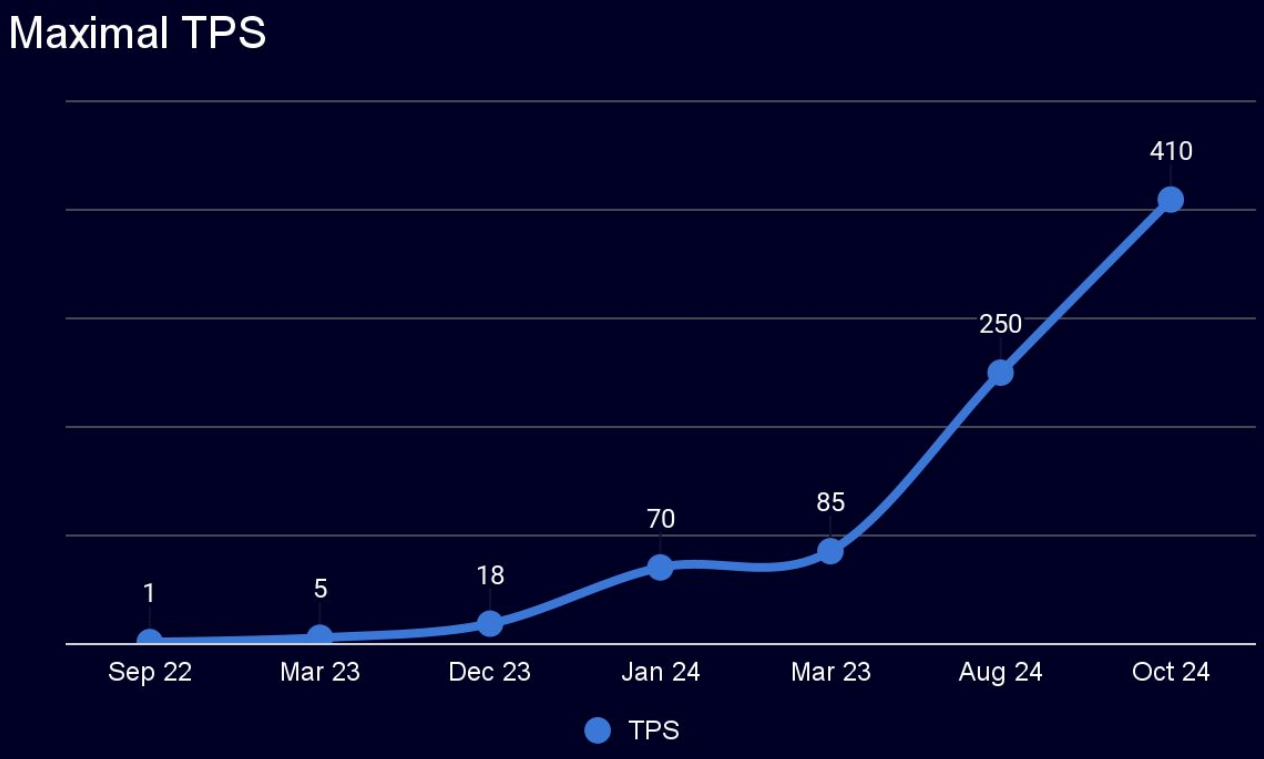
What Limits the Throughput?

	L1	Validity Rollup	Optimistic Rollup
Execution	All nodes	Consensus nodes	All nodes
Consensus	Consensus nodes	Consensus nodes	Consensus nodes
Data	Full on L1	State diffs on L1	Txs on L1
Proving	None	Doesn’t limit	None

Unless compromising security

Scalability

STARKNET - Throughput Increasing



Scalability

What Drives the Costs?

	L1	Validity Rollup	Optimistic Rollup
Execution	All nodes	Consensus nodes	All nodes
Consensus	Consensus nodes	Consensus nodes	Consensus nodes
Data	Full on L1	State diffs on L1	Txs on L1
Proving	None	Single node	None

Unless compromising security

STARKWARE

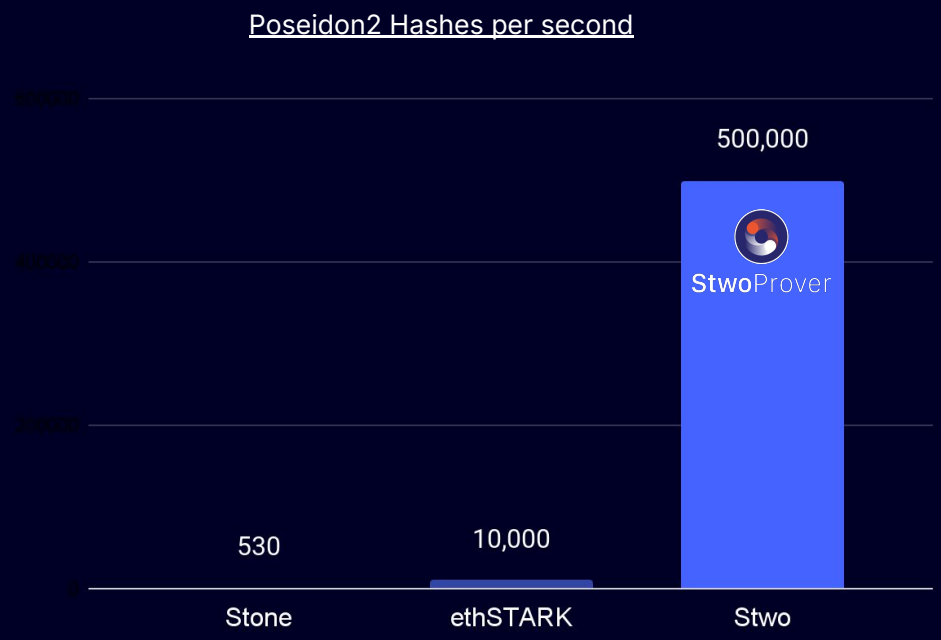
STARKNET - Cost Decreasing

Cost

Proving Stack - Performance

Cost

Proving Stack - Performance



- Stwo
- ethSTARK（*Rescue)
- Stone

- Reduces cost
- Opens new possibilities (e.g. client-side proving)

Cost

STARKNET - Expressibility

Native Account Abstraction

Cairo
Rust-like programming language

Volition
(multiple DA options)

Privacy

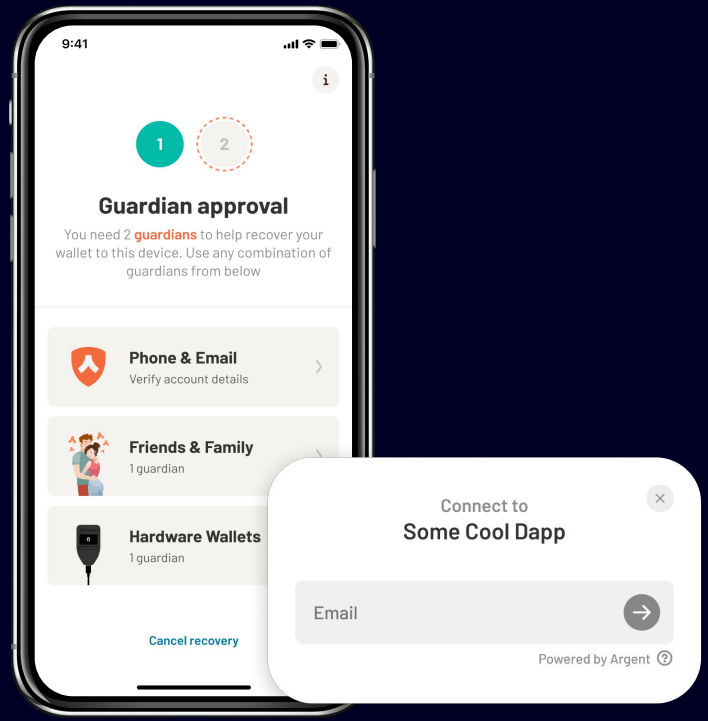
✨ Opens new possibilities for apps

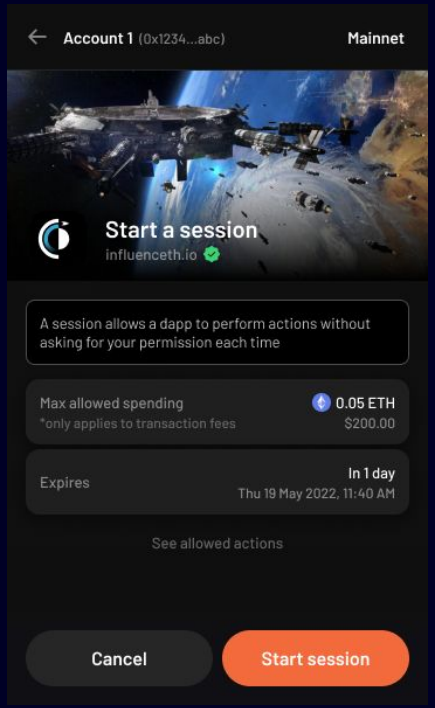
Argent - 2FA, Gaming Sessions, Infinite Approvals

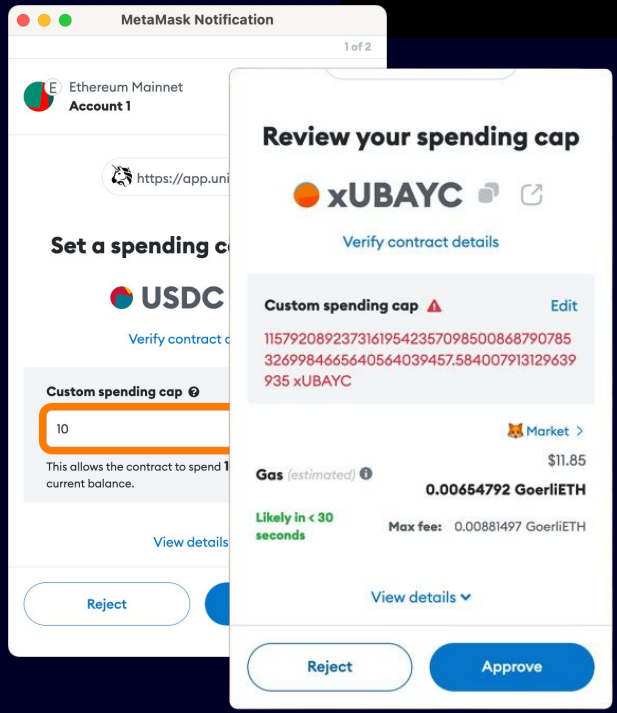
STARKWARE

Argent X

StarkNet browser wallet

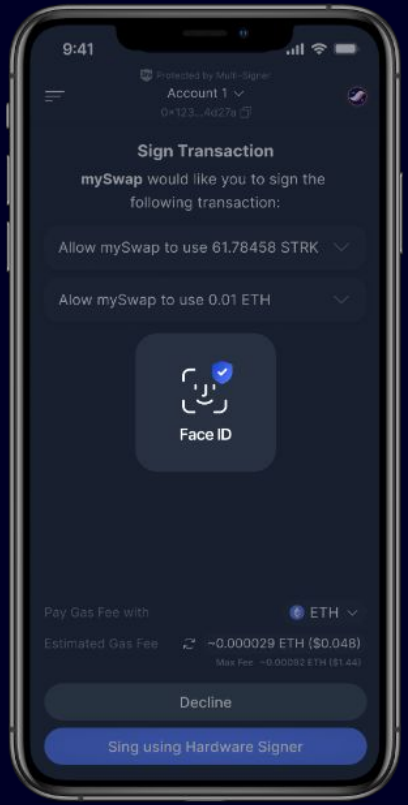


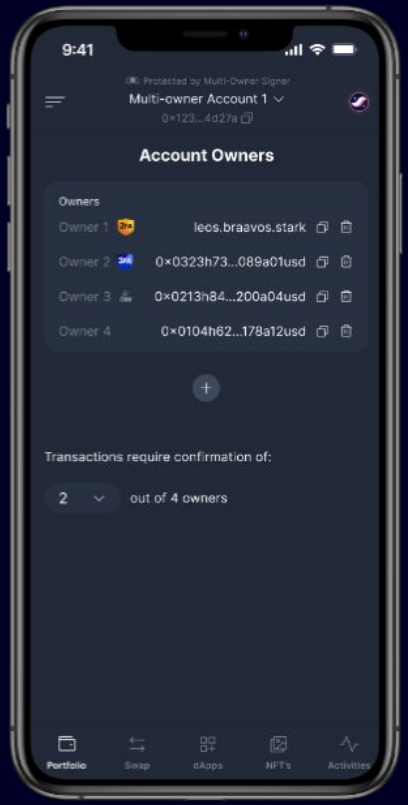


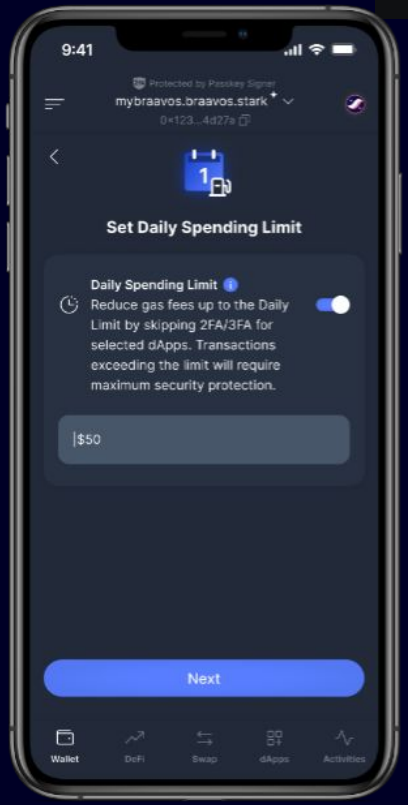


Expressibility

Braavos - Face ID, Multi-Owner Account, Spending Limit



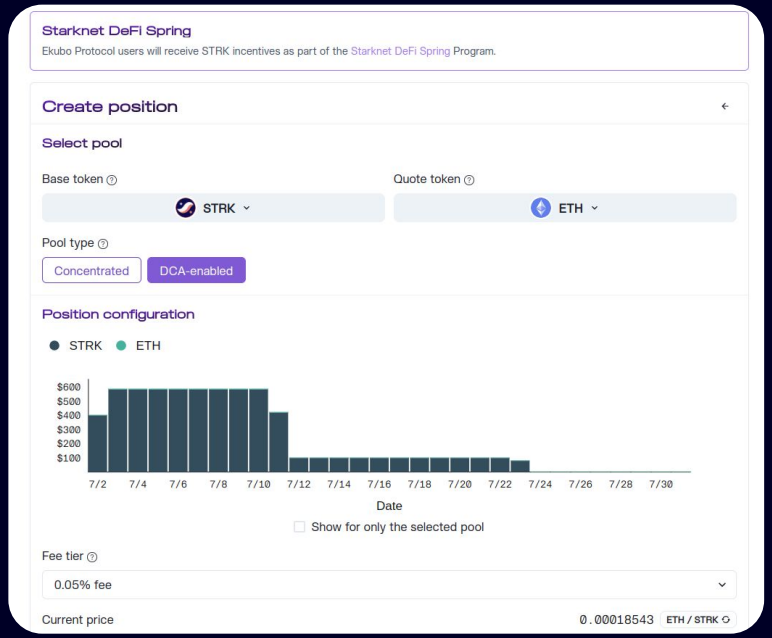


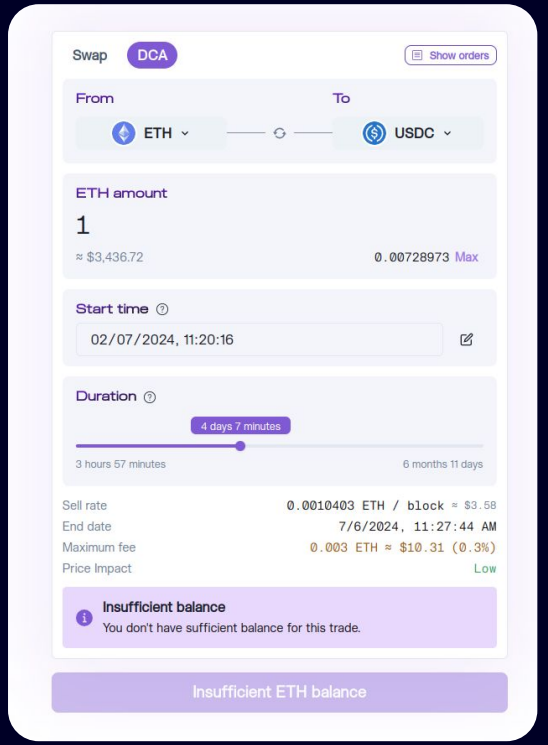


Expressibility

Ekubo - Most Efficient AMM

STARKWARE

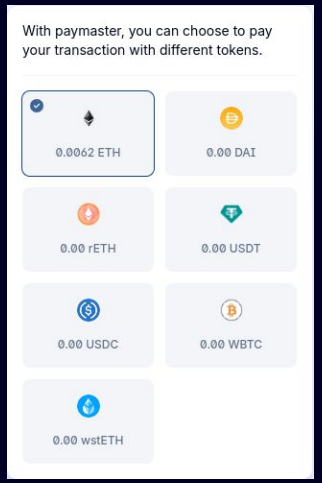


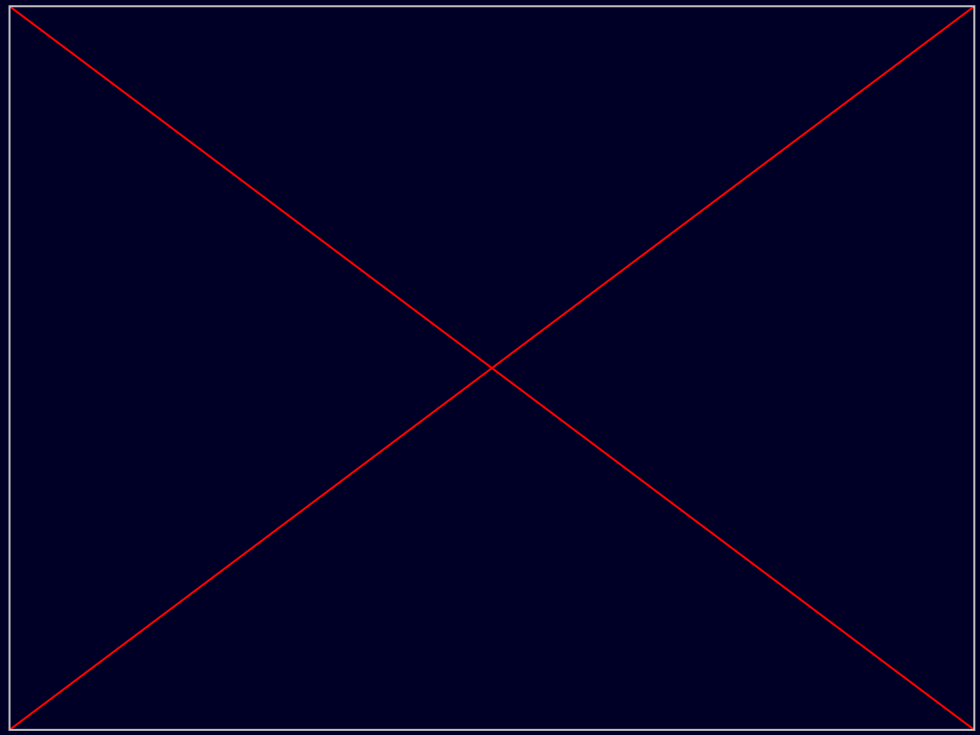


Exceptional capital efficiency with concentrated liquidity and low fees

Expressibility

Avnu - Paymaster





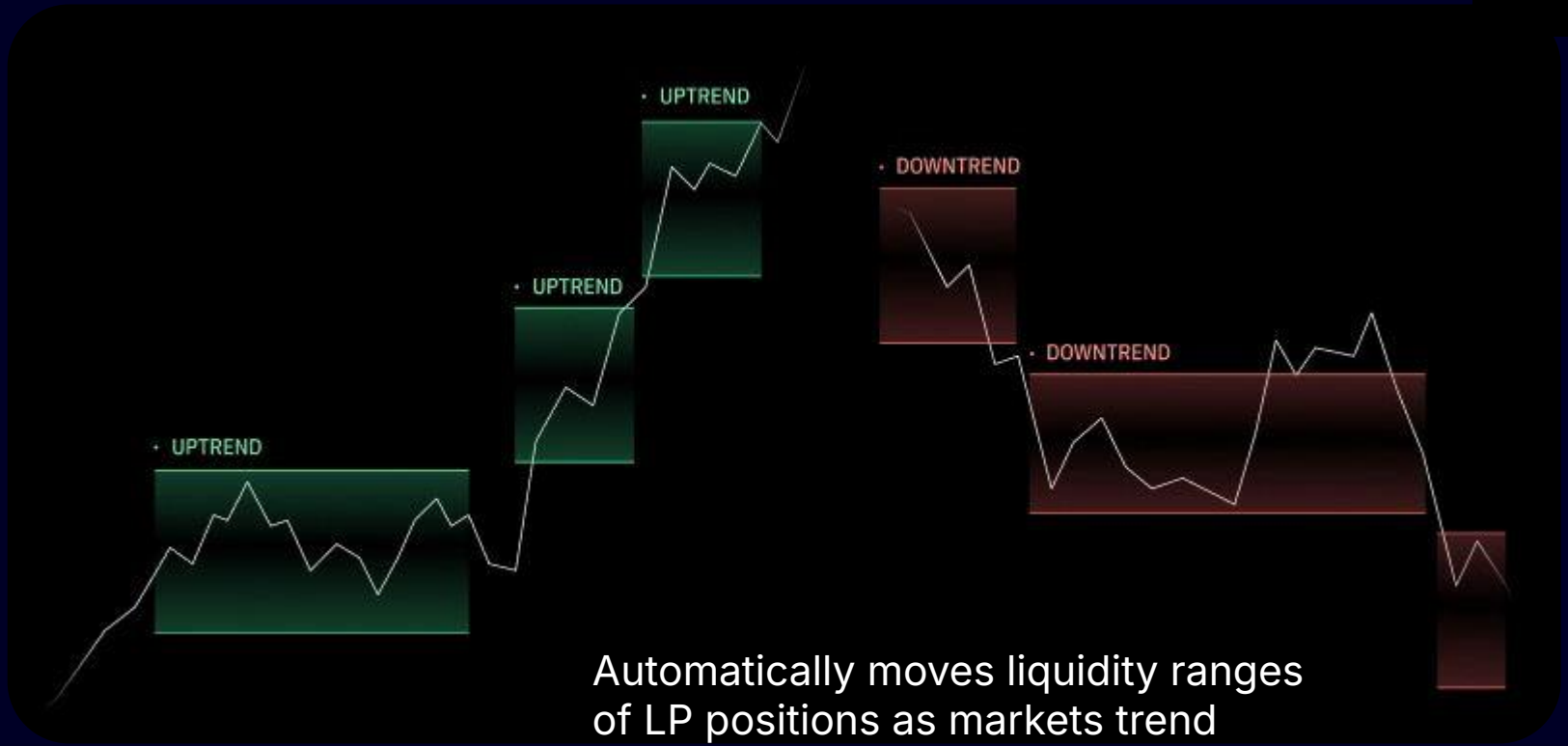
Enables easier user onboarding

Expressibility

STARKWARE

HAIKO

Haiko Automated LP Strategies



Automatically moves liquidity ranges
of LP positions as markets trend

Innovation

DOJO - Provable Game Engine for Online Games

STARKWARE

cartridge

DOJO

KEY FEATURES

- → **CAIRO COMPILER PLUGIN** TO SUPPORT DOJO CUSTOM MACROS
- → **DYNAMIC ON-CHAIN DATABASE** WITH INTROSPECTION
- → **AUTOMATIC INDEXING** AND P2P NETWORK FOR REALTIME BINDINGS TO THE WORLD STATE
- → RECURSIVE PROVING AND SETTLEMENT OF THE WORLD STATE USING **CAIRO VERIFIER ON STARKNET**

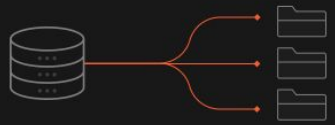
Innovation

Giza - Verifiable Machine-Learning Models

STARKWARE

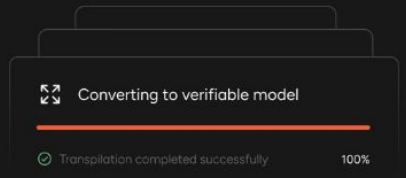
Curated onchain data

Leverage curated datasets created for Machine Learning from onchain data.
Start building



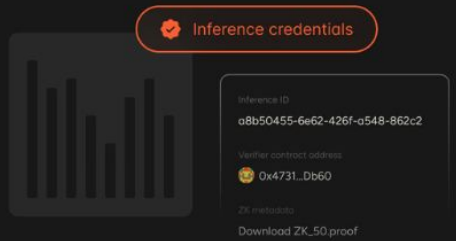
Create verifiable model

Convert any model into a Verifiable Machine Learning model leveraging Zero-Knowledge cryptography.



Run verifiable inference

We use ZK cryptography to provide verifiable, tamper-evident proofs of ML model executions.



Protocol integration

Integrate Actions into protocols through EVM verifiers, for efficiency, revenue growth and adoption.

Innovation

Influence: Fully-onchain MMP Strategy Game

STARKWARE

INFLUENCE

Innovation

What's Important in a Chain - Community ?

Innovation

Vision

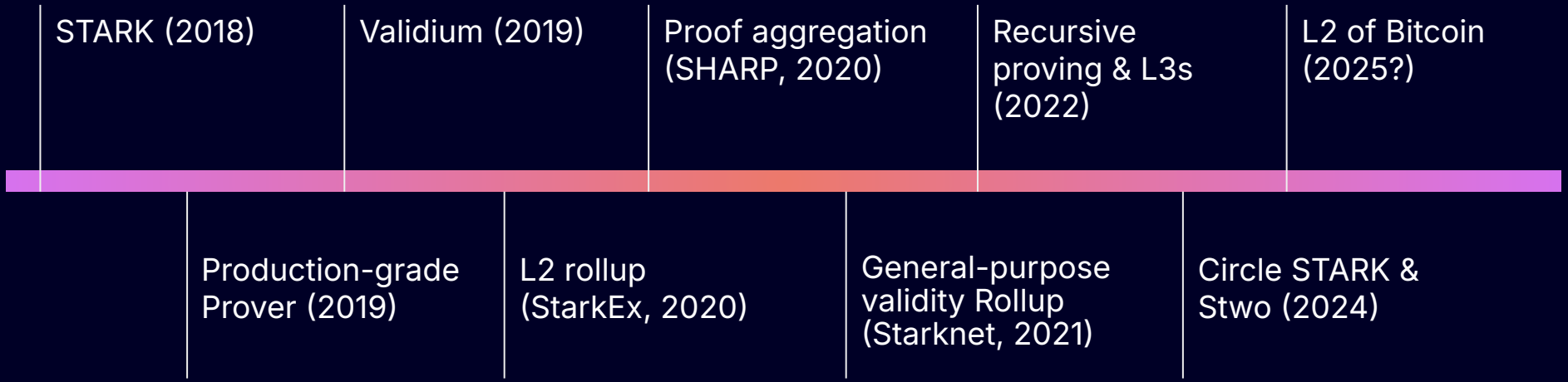
Values

Energy

Decisions

STARKWARE

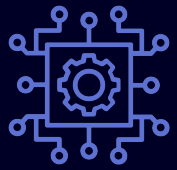
StarkWare - Technological Innovations



✨ Tech innovation fuels app innovation

Innovation

STARKNET - Vision



Fueling the Integrity Web

Running on top of both Ethereum and Bitcoin

Integrity Webs (“Blockchains”)

Blockchains are about:

- Cryptography
- Computers
- Peer-to-Peer Networks
- Proof of Work/Stake
- Byzantine Agreement

Integrity Webs (“Blockchains”)

Blockchains are about:

- Cryptography
- Computers
- Peer-to-Peer Networks
- Proof of Work/Stake
- Byzantine Agreement

Integrity Webs (“Blockchains”)

Blockchains are about:

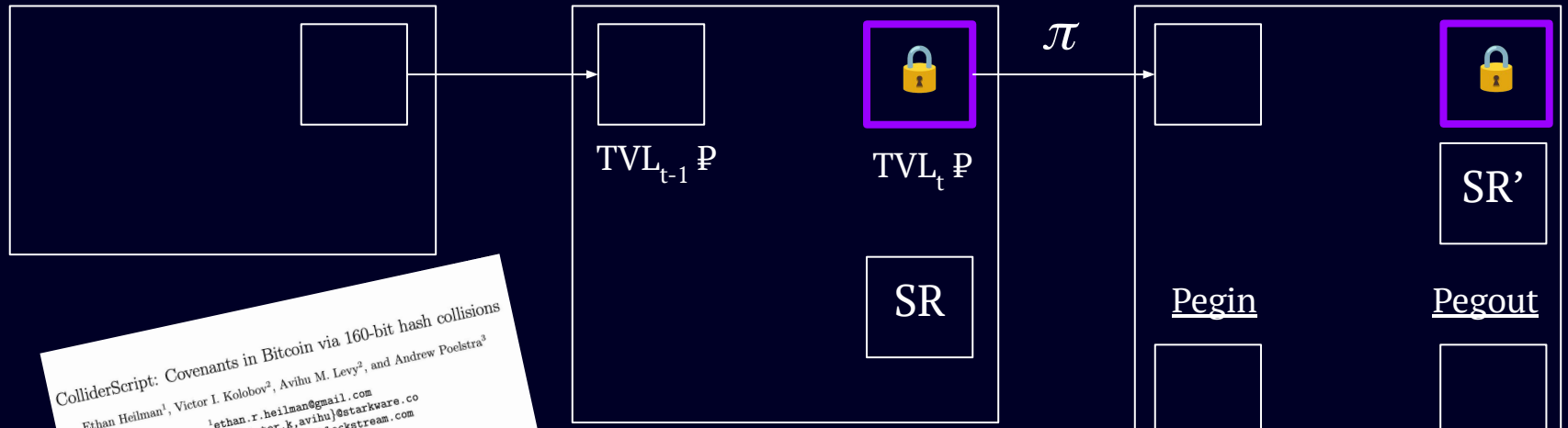
- Cryptography
- Computers
- Peer-to-Peer Networks
- Proof of Work/Stake
- Byzantine Agreement

Integrity Webs are about:

- Community
- Economics
- Freedom
- Human Dignity
- Human Rights
- Social Functions

L2 to both Ethereum and Bitcoin

Tx of State t



ColliderScript: Covenants in Bitcoin via 160-bit hash collisions

Ethan Heilman[1], Victor I. Kolobov[2], Avihu M. Levy[2], and Andrew Poelstra[3]

[1]ethan.r.heilman@gmail.com
[2]StarkWare, {victor.k,avihu}@starkware.co
[3]Blockstream, apoelstra@blockstream.com

November 7, 2024

Abstract

We introduce a method for enforcing covenants on Bitcoin outputs without requiring any changes to Bitcoin by designing a hash collision based *equivalence check* which bridges Bitcoin's limited *Big Script* to Bitcoin's *Small Script*. This allows us evaluate the signature of the spending transaction (available only to Big Script) in Small Script. As Small Script enables arbitrary computations, we can introspect into the spending transaction and enforce covenants on it.

Our approach leverages *finding collisions* in the 160-bit hash functions: SHA1 and RIPEMD. By the birthday bound this should cost $\sim 2^{80}$ work. Each spend of our covenant costs $\sim 2^{86}$ hash queries and $\sim 2^{56}$ bytes of space. For security, we rely on an assumption regarding the hardness of finding a 3-way collision (with short inputs) in 160-bit hash functions. To put this in perspective, the work to spend our covenant requires ~ 33 hours of the Bitcoin mining network, whereas the assumption holds, breaking covenant enforcement requires $\sim 2^{110}$ hash queries. We believe there are multiple directions of future work that can significantly improve these numbers.

Evaluating covenants and our equivalence check requires performing many operations in Small Script, which must take no more than 4 megabytes in total size, as Bitcoin does not allow transactions greater than 4 megabytes. We only provide rough estimates of the transaction size because, as of this writing, no Small Script implementations of the hash functions required, SHA1 and

Vision

Values

Integrity

"Do the right thing, even when no one is watching"

(-) C.S Lewis

Long-Term Thinking

"If you really look closely, most long term successes took a long time"

(-) Steve Jobs

Transparency

"Sunlight is said to be the best of disinfectants

(-) Louis D. Brandeis

Collaboration

"Many ideas grow better when transplanted into another mind than the one where they sprang up"

(-) Oliver Wendell Holmes

Creativity

"Go where there is no path and leave a trail"

(-) R.W. Emerson

Purpose

"Be not simply good, be good for something"

(-) H.D. Thoreau

STARKNET FOUNDATION

Values

STARKWARE

Community

Energy

STARKWARE

Thank You