THE STARK TRUTH ABOUT DEXes

Eli Ben-Sasson, Chief Scientist (East) | February 2019
StarkWare

$40M Funding (equity + EF grant)

20 Team members

Alpha DEX scalability engine

We’re hiring!  jobs@starkware.co

Learn more!  workshop@starkware.co
OUTLINE

1. STARKs as a Scalability Solution
2. DEXes
3. StarkDEX
STARKs and Scalability
DELEGATED ACCOUNTABILITY

OLD WORLD
(banks, pension funds...)

TRUST

assumption

delegated to auditors, accountants, regulators
DELEGATED ACCOUNTABILITY
OLD WORLD
(banks, pension funds...)

assumption
dele gated to auditors, accountants, regulators

INCLUSIVE ACCOUNTABILITY
NEW WORLD
don’t trust, verify

TRUST
VERIFY
everyone should be able to verify integrity of the system, using a laptop
everyone sees every Tx

require small throughput to allow accountability even on weaker devices (i.e: laptop)
everyone sees every Tx

shield transactions
(like ZK-SNARKs do for Zcash)

require small throughput to
include accountability on
weaker devices (i.e: laptop)

S == scalability

PRIVACY

ZK-STARKs

SCALABILITY

ZK-STARKs
Inclusive Accountability - Scalability Problem
Inclusive Accountability - Scalability Problem

NETWORK THROUGHPUT (T) vs. COMPUTATION TIME

- Computational resources threshold
Inclusive Accountability - Scalability Problem

Network Throughput (T) vs. Computation Time (on chain vs. off chain)

- Computational resources threshold
- Block limit
STARK Scalability

Prover time is nearly linear in $T$

&

Verifier time exponentially smaller than $T$
STARK Scalability

Prover time is nearly linear in $T$

&

Verifier time exponentially smaller than $T$
STARK & Other ZKP Systems

**BulletProof**
- Verifier time scales linearly

**SNARK**
- Trusted setup scales linearly

**Recursive SNARK**
- Trusted setup, inefficient prover

### Diagram Notes
- **SCALABILITY FACTOR**
- **COMPUTATION TIME**
- **NETWORK THROUGHPUT (T)**
- **PROOF COMPUTE / UNIT OF TIME**
- **VERIFIER COMPUTE / UNIT OF TIME**

### Computational Resources Threshold
- Block limit

---

**STARKWARE**
DEXes and Scalability
Exchange: the 3-Act Play

- List orders & manage order book
- Match-making
- Settlement
Exchange: the 3-Act Play

- List orders & manage order book
- Match-making
- Settlement
Centralized Exchange (CEX)

- Custody: Exchange holds all assets
- Settlement: Off-chain
- Tx / Trades: #On-chain tx’s << #trades

Decentralized Exchange (DEX)

- Custody: Stays with traders
- Settlement: On-chain
- Tx / Trades: #On-chain tx’s == #trades
DEXes

**ADVANTAGES**

- No central honeypot luring thieves & embezzlers
- DEX does not assume counterparty risk:
  - No exposure to 51% attack
  - Faster/cheaper listing of crypto pairs

**DISADVANTAGES**

- Total dex volume ~ 1% of total CEX volume
- Transaction (settlement) cost: ~200K gas, implies upper bound of 3 tx/sec in Ethereum

*low tx volume means poor liquidity*
StarkDEX Overview
Current DEXes
StarkDEX – High Level

ON-CHAIN

Verifier contract

DEX contract

Storage

OFF-CHAIN

data

PROVER

DEX
StarkDEX – High Level

**On-chain**
- **Verifier contract**
- **Storage**
- **DEX contract**

**Off-chain**
- **PROVER**
- **DEX**
- **Data**
StarkDEX – High Level

Diagram:
- **ON-CHAIN**
  - Storage
  - DEX contract
  - Verifier contract
  - O(1) ( ladybug)

- **OFF-CHAIN**
  - PROVER
  - DEX
  - data
  - Proof

Text:
- StarkDEX
- High Level
- DEX contract
- Verifier contract
- MR
- log(n)
- storage

Diagram:
- On-chain components: Storage, DEX contract, Verifier contract, O(1)
- Off-chain components: PROVER, DEX, data, Proof

Starkware logo at the bottom.
StarkDEX – High Level

OFF-CHAIN

- PROVER
- DEX
- Tx

ON-CHAIN

- Verifier contract
- DEX contract
- Storage

O(0)
StarkDEX – High Level

**On-chain**

- **Verifier contract**
  - Linked to **DEX contract**
  - Linked to **Storage**

**Off-chain**

- **PROVER**
  - Linked to **DEX**
  - Linked to **data**

- **DEX**
  - Contains **Tx**

---

**StarkDEX**

- **PROVER**
- **DEX contract**
- **Verifier contract**
- **Storage**
StarkDEX – High Level
OVER
PROVER
Verifier Contract
Verifier Contract

PROVER

PROOF

MR

data
data

Verifier Contract

PROVER

MR

PROOF

OFF-CHAIN

ON-CHAIN
Verifier Contract
StarkEx Dex - TX Anatomy

Verifer Contract

ON-CHAIN

PROVER

OFF-CHAIN

data

DEX Contract

Storage

DEX
Starked Dex - Tx Anatomy

ON-CHAIN

Off-chain data

PROVER

Verifier Contract

DEX Contract

Storage

OFF-CHAIN

DEX
Starked Dex - Tx Anatomy

On-chain:
- Verifier Contract
- EX Contract
- Storage

Off-chain:
- PROVER
- DEX

Data flows from off-chain to on-chain through PROVER, which interacts with the Verifier Contract.
ONE MORE THING...
DEMO

LOCAL LAPTOP

browser

METAMASK

WASM

Ethereum Node (Ganache)

VERIFIER SMART CONTRACT

Local Proof Service

Big Proof Service
STARK Scalability

- **Computational resources threshold**
  - Block limit
  - 8M GAS
  - 30
  - 50
  - 500
  - >10K

**Network throughput (T):**
- On chain
- Off chain
- PROVER compute / unit of time
- VERIFIER compute / unit of time

Native: •
Prover: ●
Verifier: ▲

Diagram showing scalability with computational resources threshold.
Current DEX

max out @ 50 DEX Txs / Block
(100K-200K gas / DEX tx)

StarkDEX

30 DEX Txs @ 5.5M gas
(180K gas / StarkDEX tx)

500 DEX Txs @ 6.7M gas
(13.5K gas / StarkDEX tx)

verification on-chain can be done for over 10K txs/block
(800 gas / StarkDEX tx)
THANK YOU