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**

STARKWARE

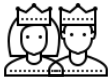
OUTLINE

1. STARKs as a Scalability Solution

2. DEXes

3. StarkDEX

STARKs and Scalability

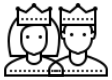


DELEGATED ACCOUNTABILITY

OLD WORLD
(banks, pension funds...)

TRUST — assumption

VERIFY — delegated to auditors, accountants, regulators



DELEGATED ACCOUNTABILITY

OLD WORLD
(banks, pension funds...)

TRUST

assumption

VERIFY

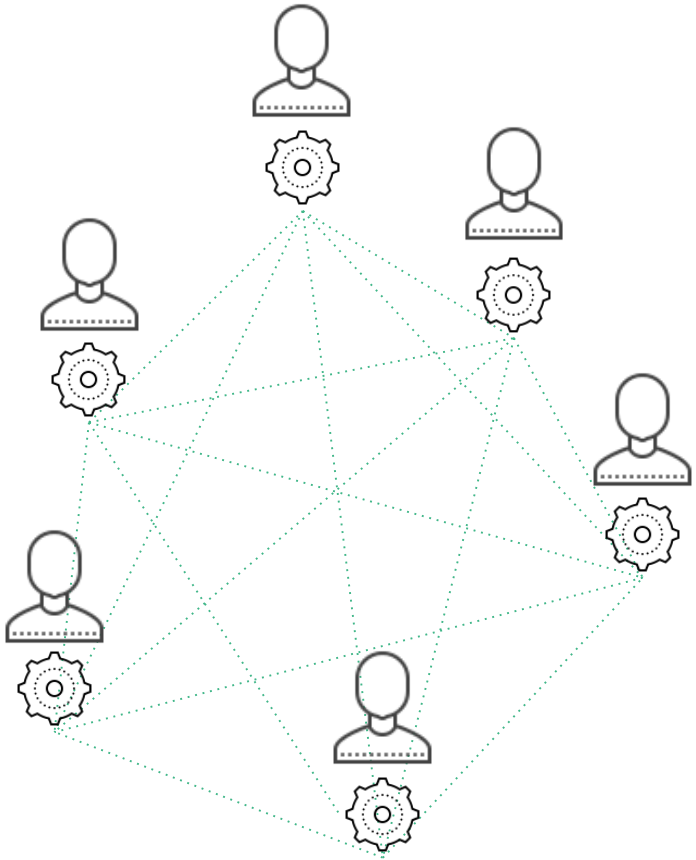
delegated to auditors, accountants, regulators

INCLUSIVE ACCOUNTABILITY

NEW WORLD

don't trust, verify

TRUST



INCLUSIVE ACCOUNTABILITY

NEW WORLD

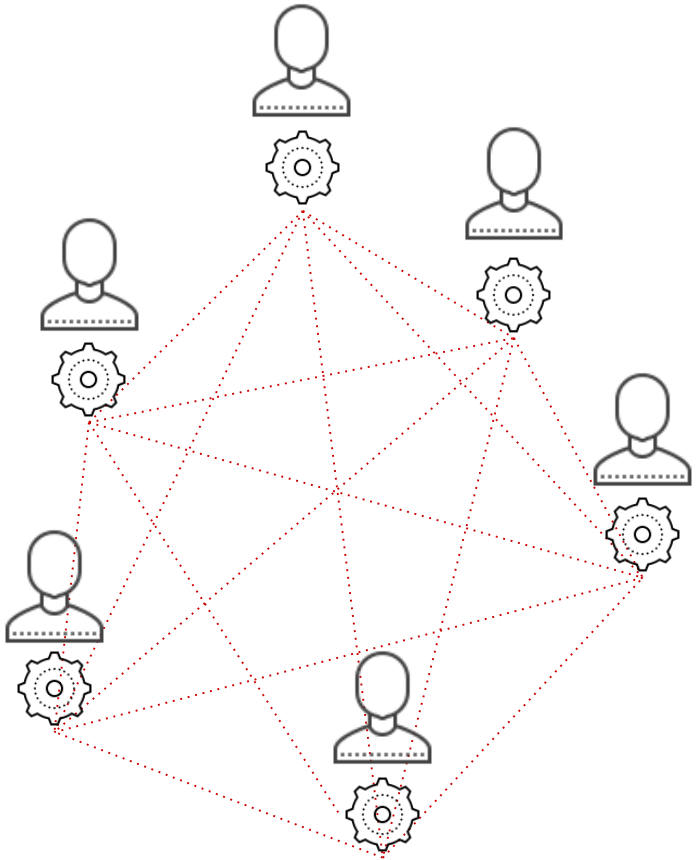
don't trust, verify

TRUST

everyone should be able to verify integrity of the system, using a laptop

VERIFY

STARKWARE

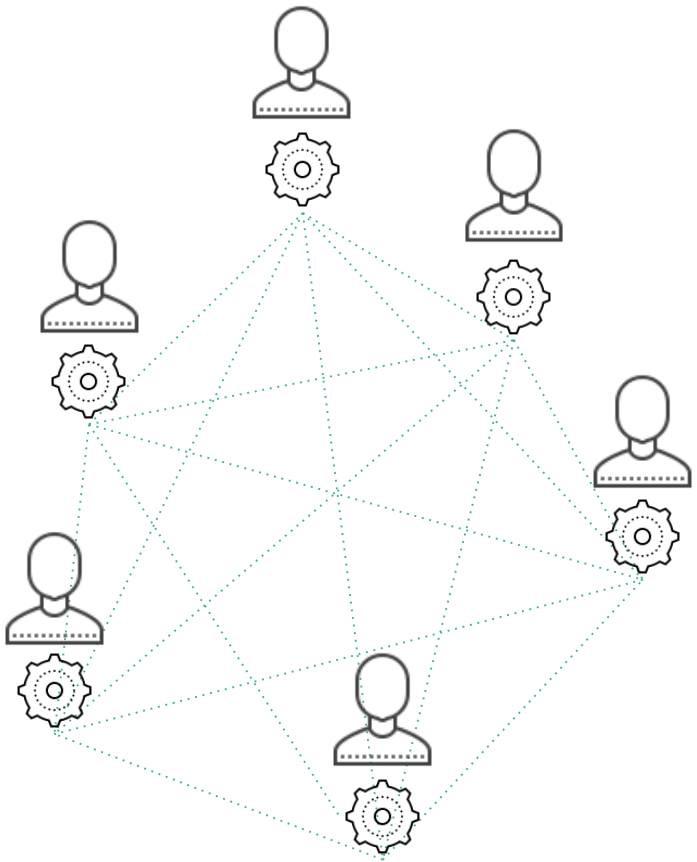


INCLUSIVE ACCOUNTABILITY

2 PROBLEMS

everyone sees every Tx — PRIVACY

require small throughput to allow accountability even on weaker devices (i.e: laptop) — SCALABILITY



INCLUSIVE ACCOUNTABILITY

STARK SOLVES BOTH

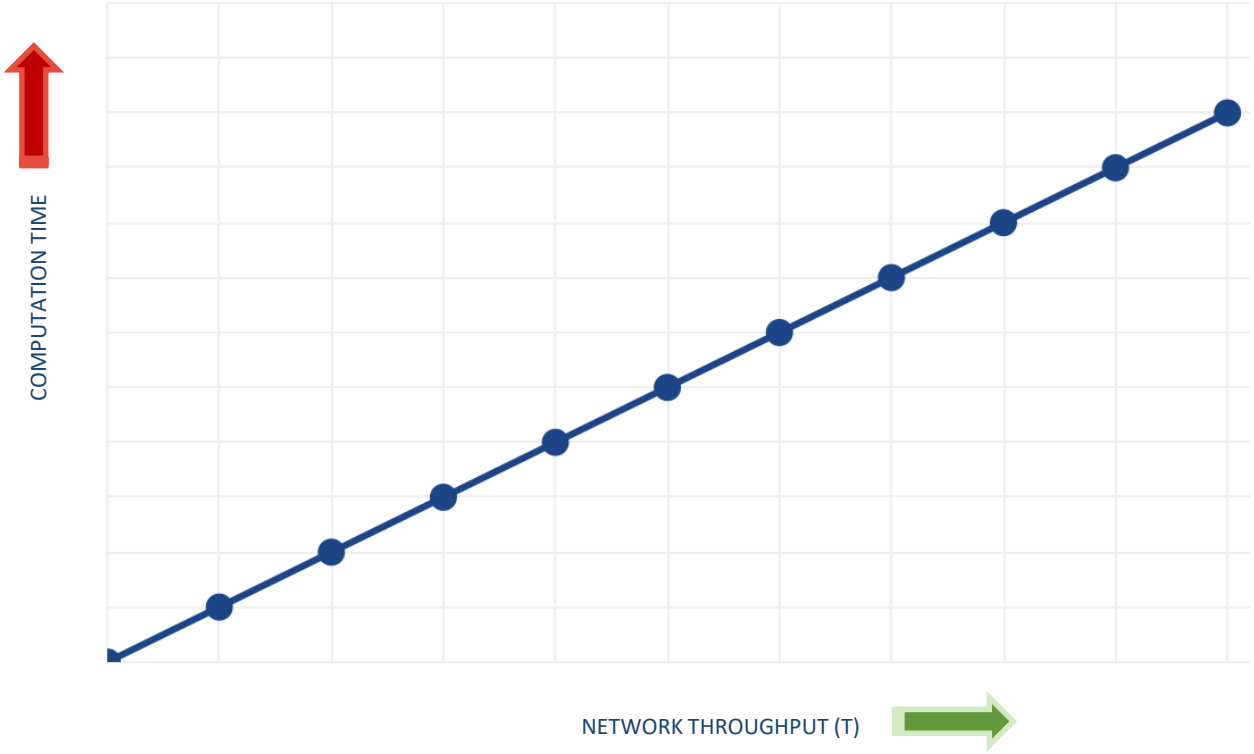
everyone sees every Tx — PRIVACY

shield transactions
(like ZK-SNARKs do for Zcash) — ZK-STARKs

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

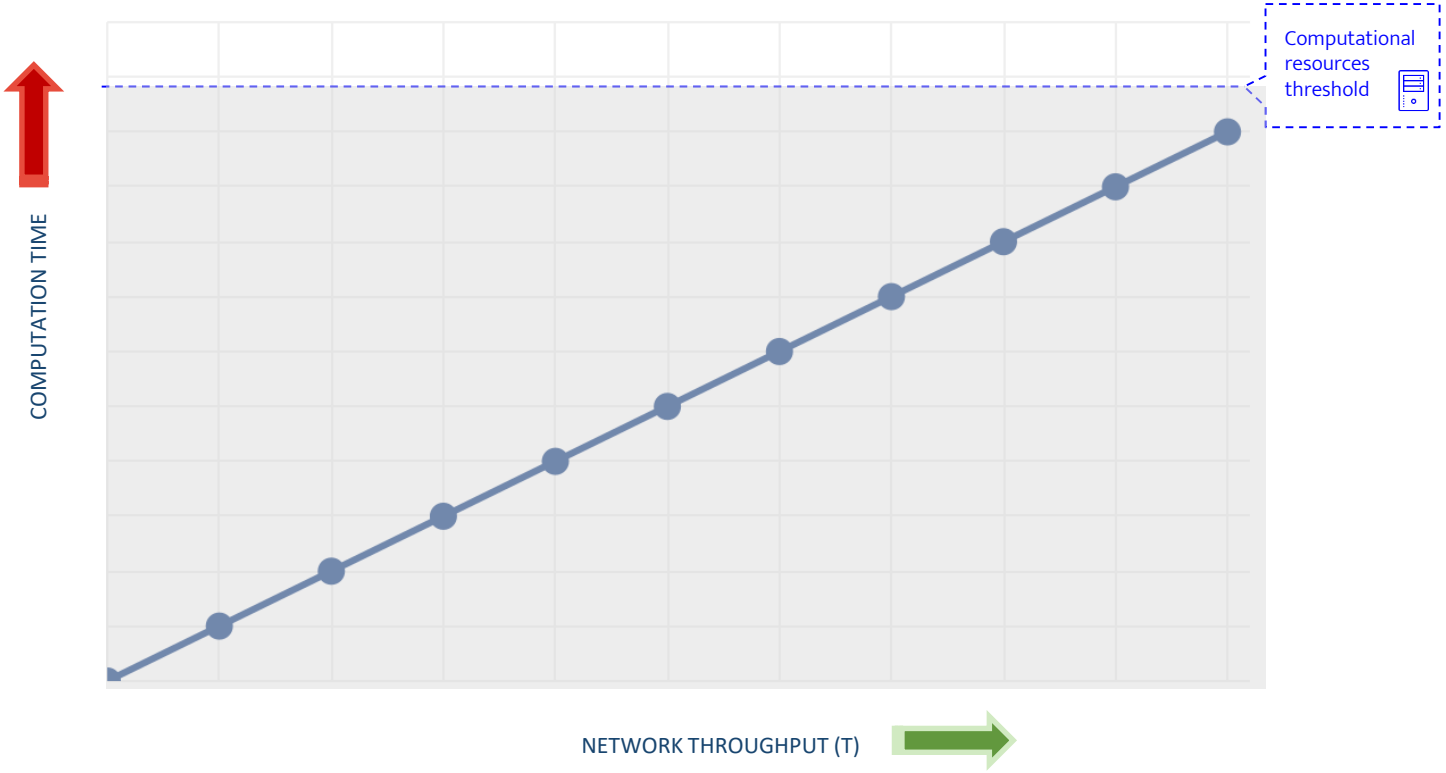
S == scalability — ZK-STARKs

Inclusive Accountability - Scalability Problem



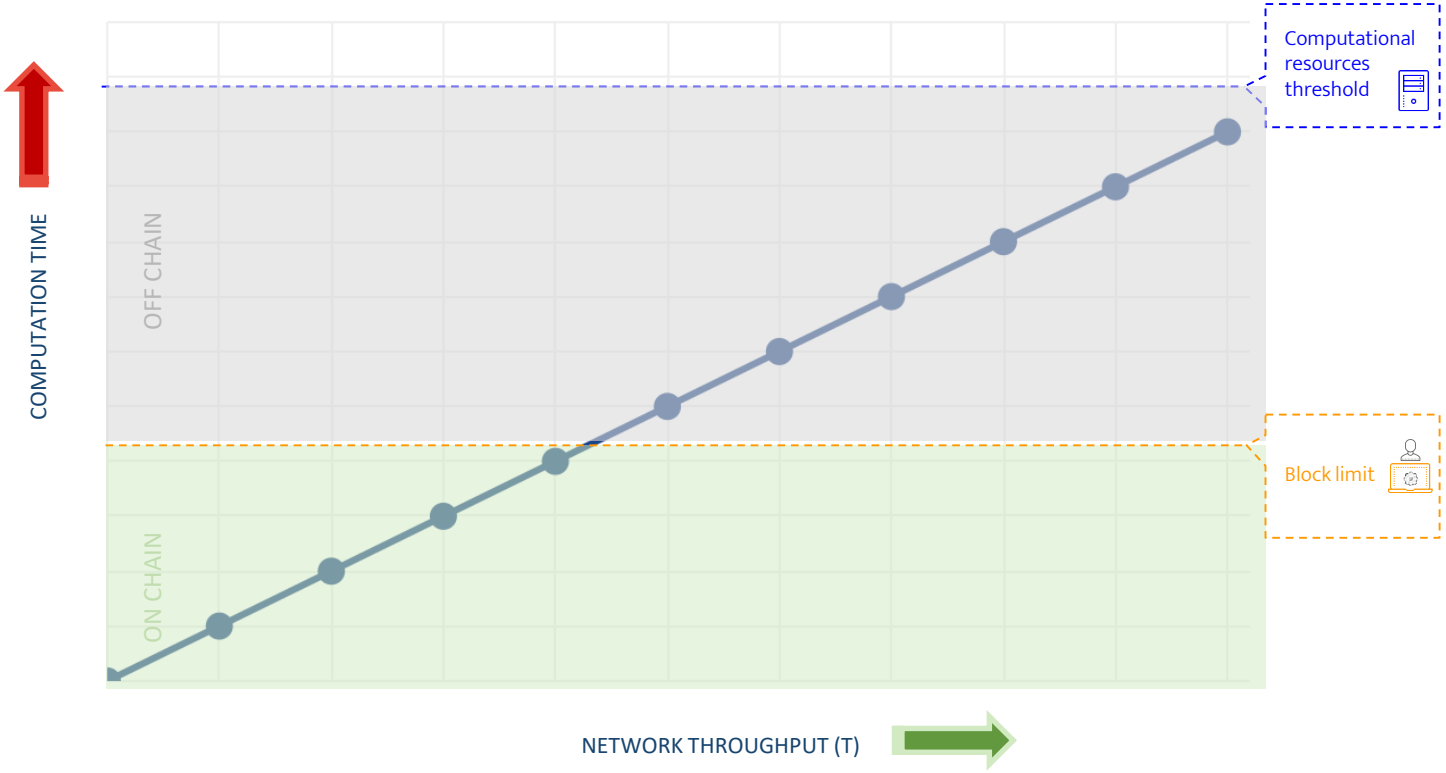
STARKWARE

Inclusive Accountability - Scalability Problem



STARKWARE

Inclusive Accountability - Scalability Problem



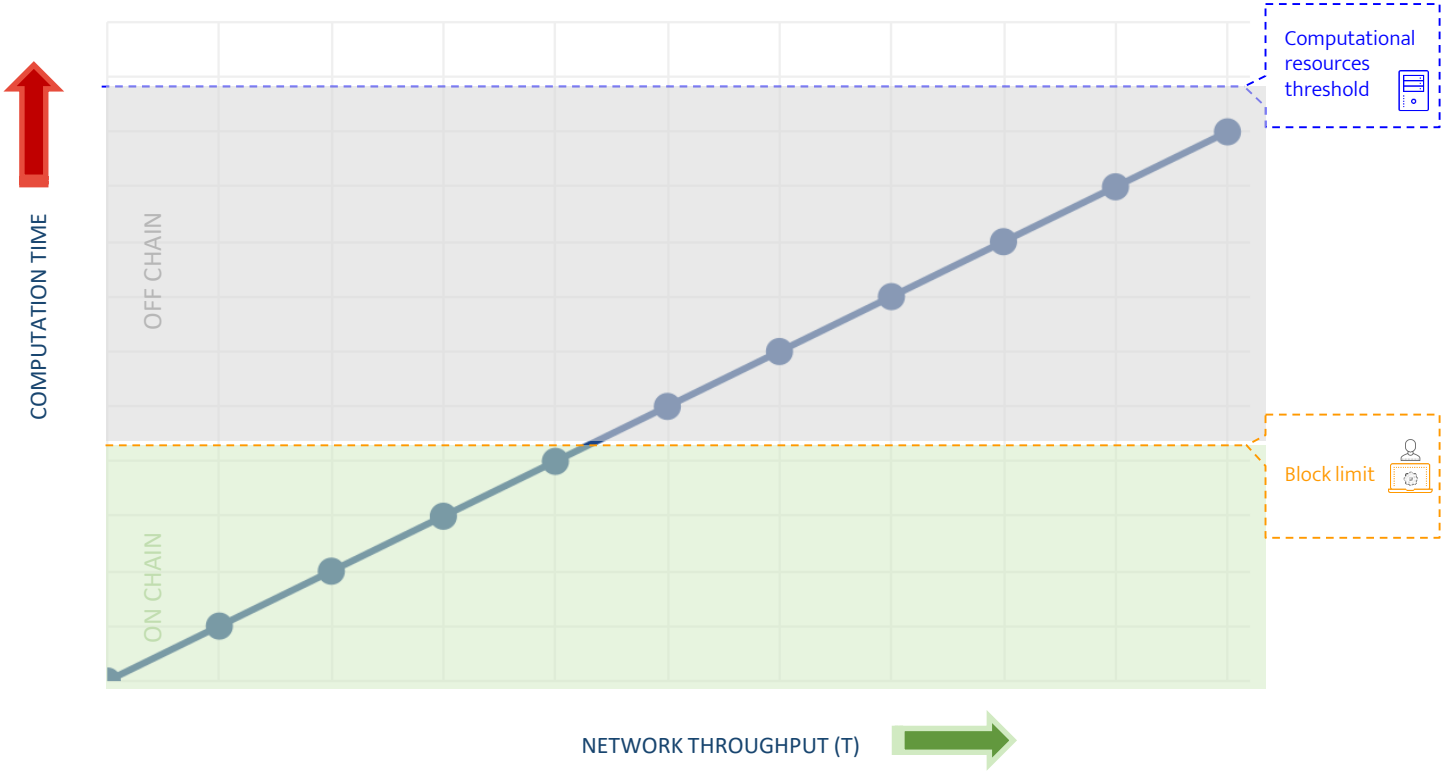
STARKWARE

STARK Scalability

Prover time is nearly linear in T

&

Verifier time exponentially smaller than T



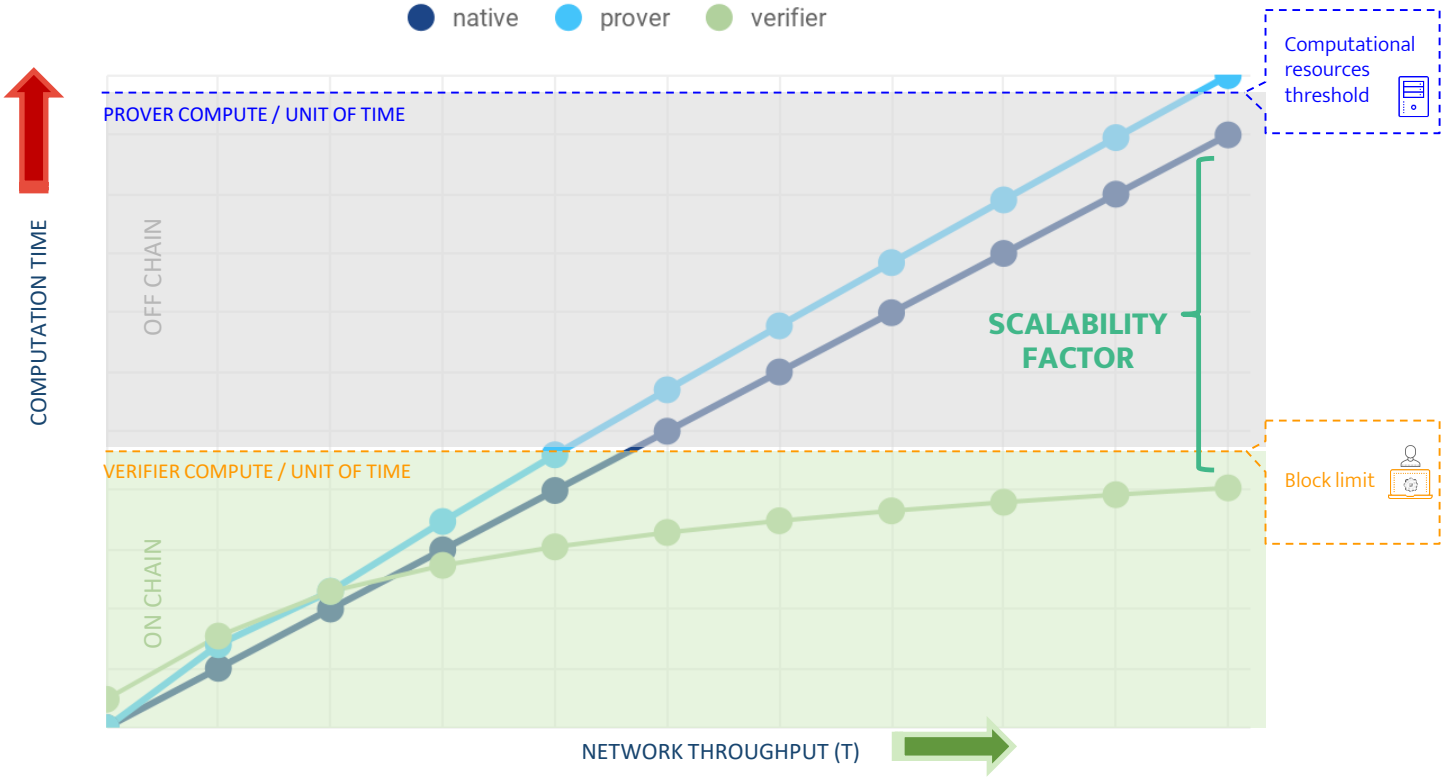
STARKWARE

STARK Scalability

Prover time is nearly linear in T

&

Verifier time exponentially smaller than T



STARK & Other ZKP Systems

BulletProof

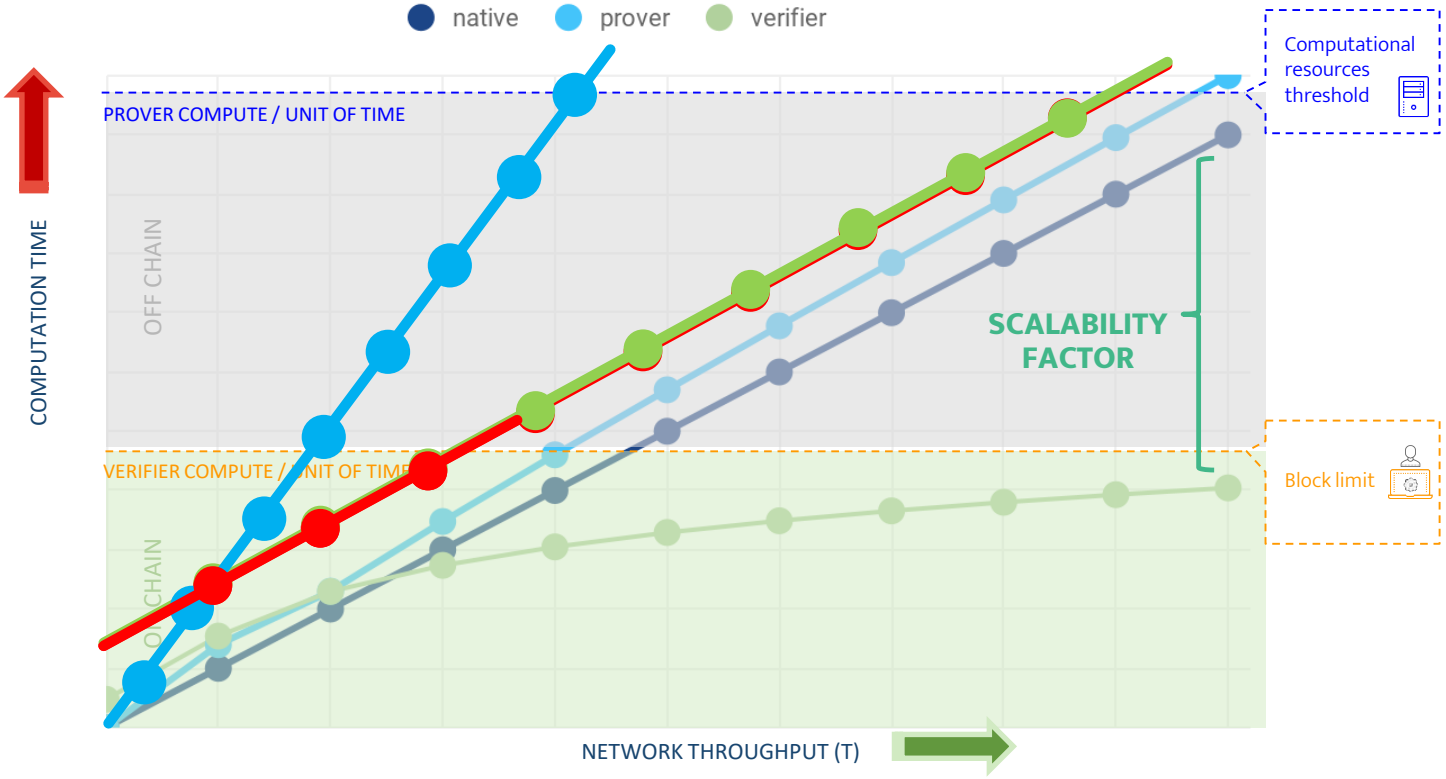
Verifier time scales linearly

SNARK

Trusted setup scales linearly

Recursive SNARK

Trusted setup, inefficient prover



STARKWARE

DEXes and Scalability

Exchange: the 3-Act Play

Exchange: the 3-Act Play

Centralized Exchange

(CEX)

Decentralized Exchange

(DEX)

CUSTODY	exchange holds all assets	stays with traders	CUSTODY
SETTLEMENT	off-chain	on-chain	SETTLEMENT
Tx / TRADES	#On-chain tx's << #trades	#On-chain tx's == #trades	Tx / 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

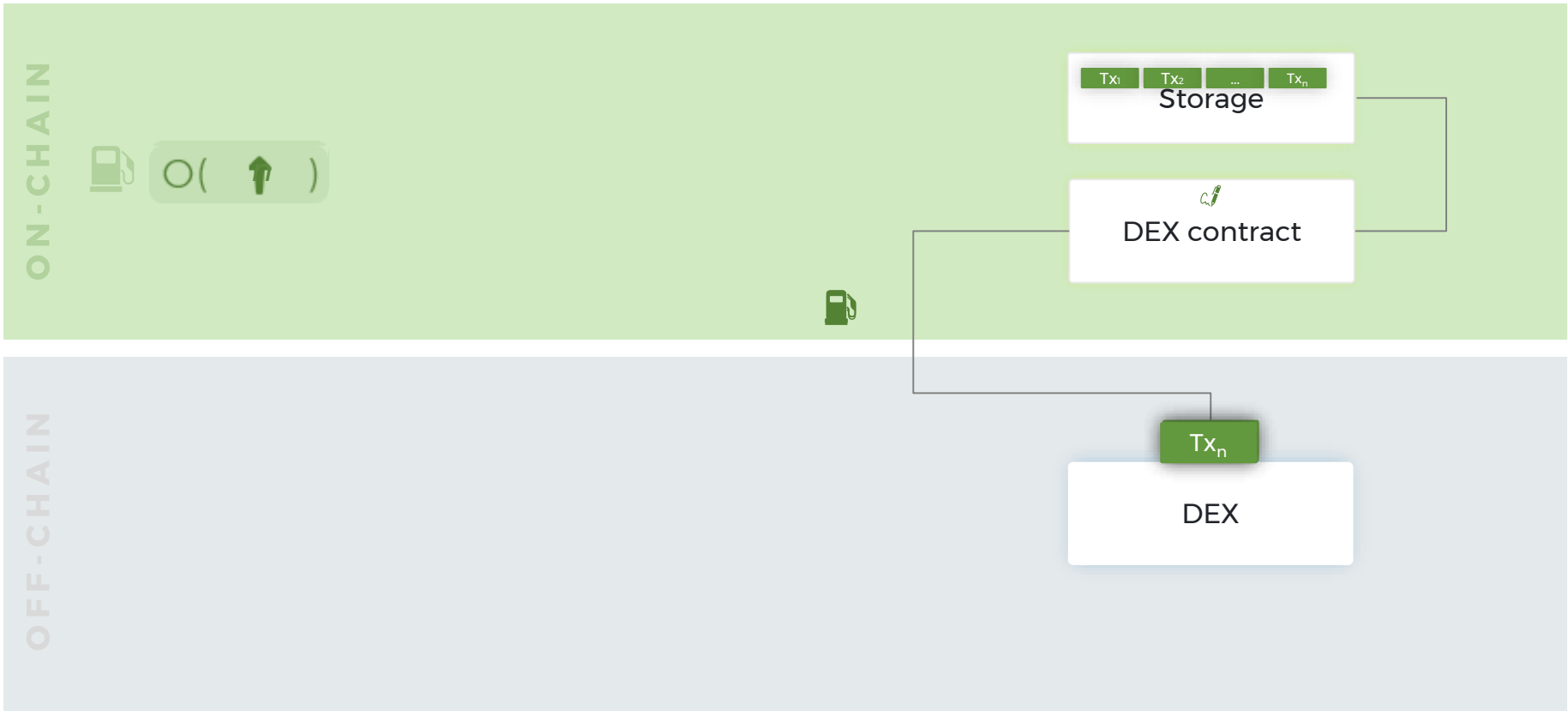
StarkDEX Overview

ON-CHAIN

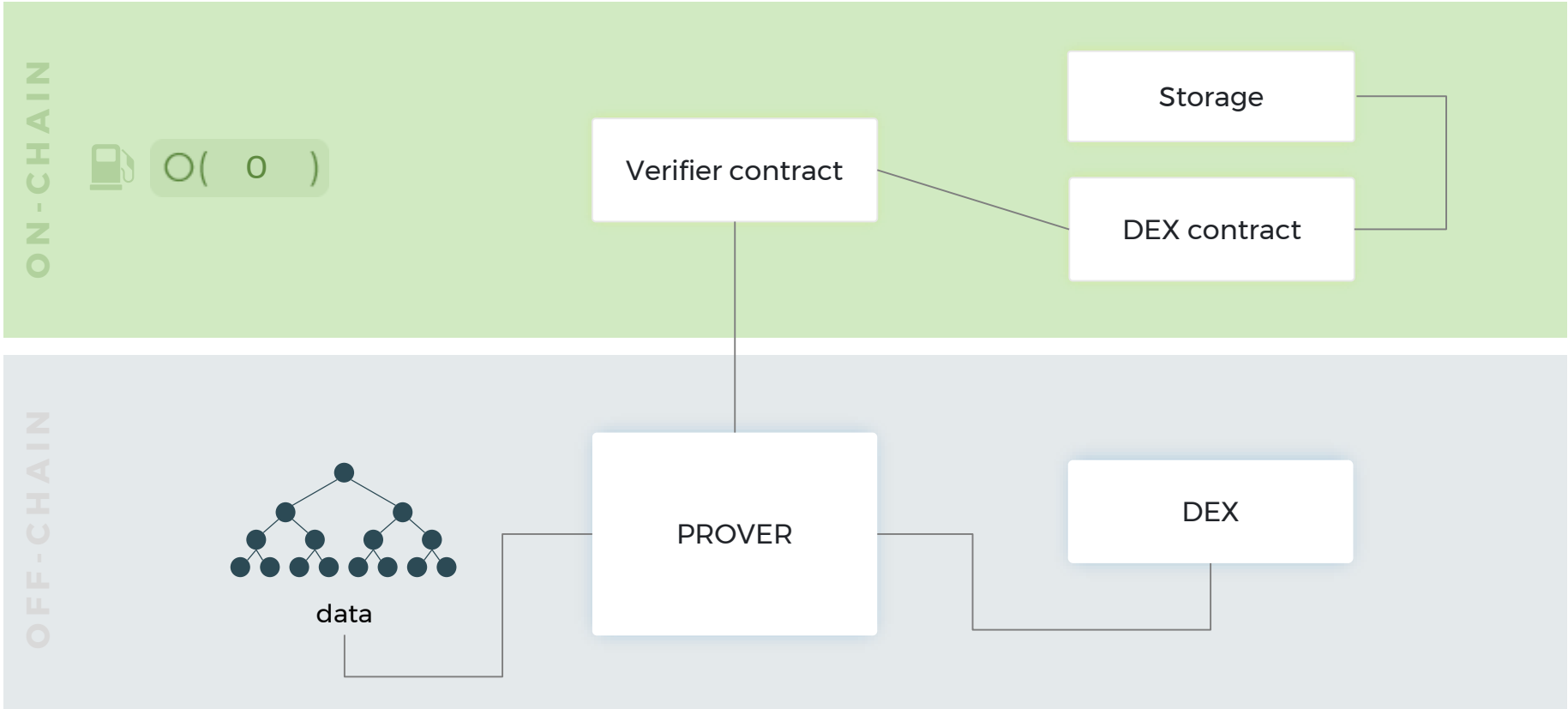
OFF-CHAIN

STARKWARE

Current DEXes

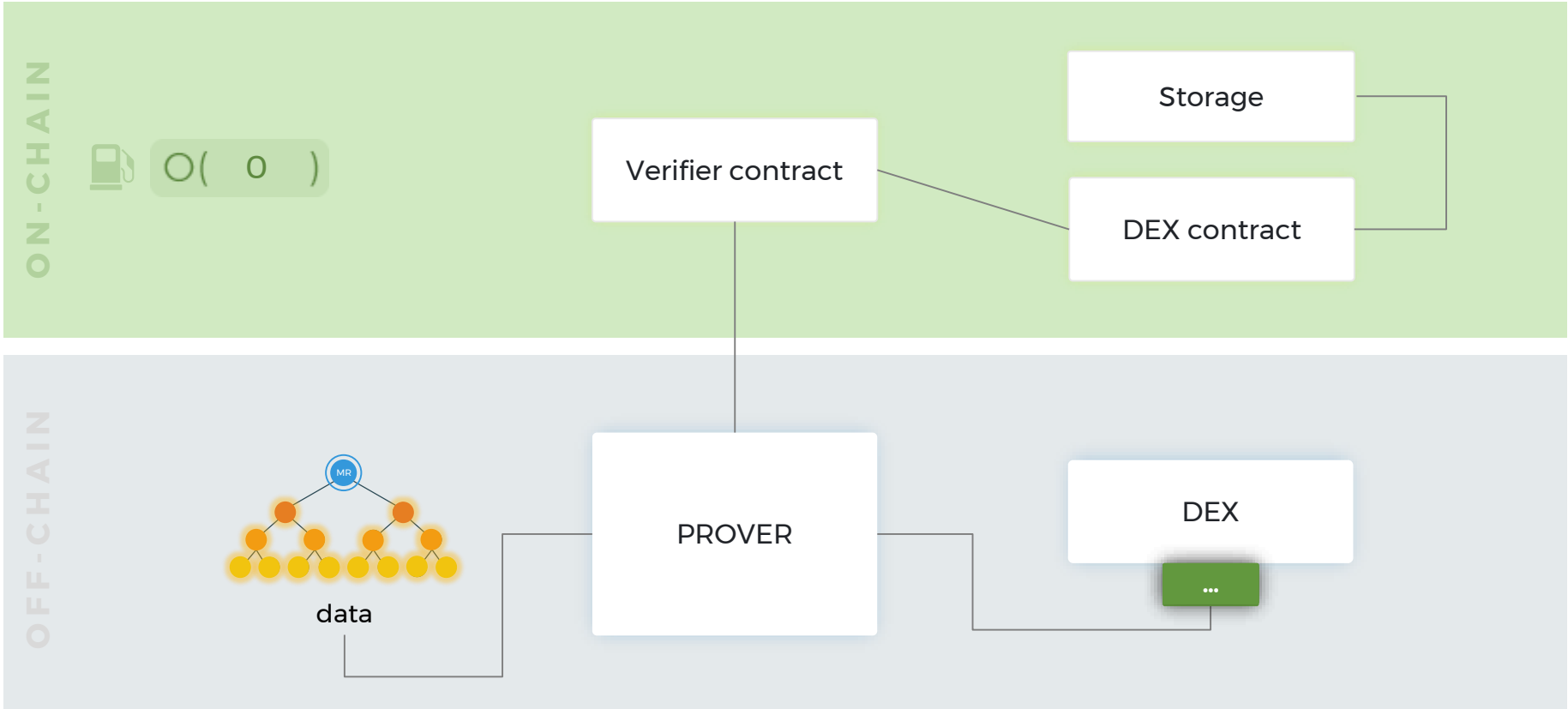


StarkDEX – High Level



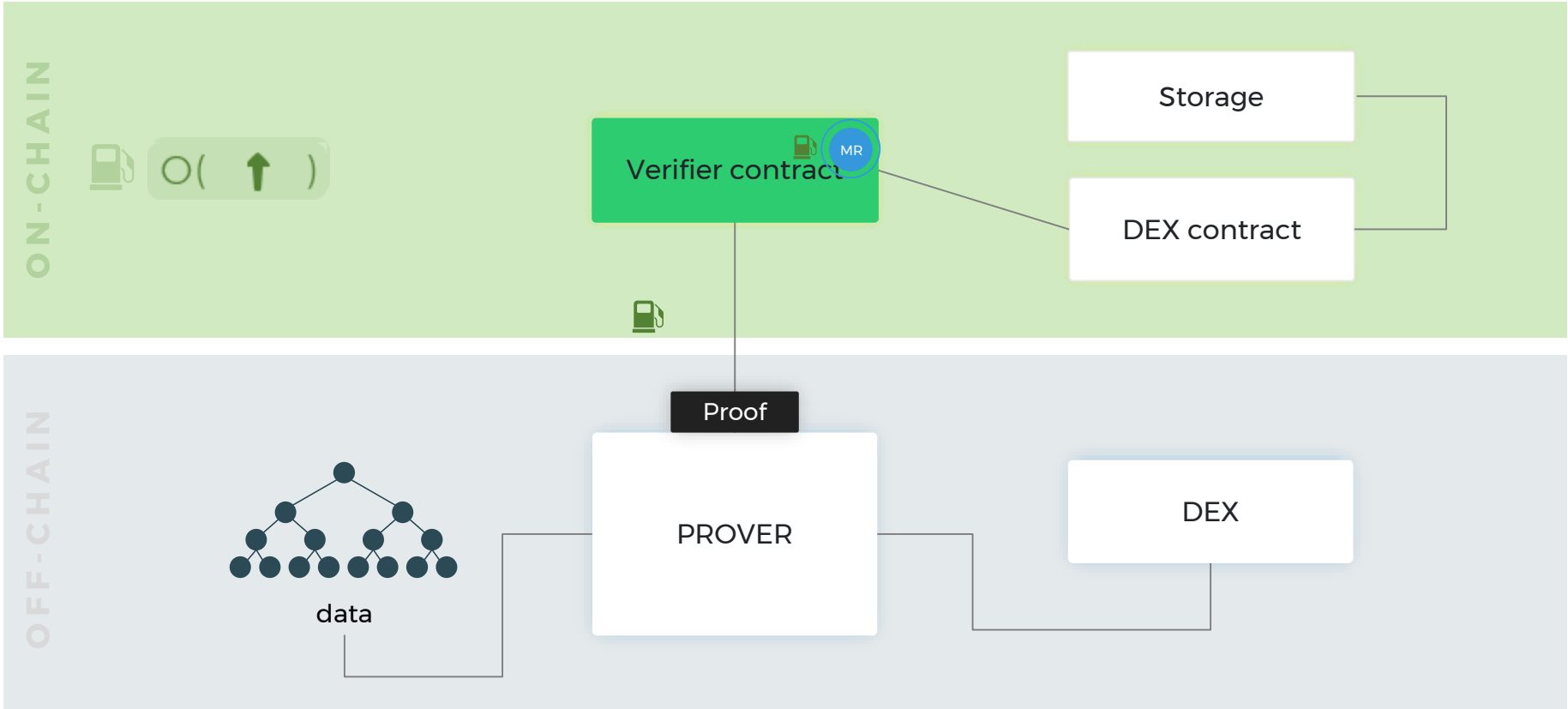
STARKWARE

StarkDEX – High Level

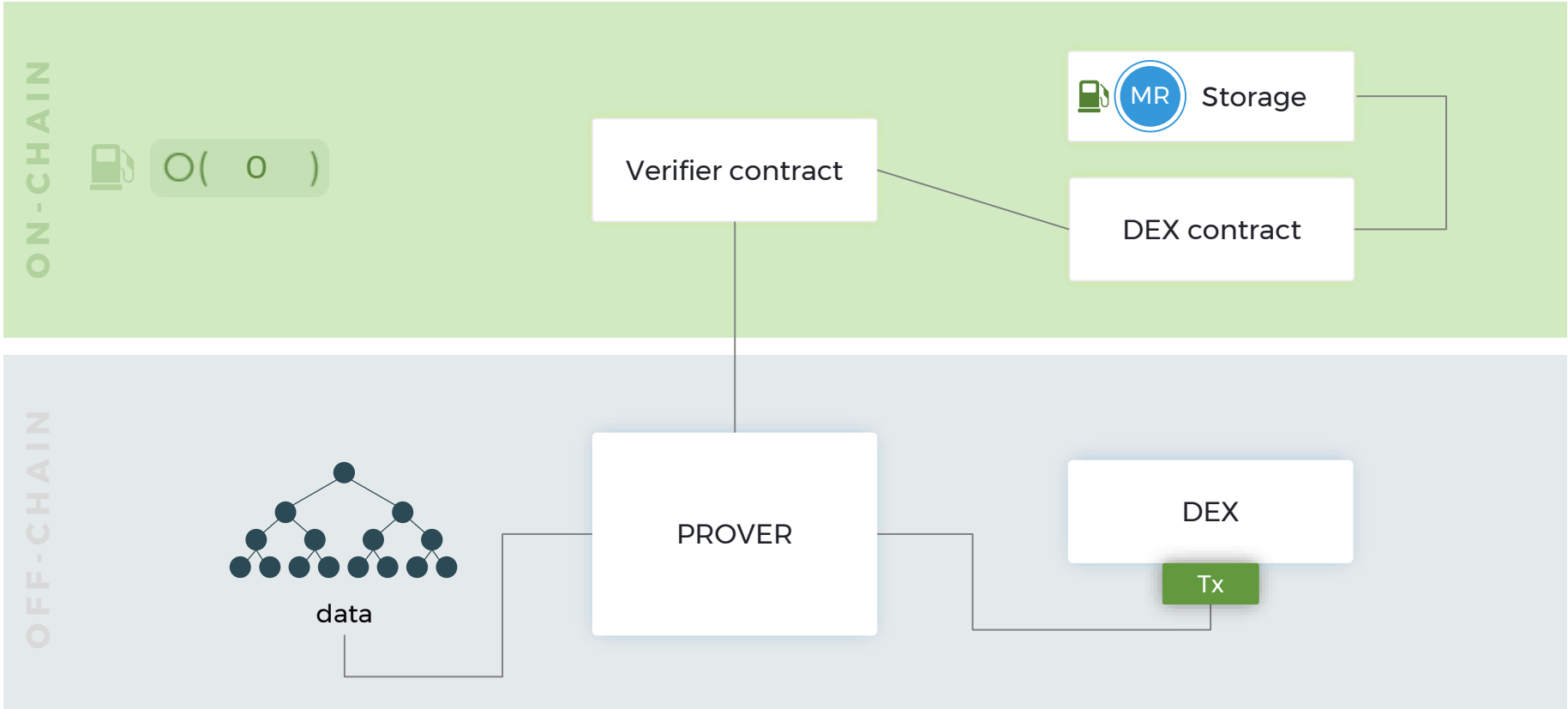


STARKWARE

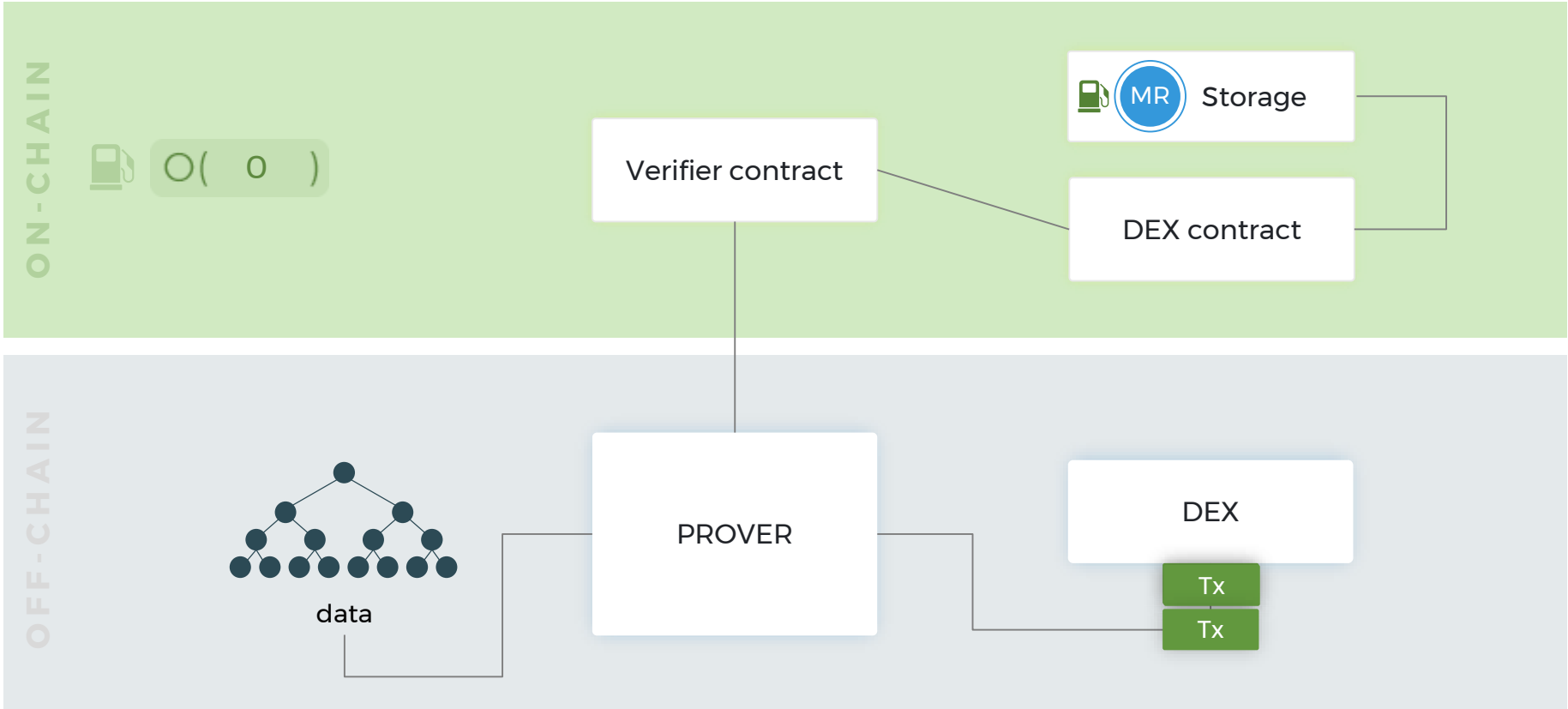
StarkDEX – High Level



StarkDEX – High Level

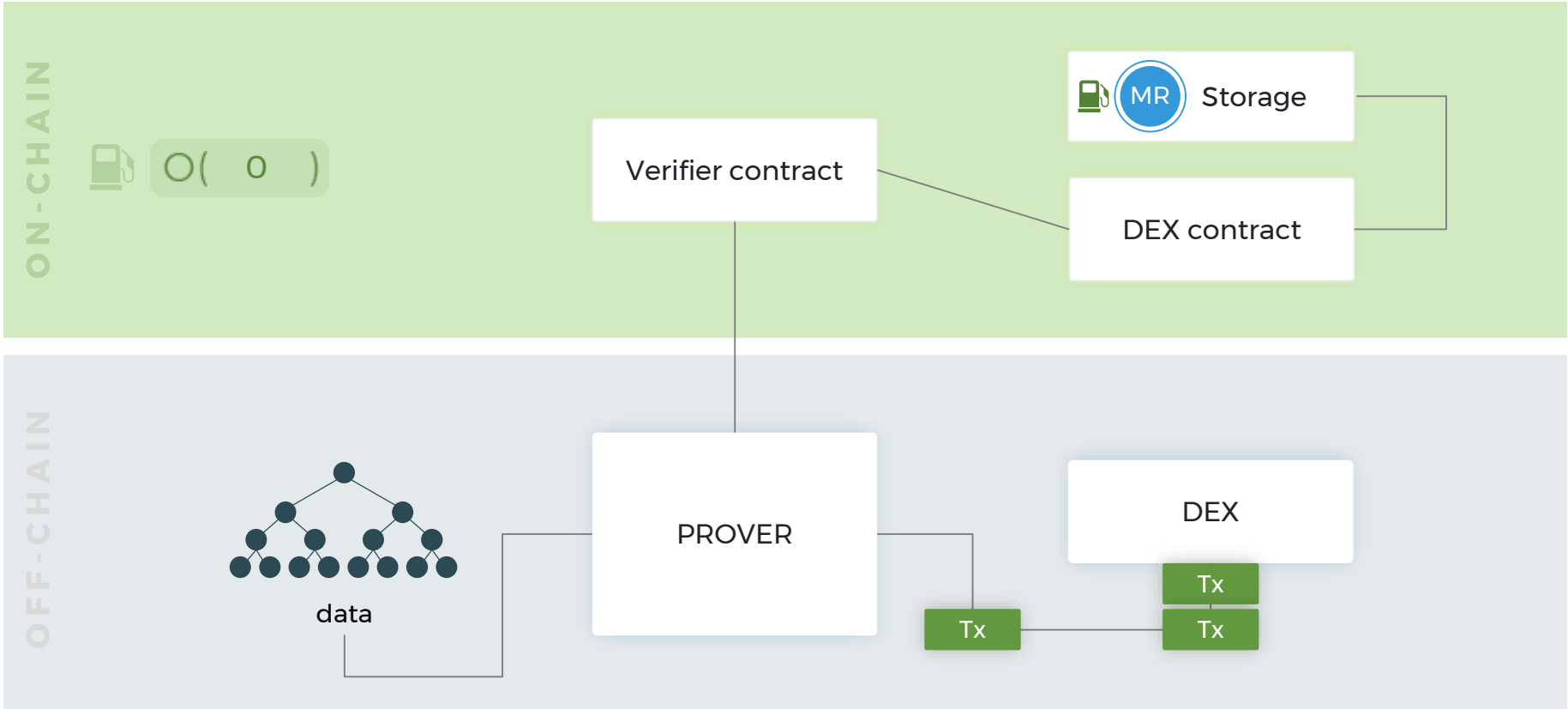


StarkDEX – High Level

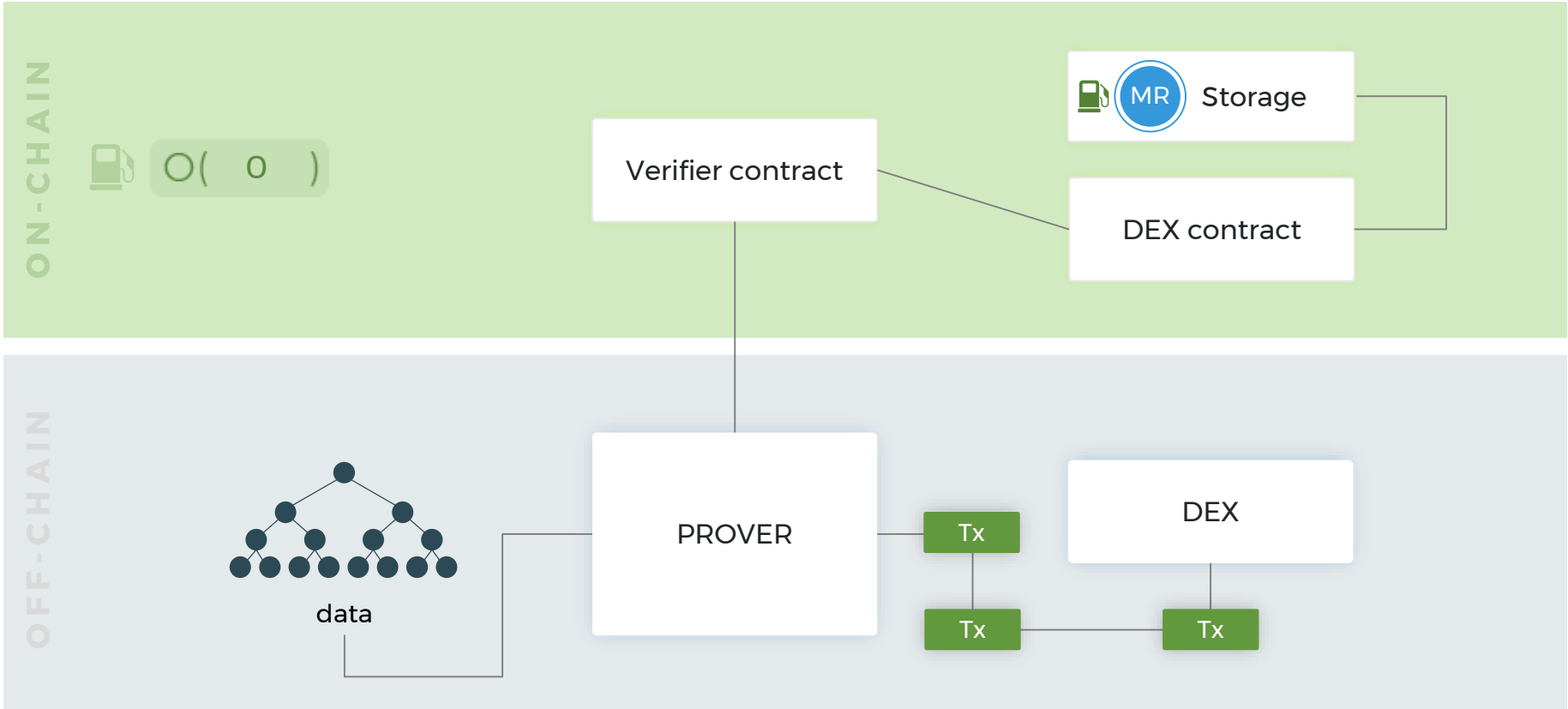


STARKWARE

StarkDEX – High Level

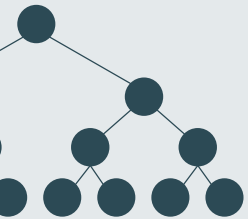


StarkDEX – High Level



Verifier contract

DEX contract



data

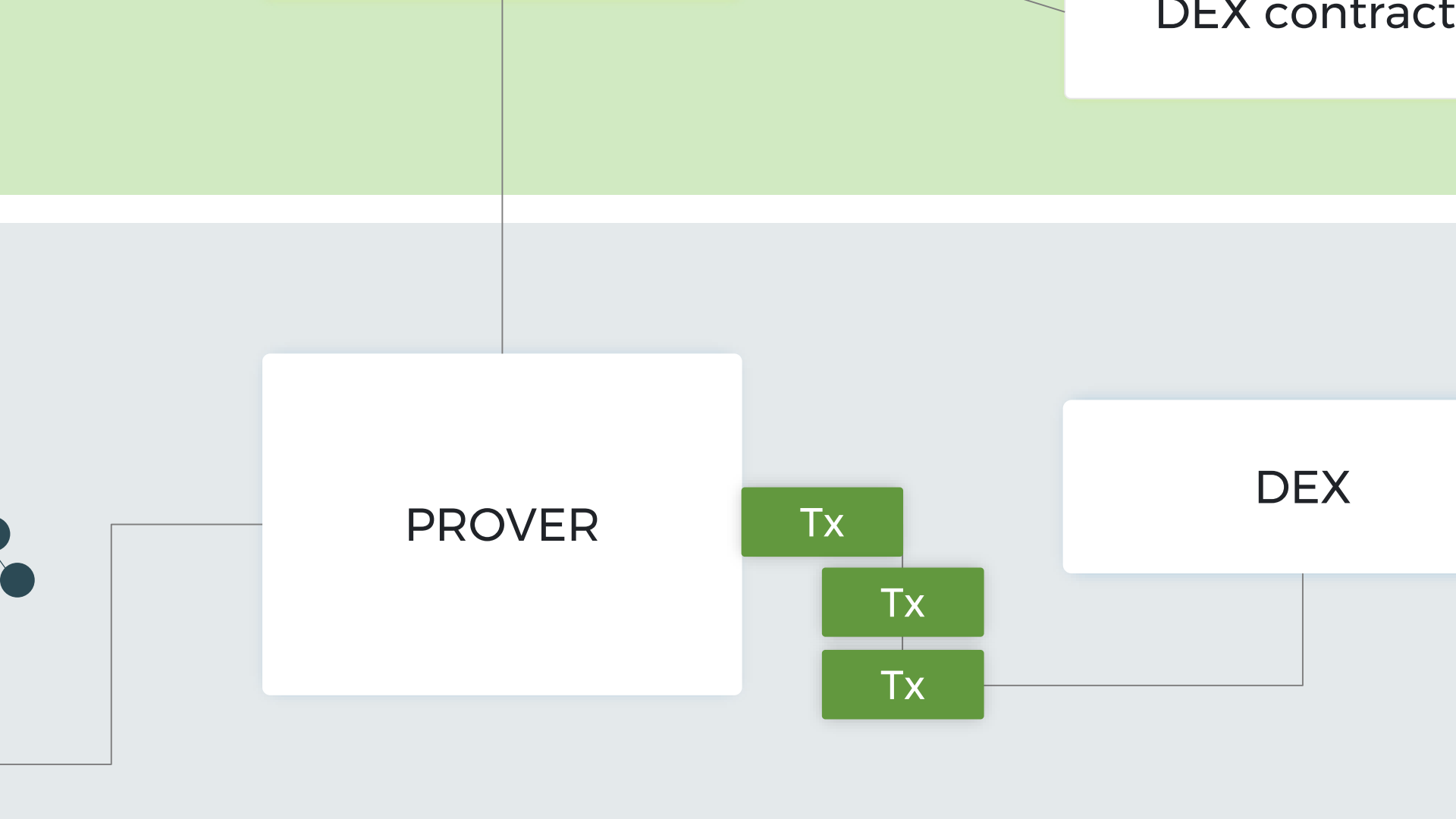
PROVER

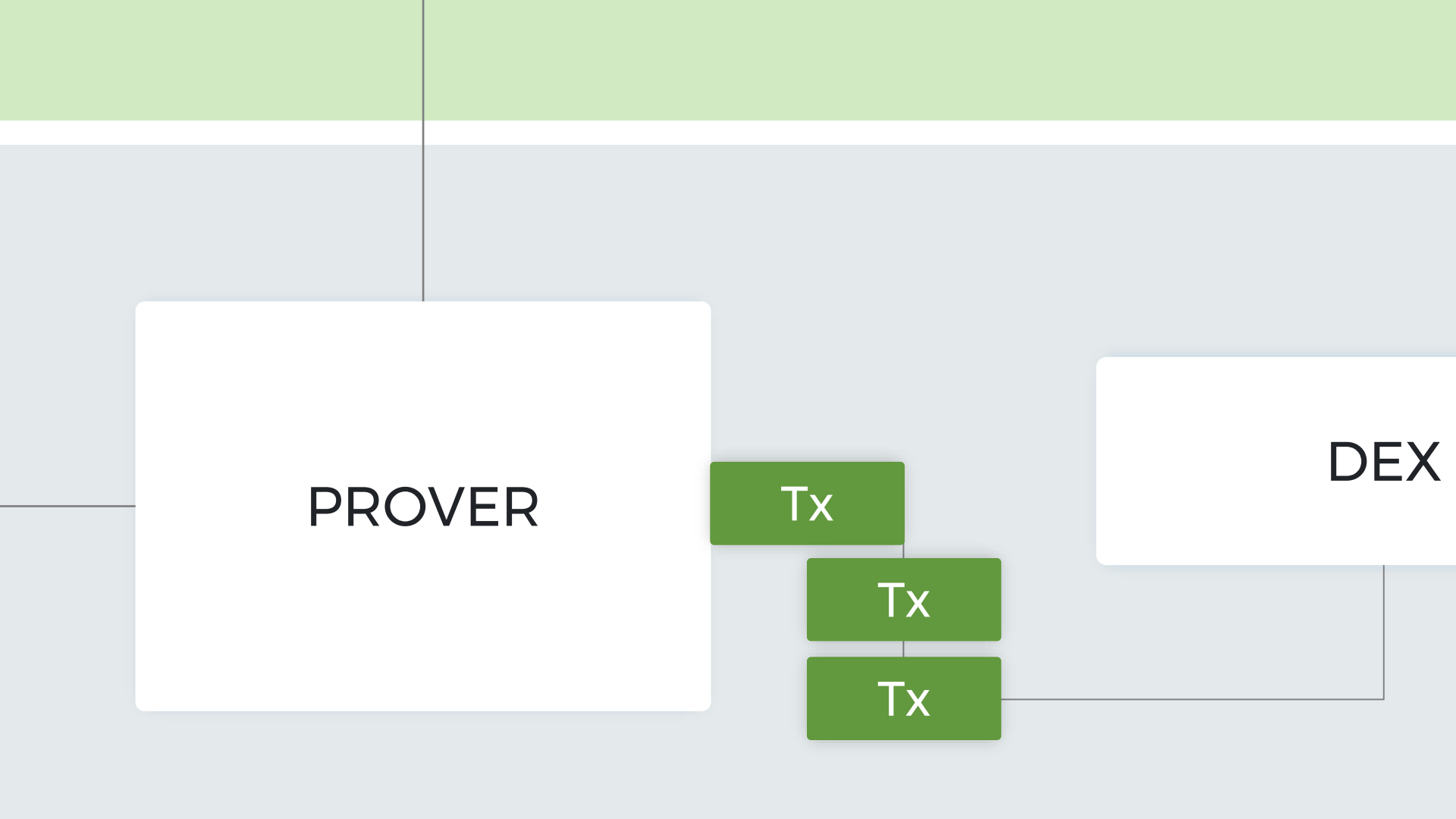
Tx

Tx

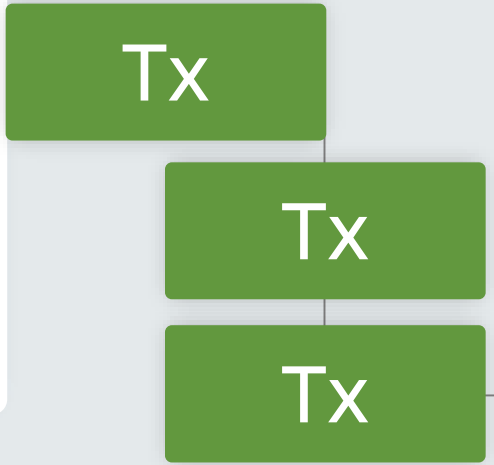
Tx

DEX

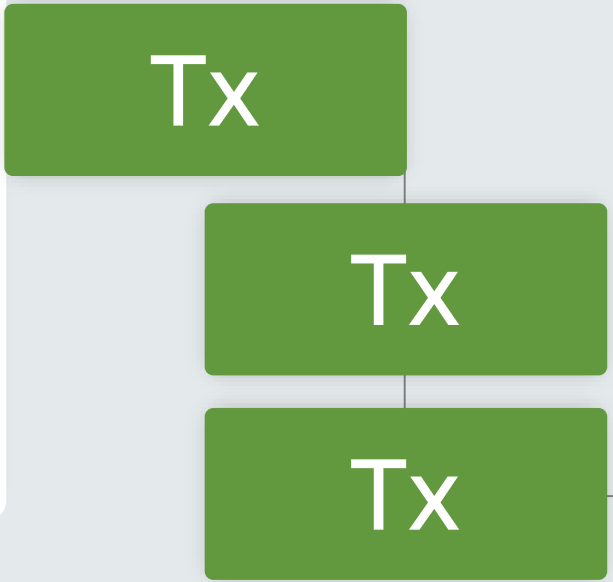

DEX contract
PROVER
Tx
Tx
Tx
DEX


PROVER
Tx
Tx
Tx
DEX

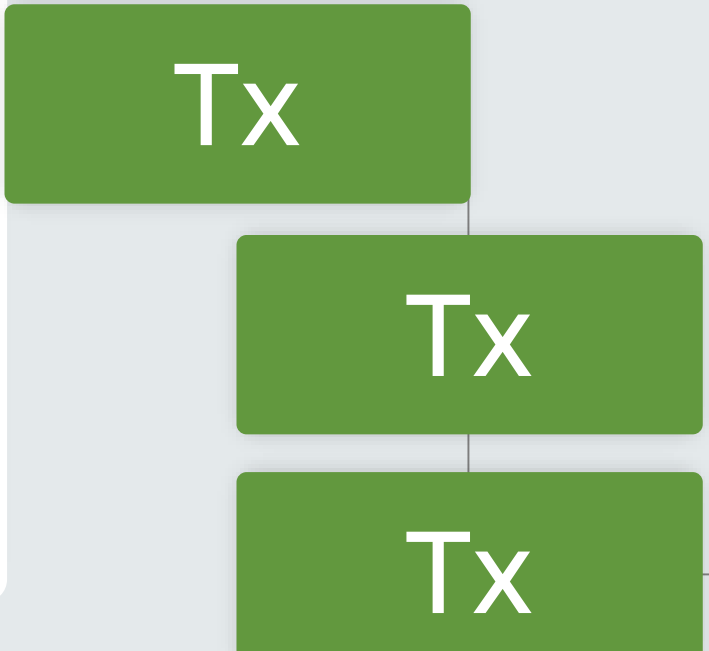
PROVER



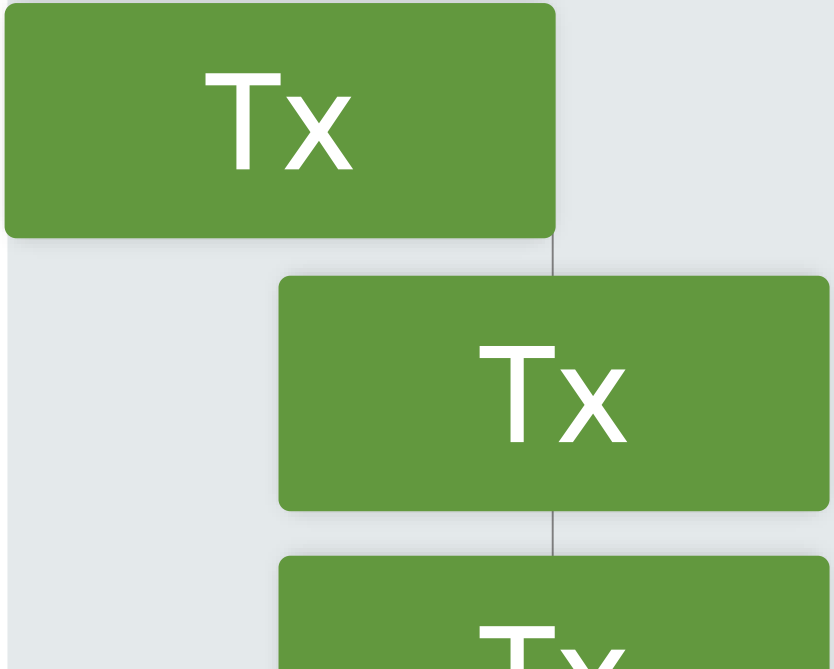
PROVER

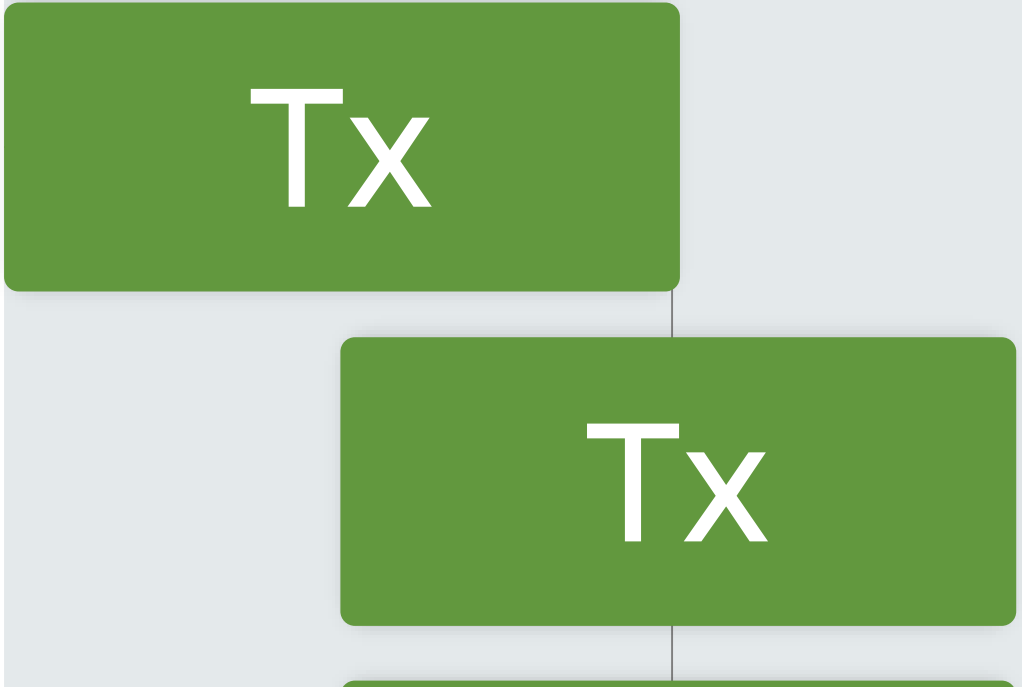


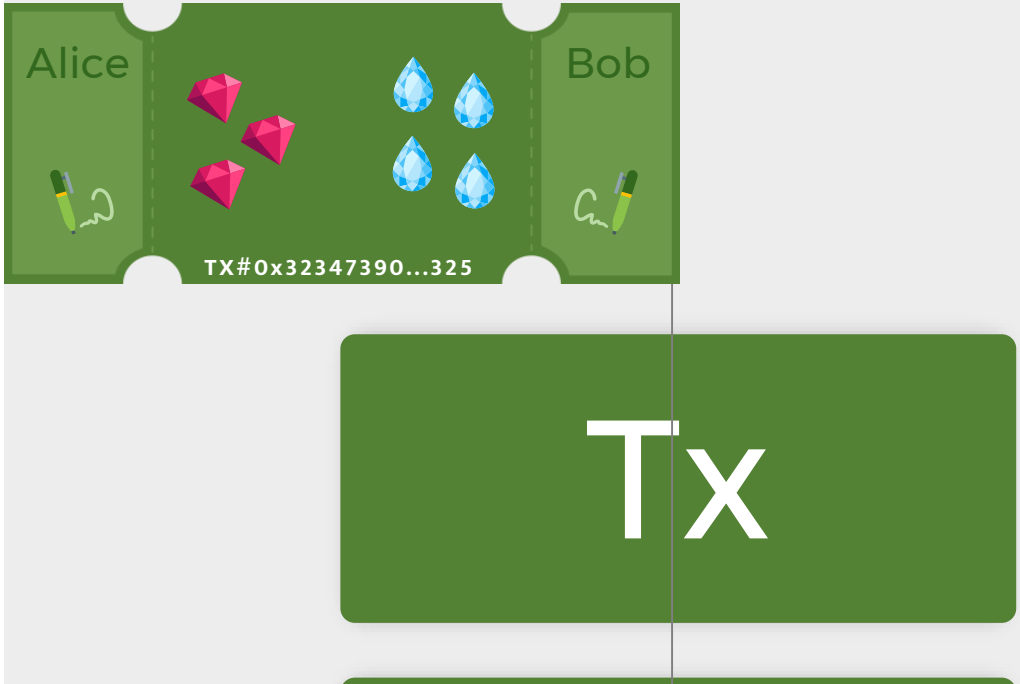
OVER



VER




Tx
Tx


Alice
Bob
TX#0x32347390...325
Tx

OVER

Tx

Tx

PROVER

Tx

Tx

Verifier Contract

PROVER

Tx

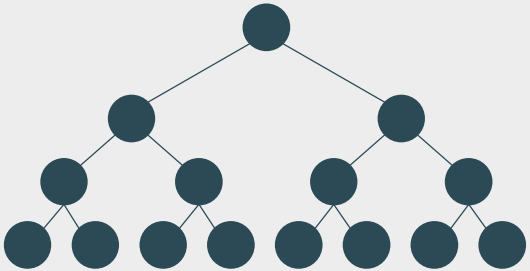
Tx

DEX

ON-CHAIN

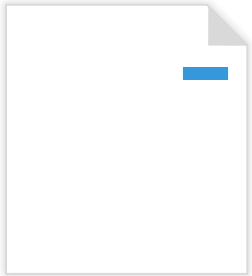
Verifier Contract

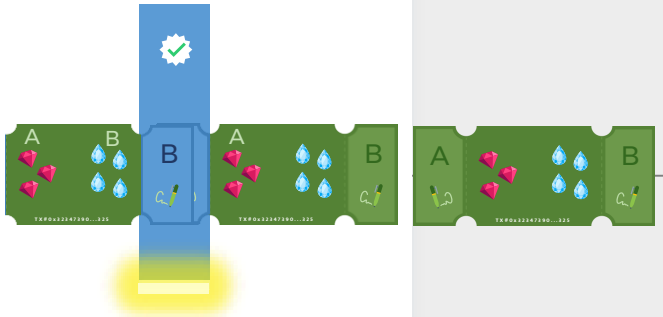
OFF-CHAIN



data

PROVER





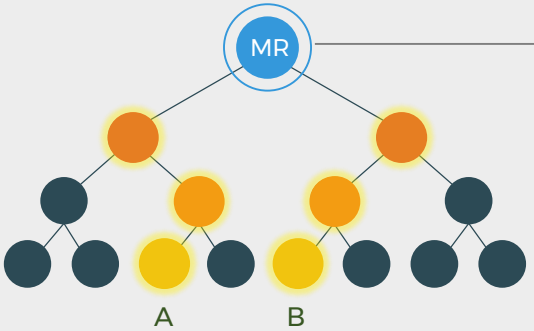
T

T

ON-CHAIN

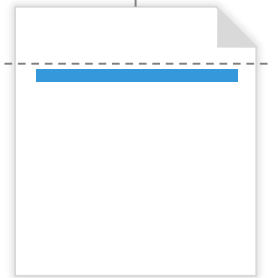
Verifier Contract

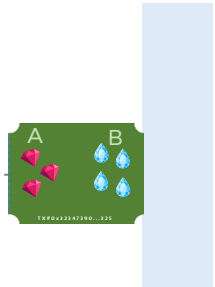
OFF-CHAIN



data

PROVER





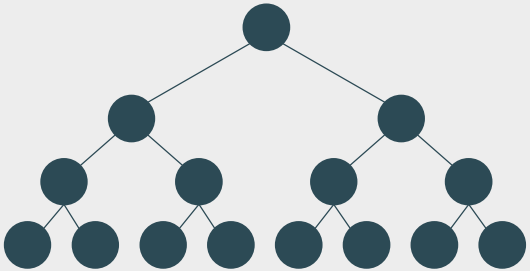
T

T

ON-CHAIN

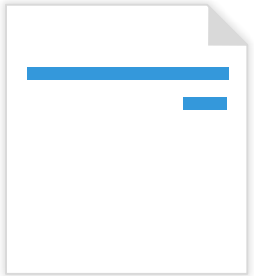
Verifier Contract

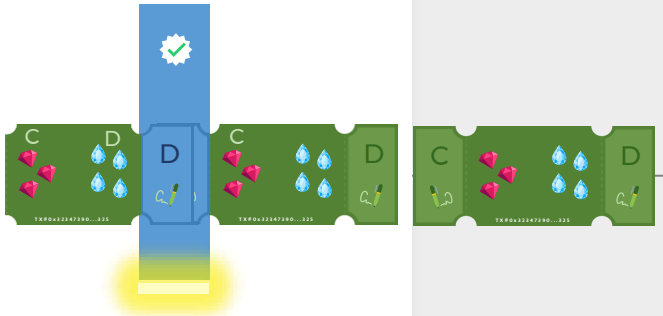
OFF-CHAIN



data

PROVER

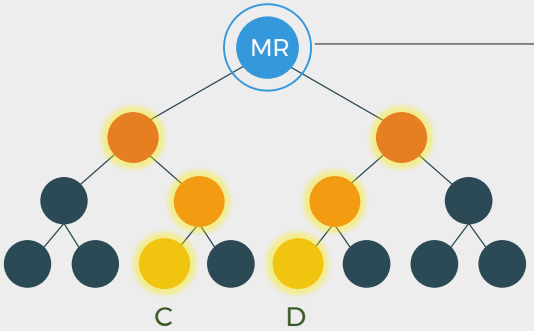




ON-CHAIN

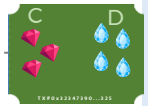
Verifier Contract

OFF-CHAIN



data

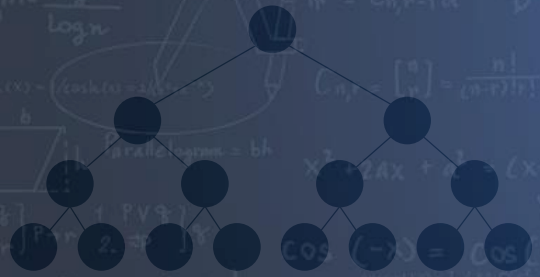
PROVER



T

T

Verifier Contract



data

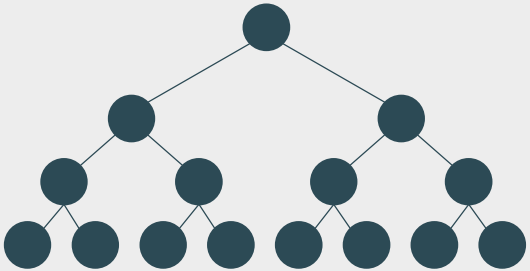
PROVER

PROOF

ON-CHAIN

Verifier Contract

OFF-CHAIN



data

PROVER

MR

PROOF

MR

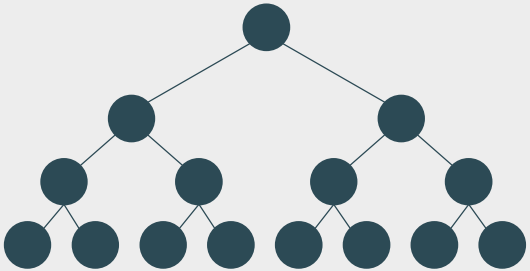
T

ON-CHAIN

O( )

Verifier Contract

OFF-CHAIN



data

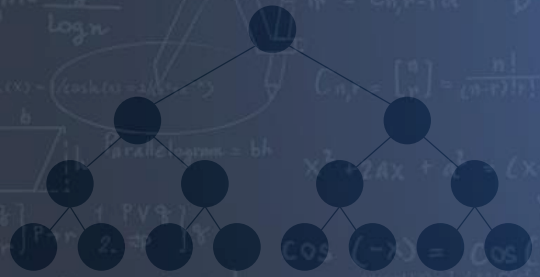
PROVER

MR PROOF

T

Verifier Contract

PROVER



data

ON-CHAIN

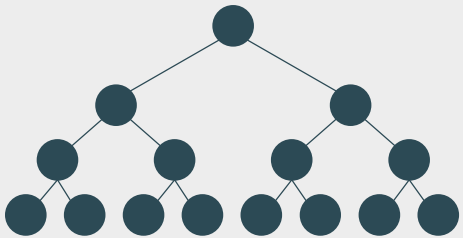
O( )

MR Verifier Contract

DEX Con

Storag

OFF-CHAIN

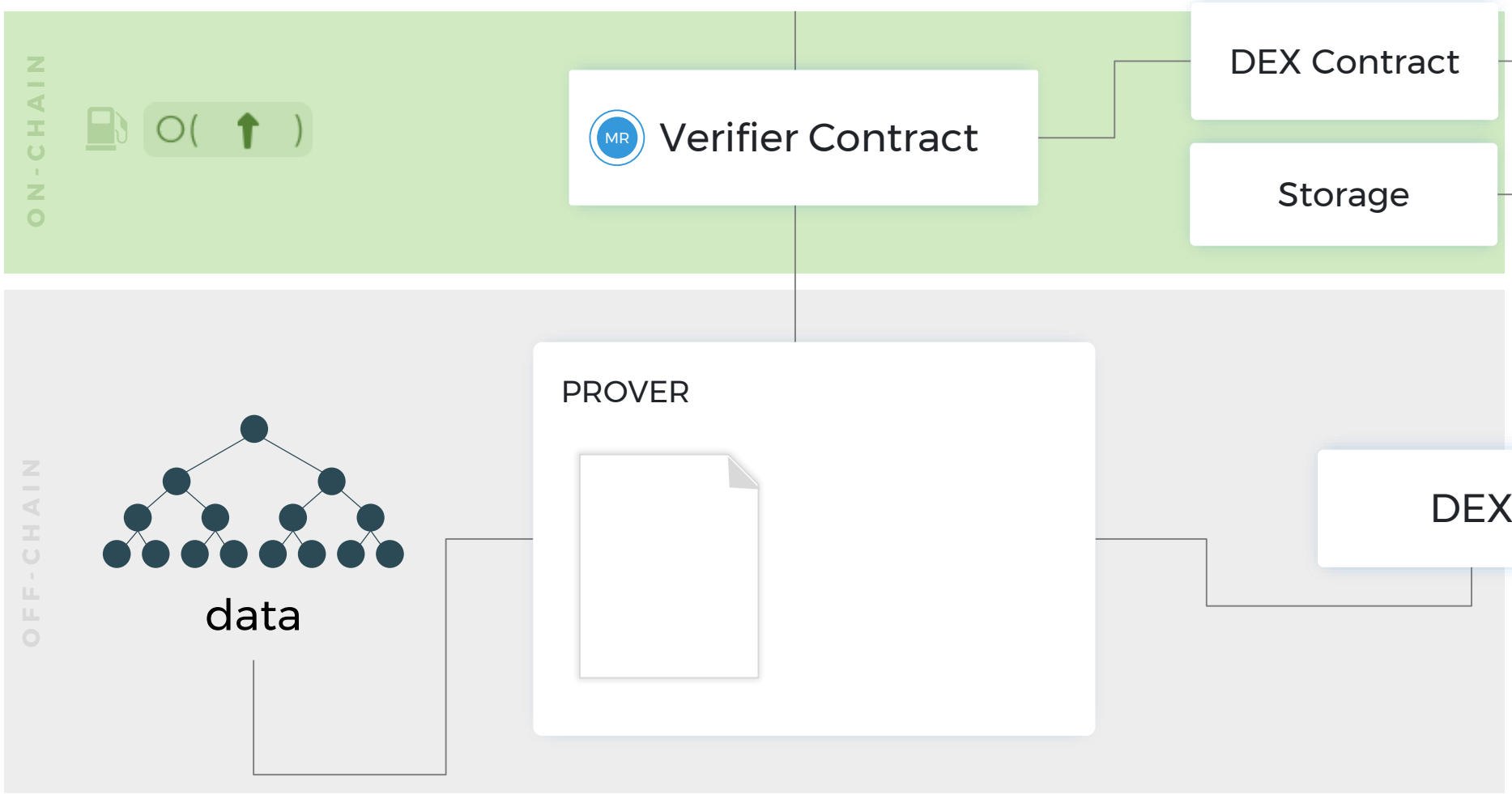


data

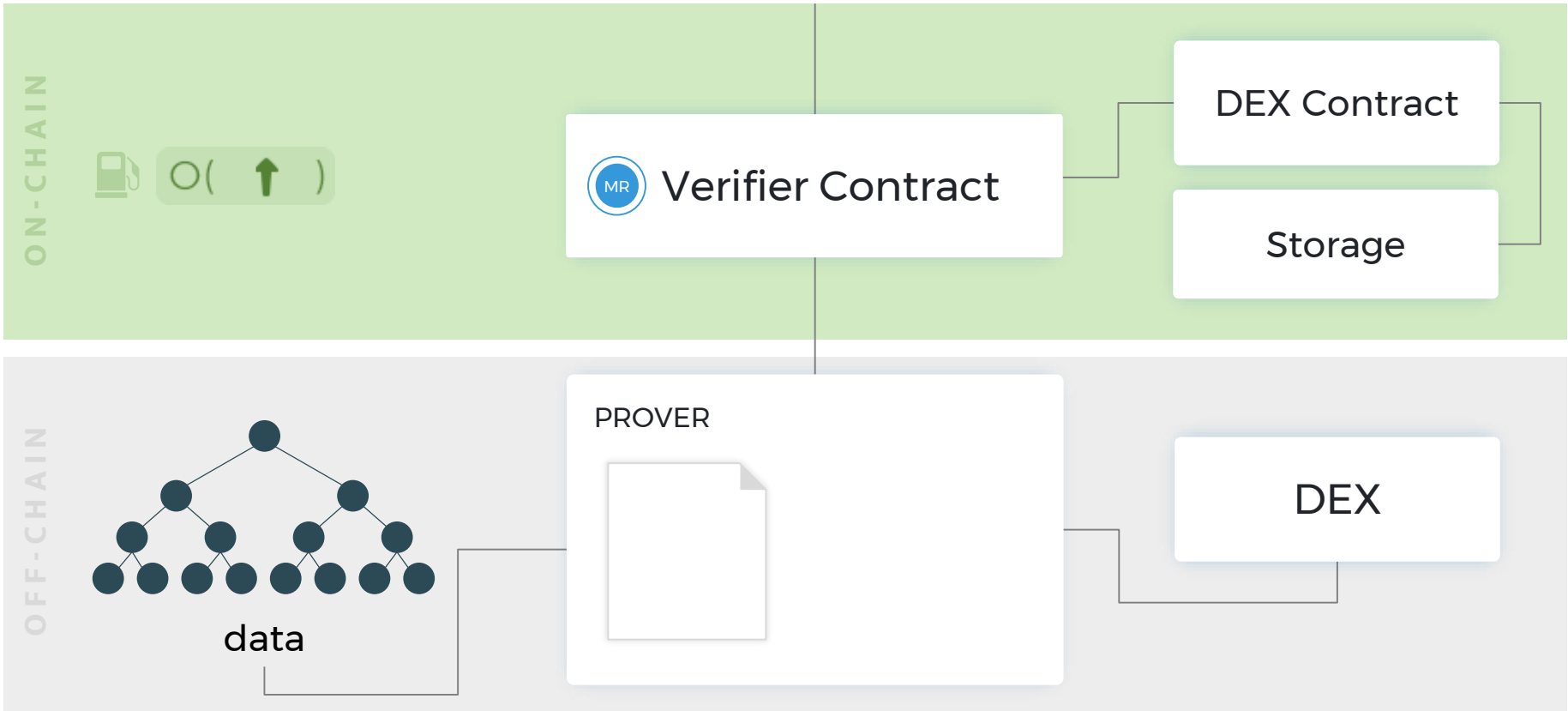
PROVER

D

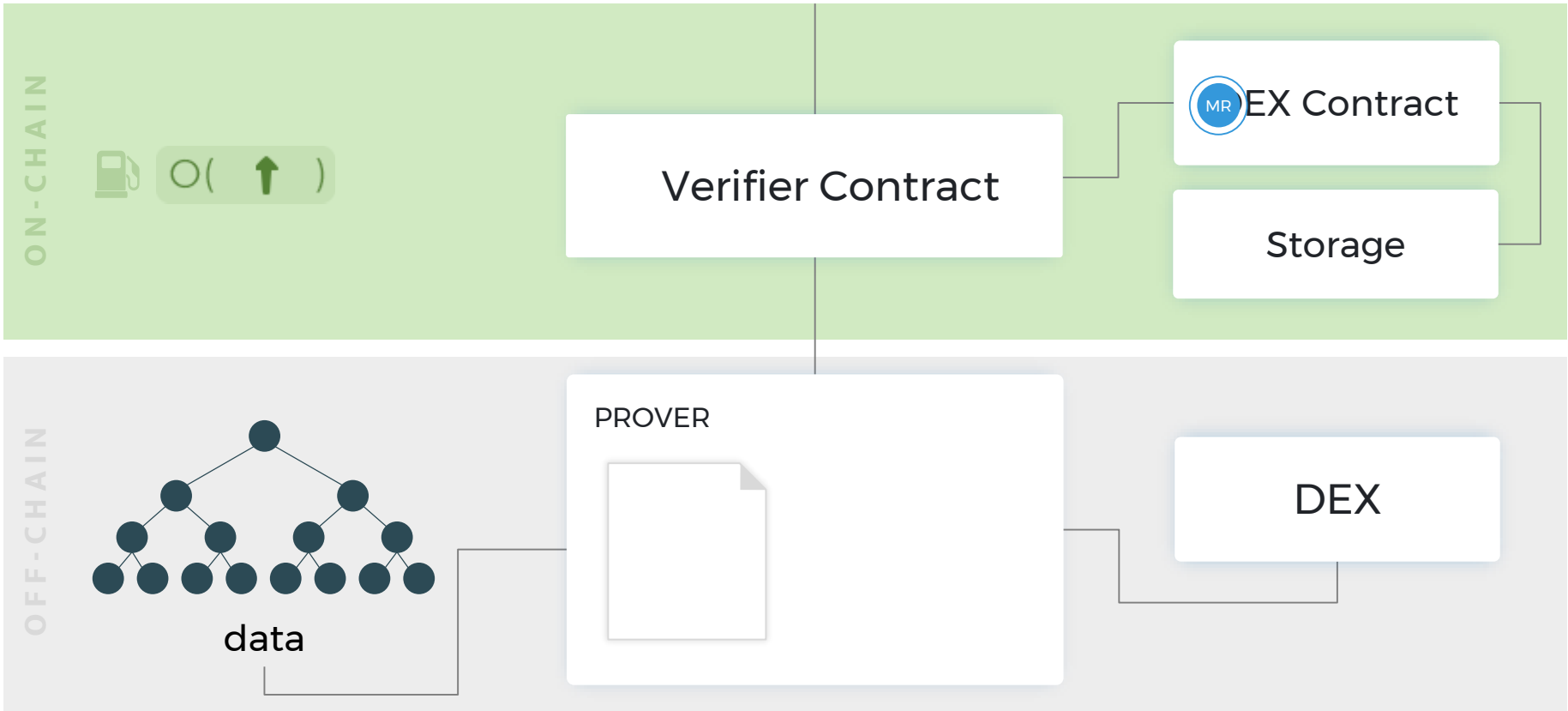
Stateful DEX - TX Anatomy



Starked Dex - Tx Anatomy



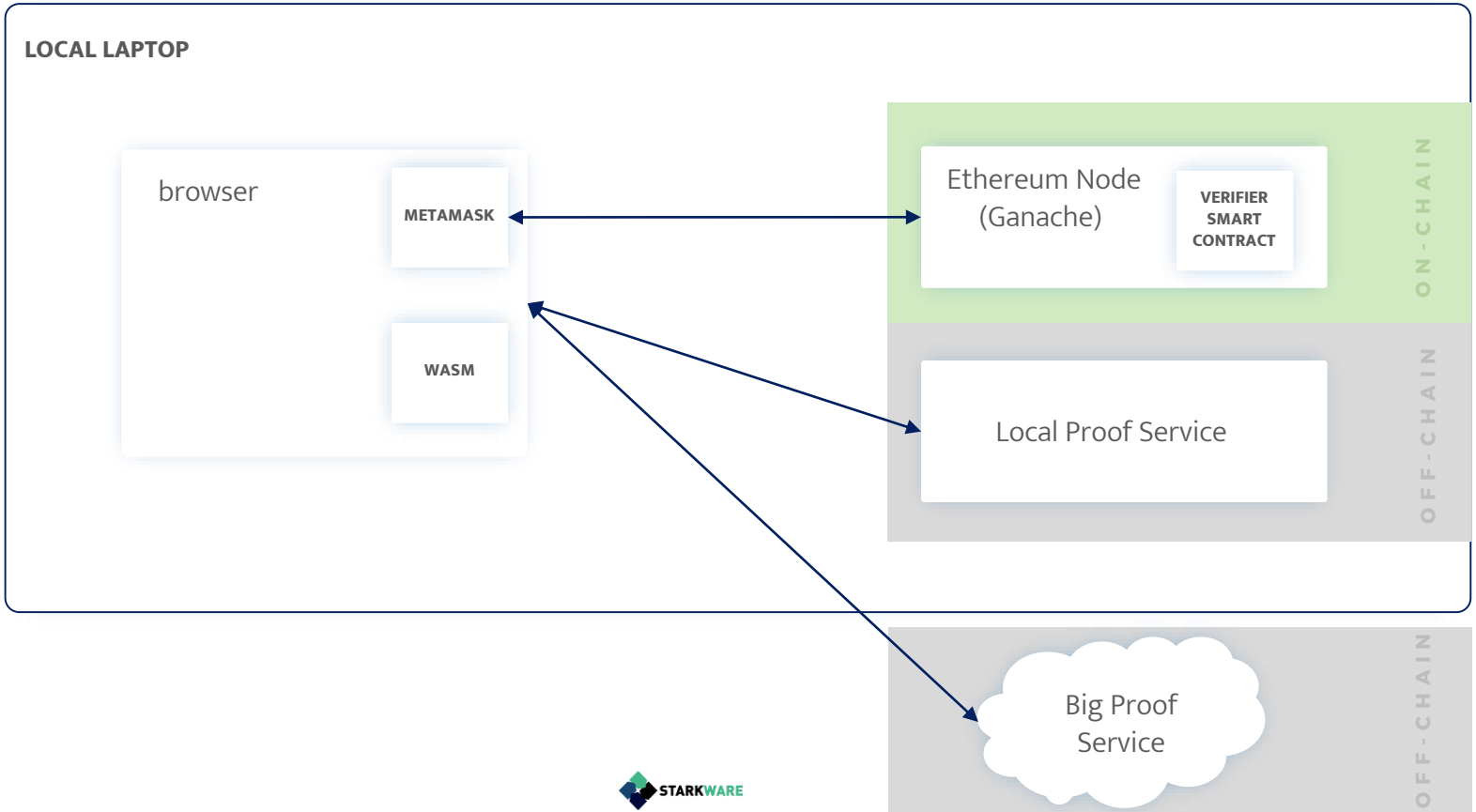
Starked Dex - Tx Anatomy



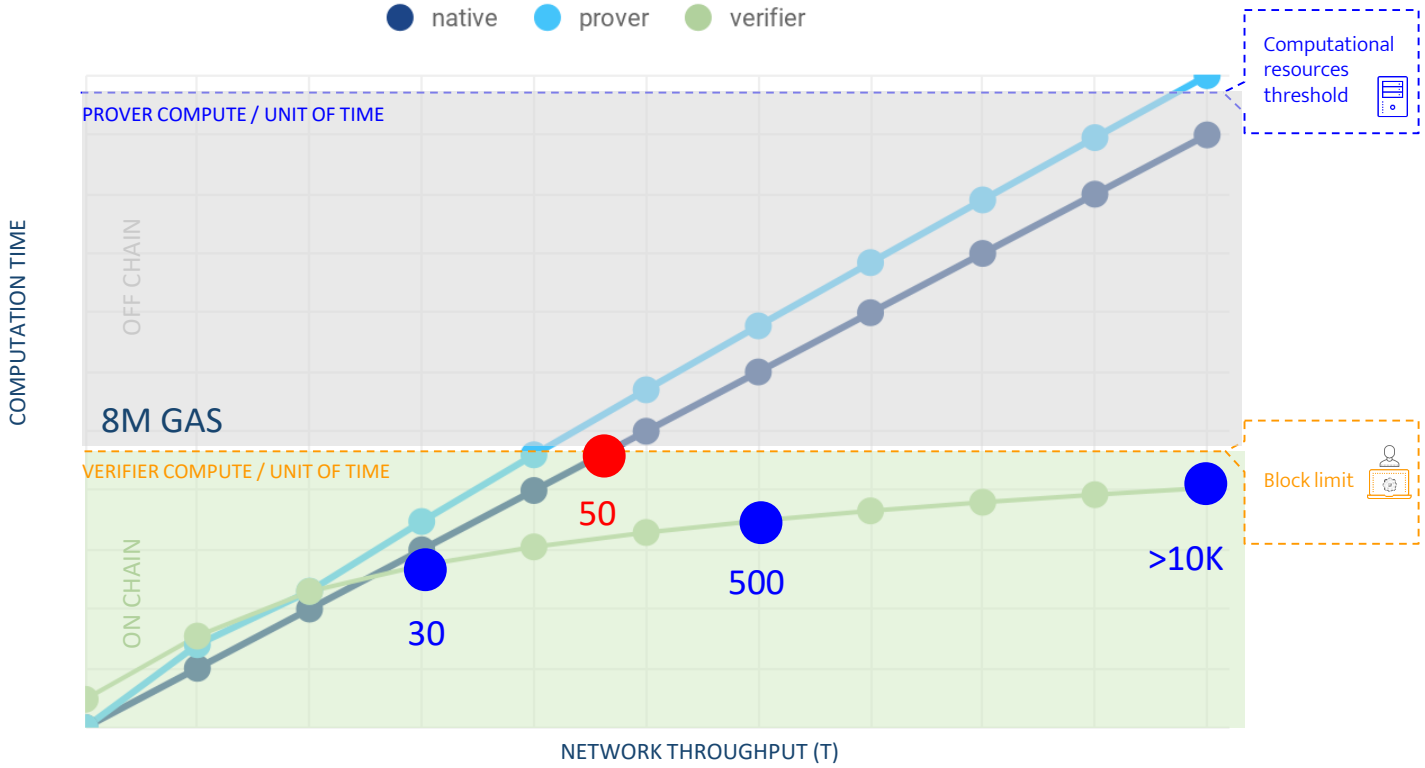
STARKWARE

ONE MORE THING...

DEMO


LOCAL LAPTOP
browser
METAMASK
WASM
Ethereum Node
(Ganache)
VERIFIER
SMART
CONTRACT
ON-CHAIN
Local Proof Service
OFF-CHAIN
Big Proof
Service
OFF-CHAIN

STARK Scalability



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)

Blockchain-Bound → **AWS-Bound**

THANK YOU