# THE STARK TRUTH ABOUT DEXes

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

STARKWARE

# 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<br>(banks, pension funds...) |
|---|---|
| TRUST | assumption |
| VERIFY | delegated to auditors, accountants, regulators |

## DELEGATED ACCOUNTABILITY

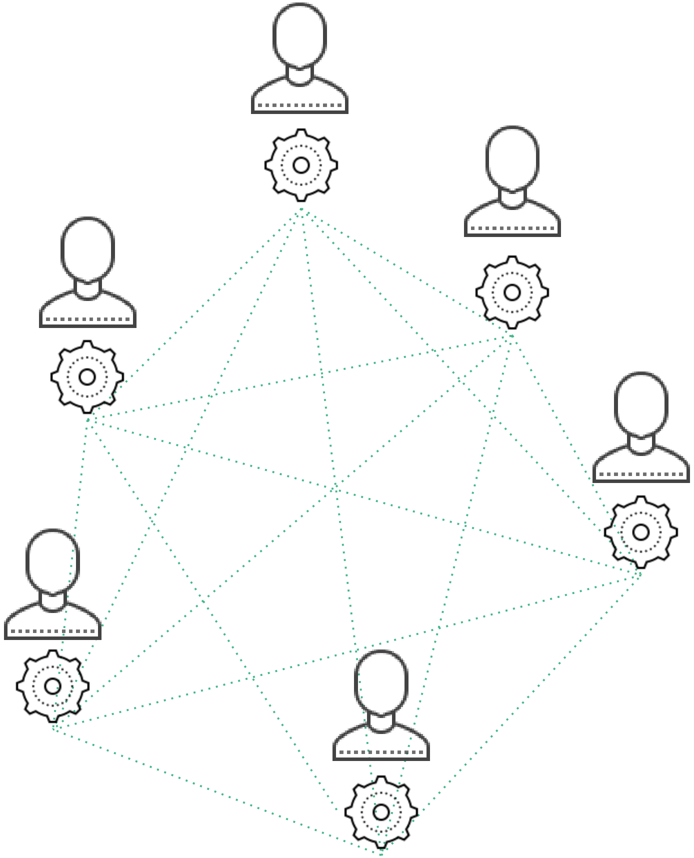
### OLD WORLD

(banks, pension funds...)

## INCLUSIVE ACCOUNTABILITY

### NEW WORLD

| | DELEGATED ACCOUNTABILITY | INCLUSIVE ACCOUNTABILITY | |
|---|---|---|---|
| TRUST | assumption | don’t trust, verify | TRUST |
| VERIFY | delegated to auditors, accountants, regulators | | |



# INCLUSIVE ACCOUNTABILITY

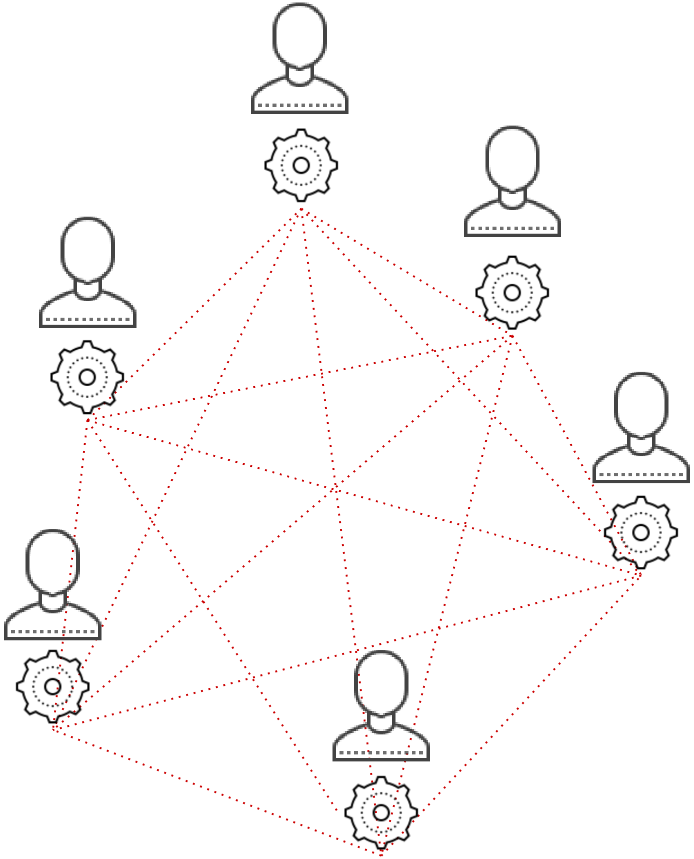
## NEW WORLD

don't trust, verify

TRUST

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

VERIFY

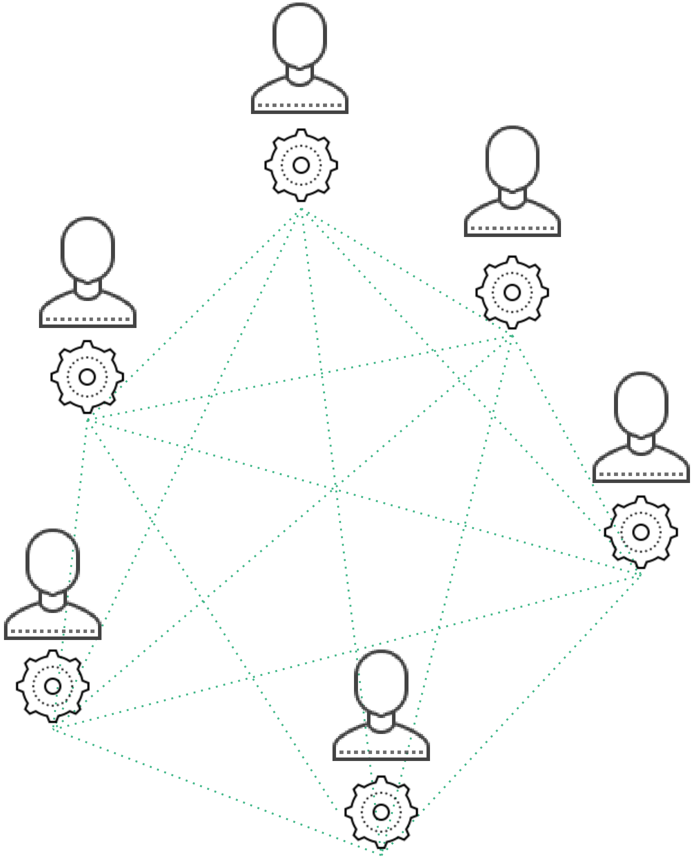


# INCLUSIVE ACCOUNTABILITY

## 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

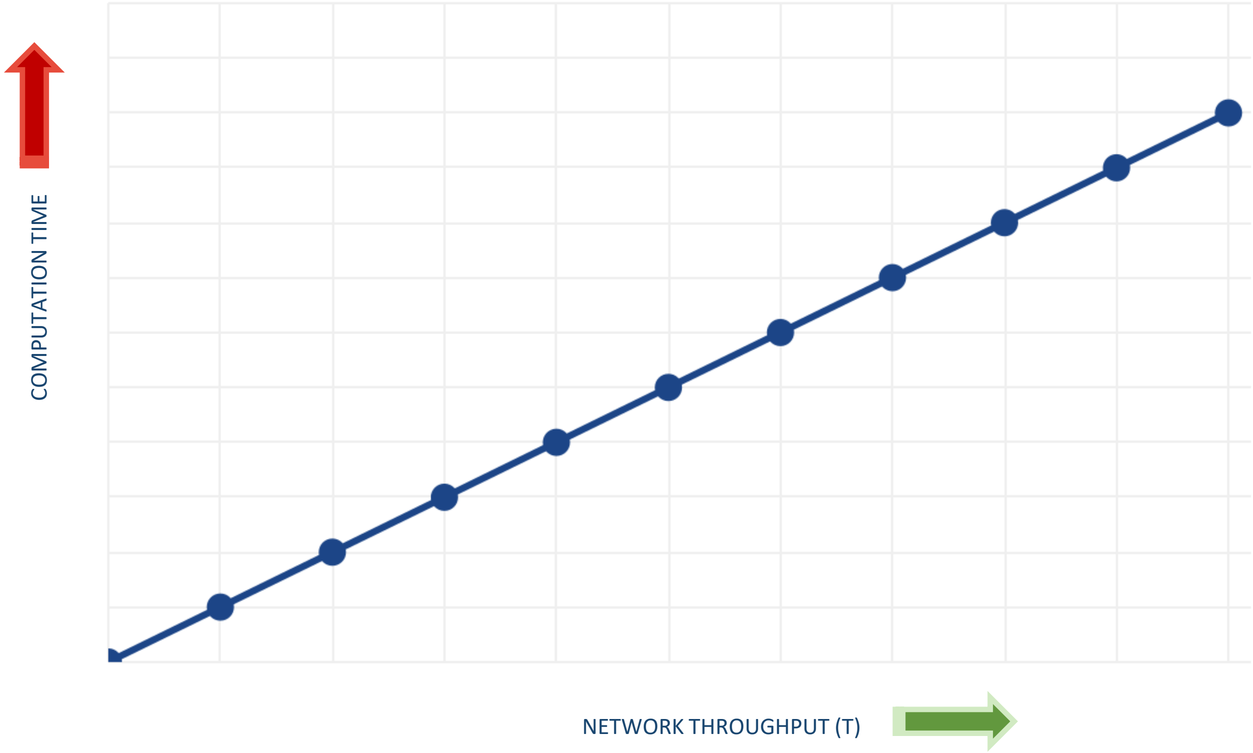
require small throughput to
include accountability on
weaker devices (i.e: laptop)

SCALABILITY

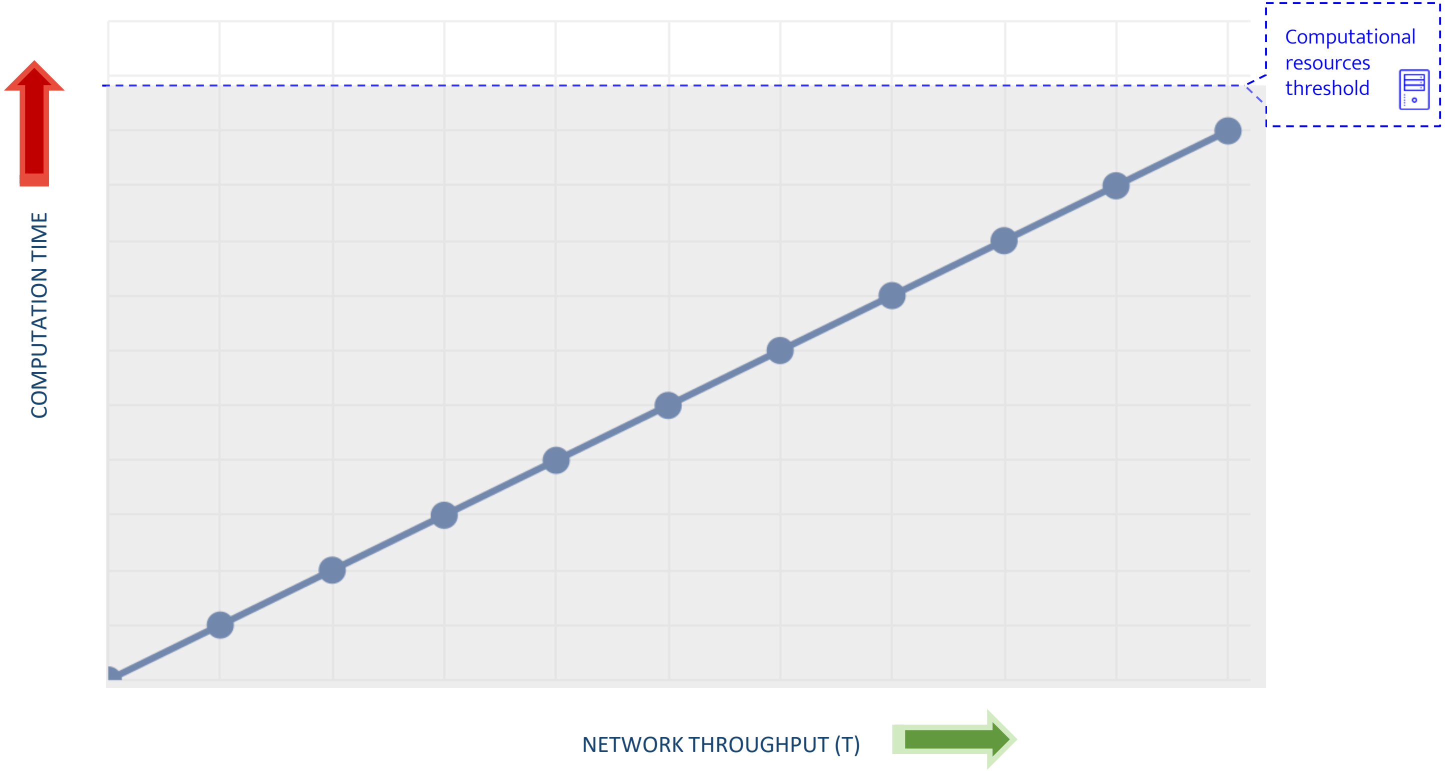
S == scalability

ZK-STARKs

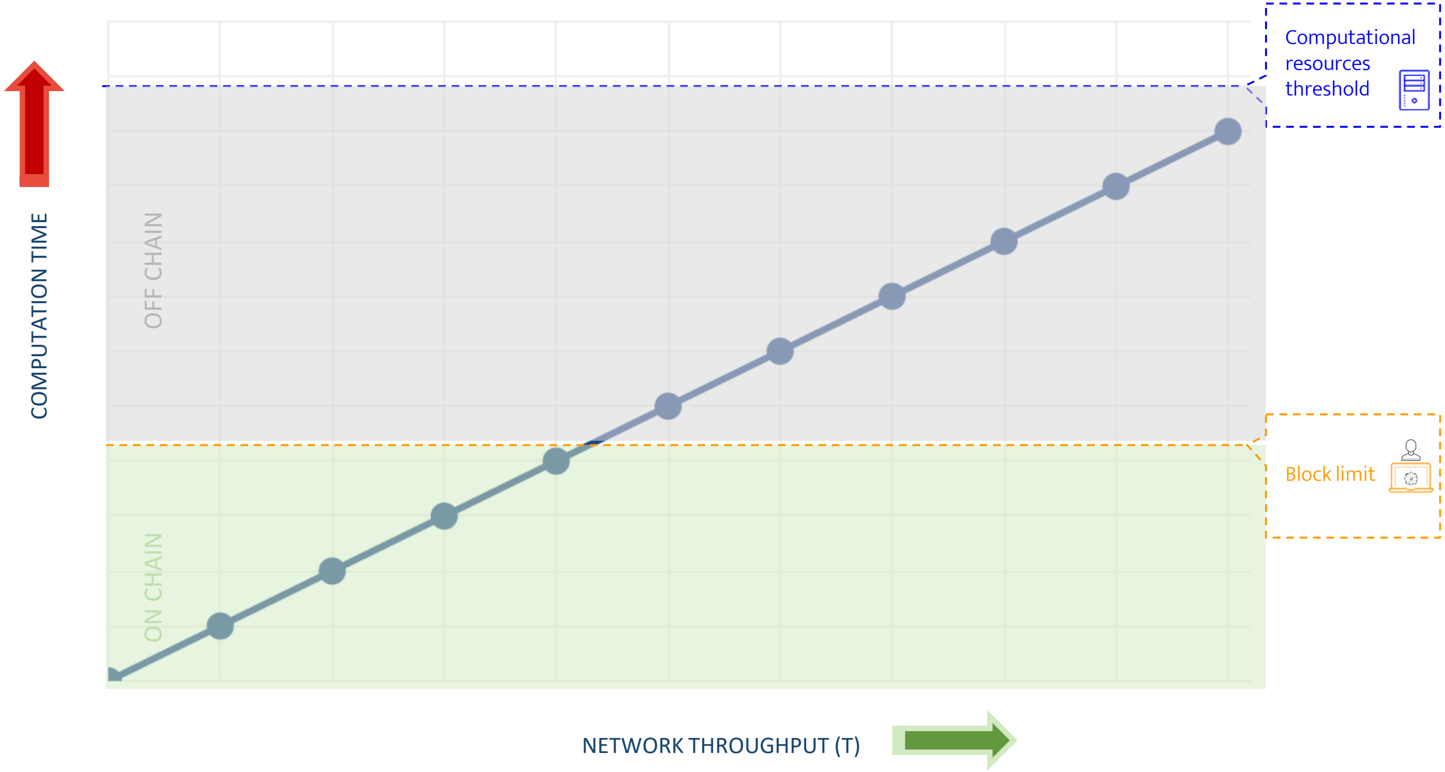
# Inclusive Accountability - Scalability Problem



# Inclusive Accountability - Scalability Problem



# Inclusive Accountability - Scalability Problem

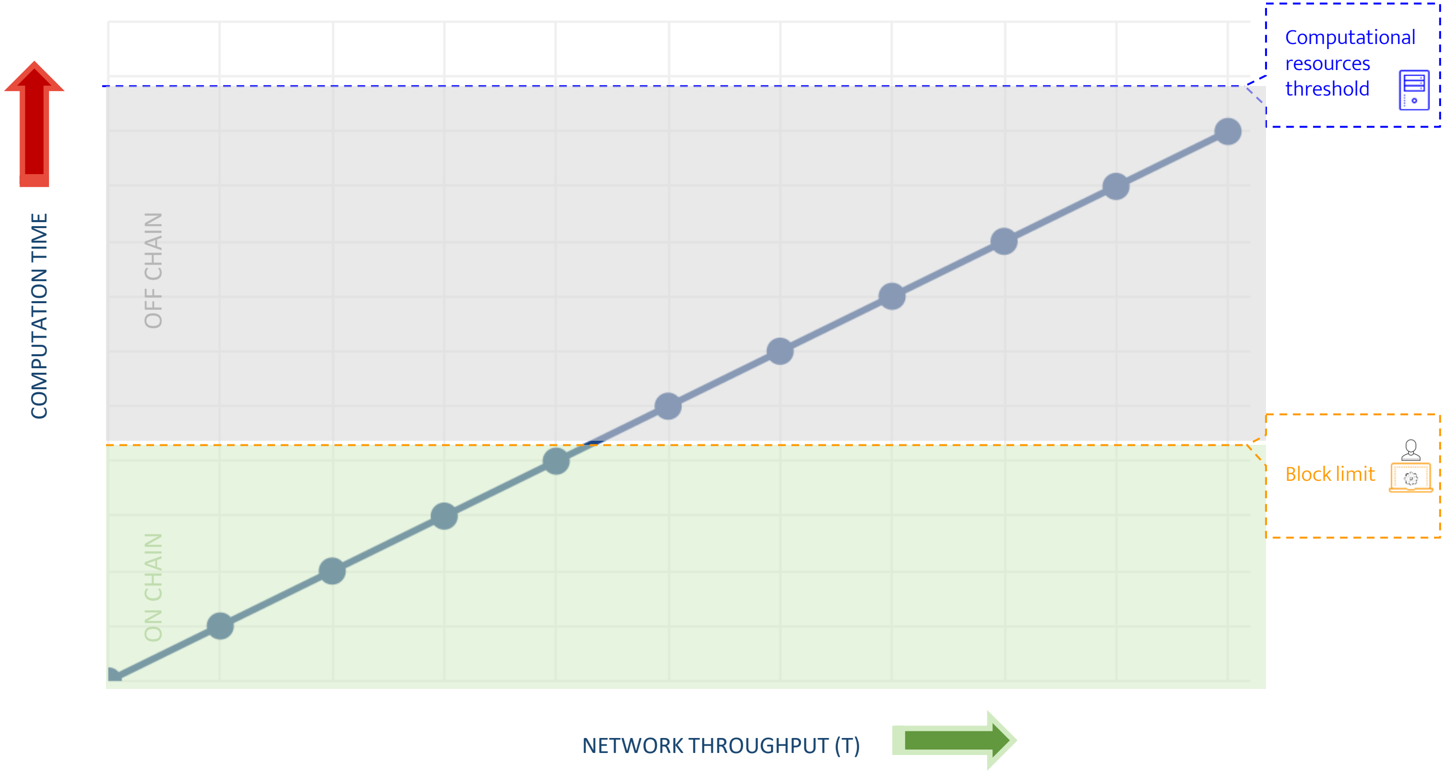


# STARK Scalability

Prover time is nearly linear in T

&

Verifier time exponentially smaller than T

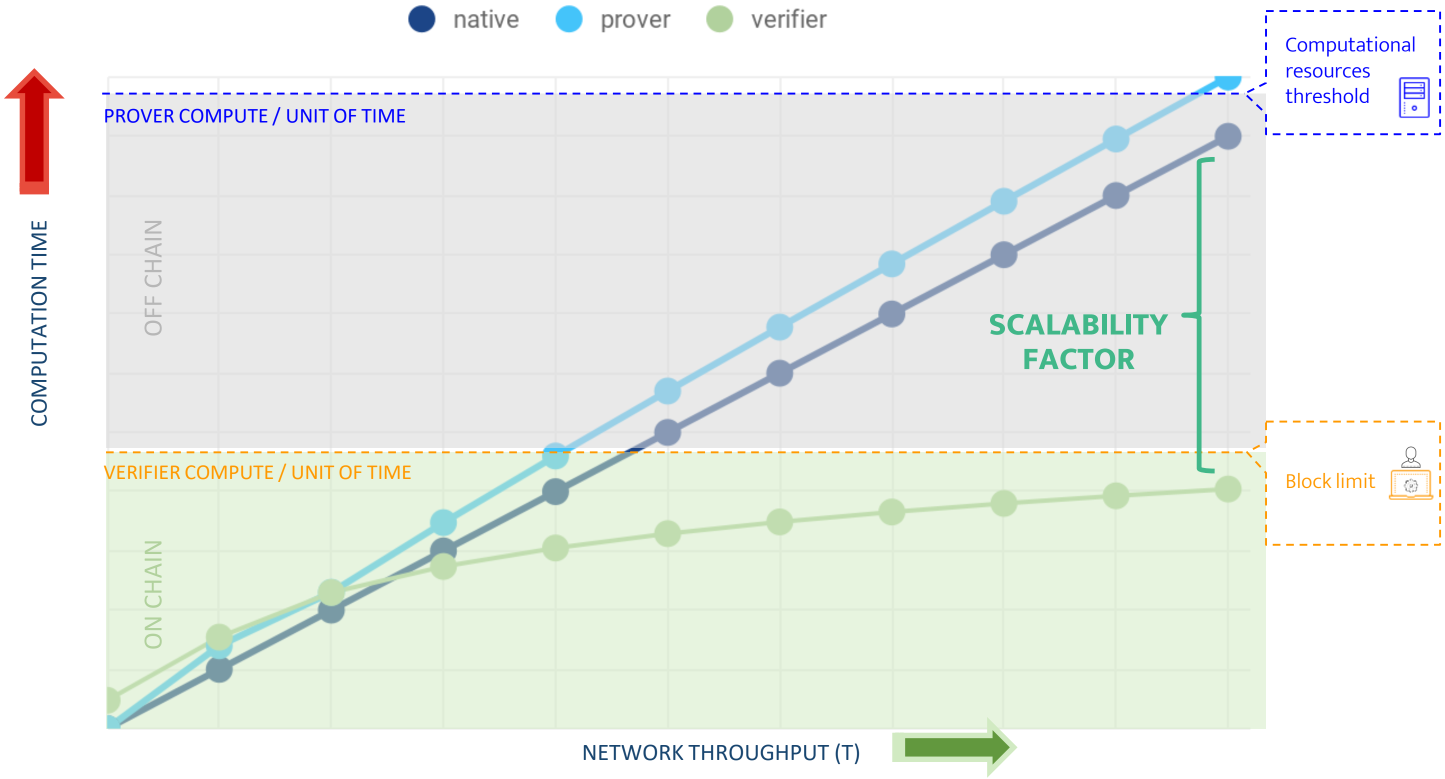


# STARK Scalability

Prover time is nearly linear in T

&

Verifier time exponentially smaller than T



STARKWARE

# STARK & Other ZKP Systems

BulletProof

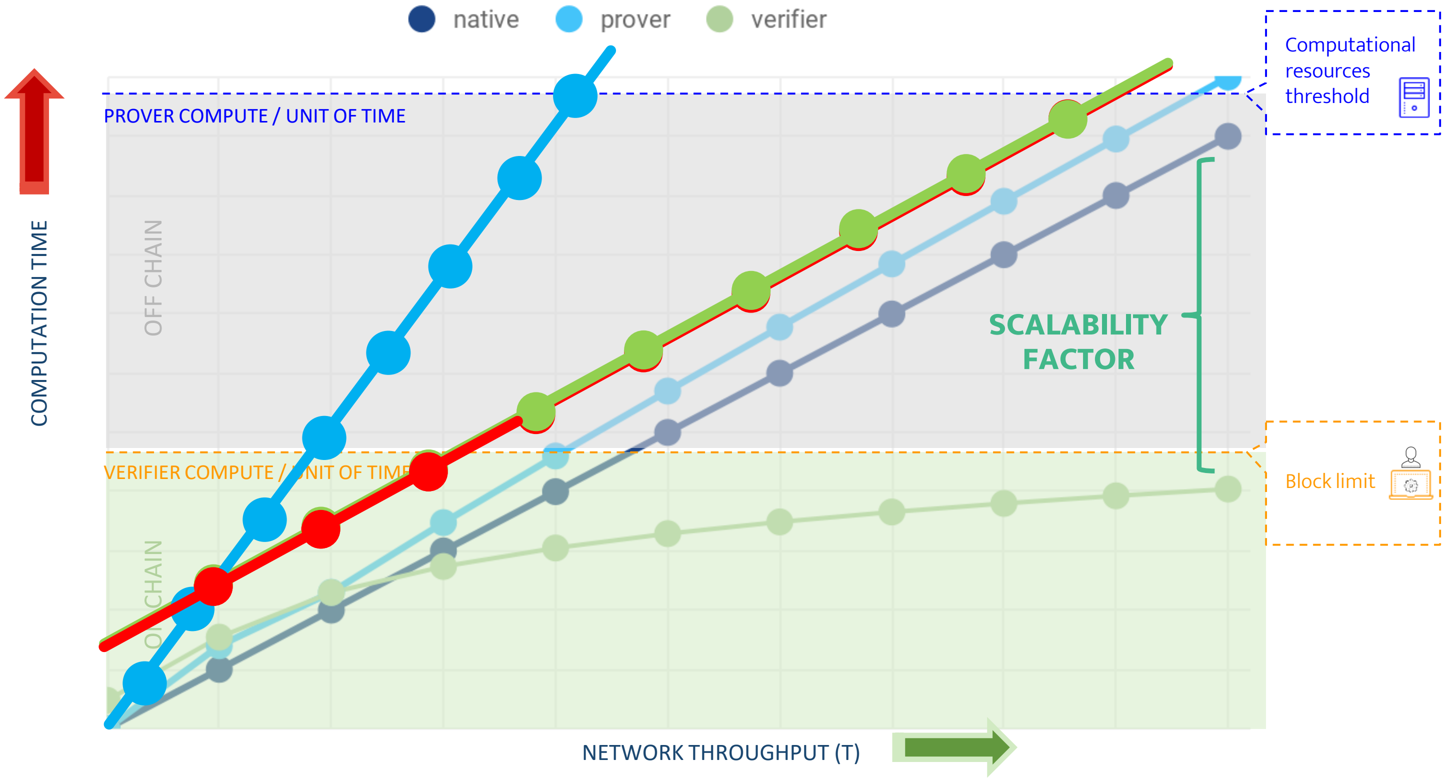
Verifier time scales linearly

SNARK

Trusted setup scales linearly

Recursive SNARK

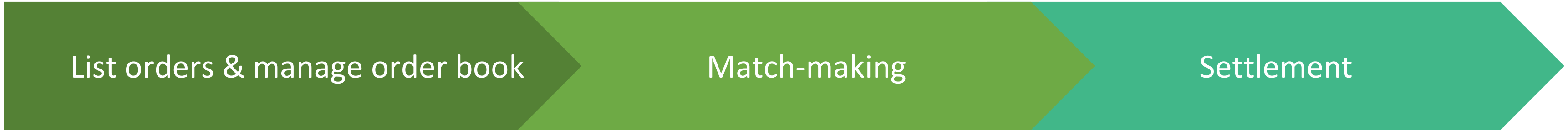
Trusted setup, inefficient prover



STARKWARE

# DEXes and Scalability

# Exchange:  the 3-Act Play



List orders & manage order book

Match-making

Settlement

# Exchange:  the 3-Act Play

List orders & manage order book

Match-making

Settlement

|  | Centralized Exchange<br>(CEX) | Decentralized Exchange<br>(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

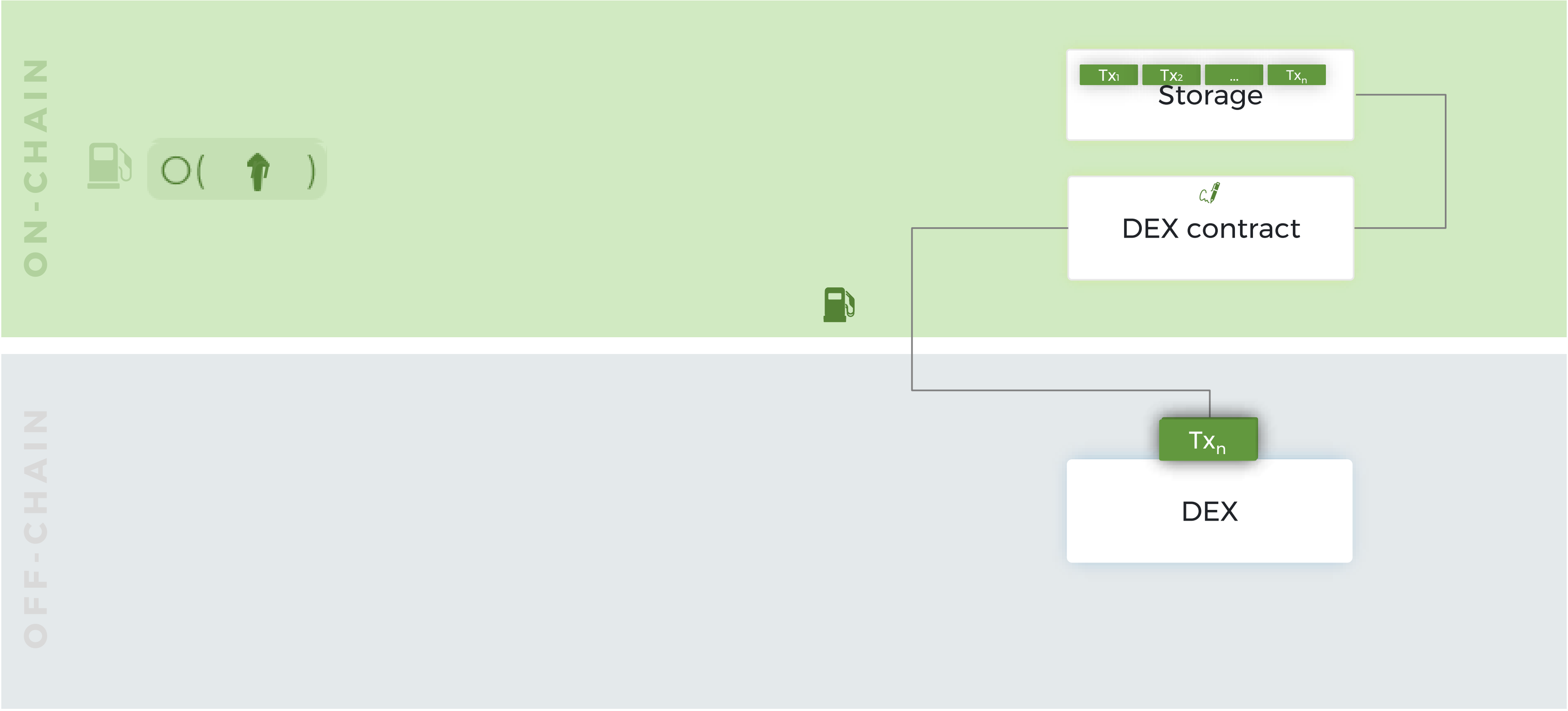
# StarkDEX

# StarkDEX Overview

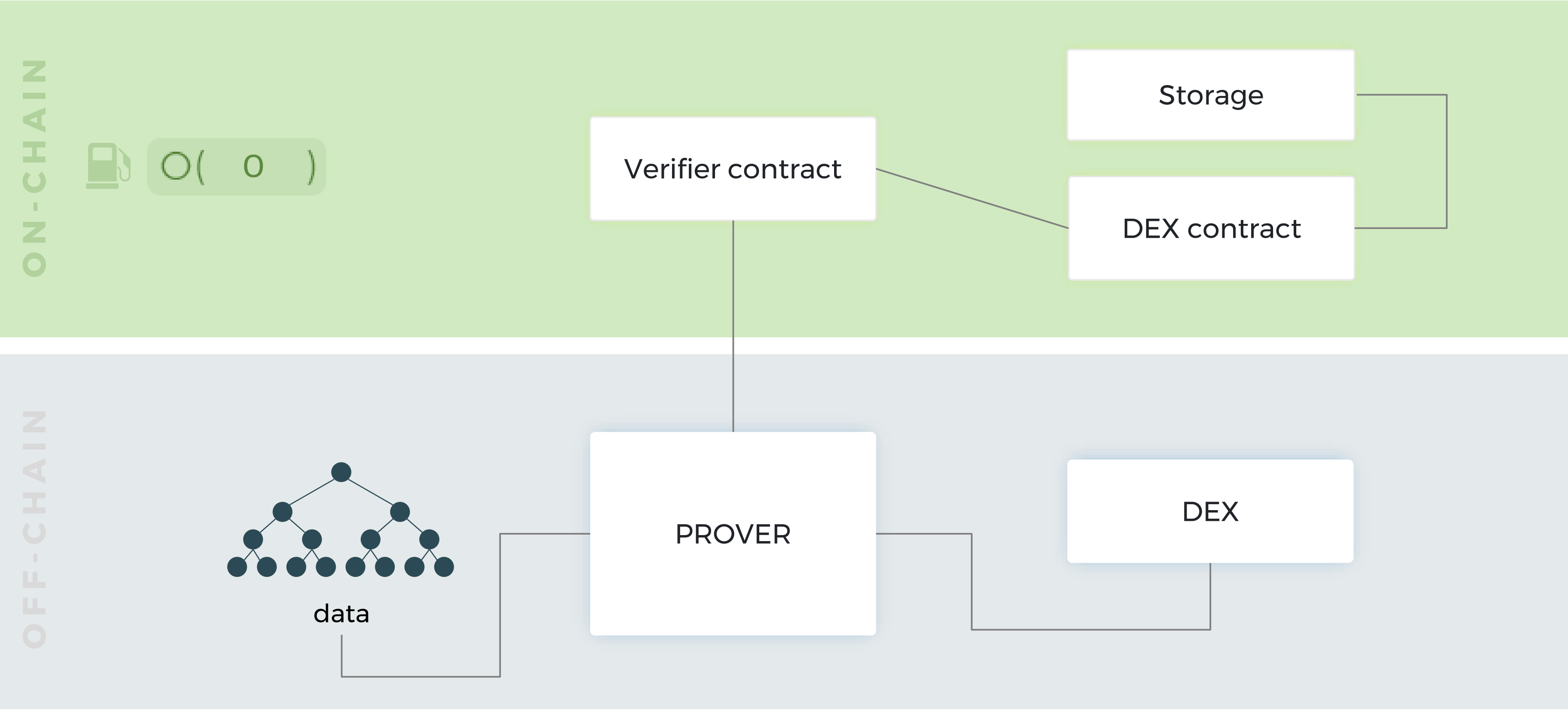
ON-CHAIN

OFF-CHAIN

# Current DEXes

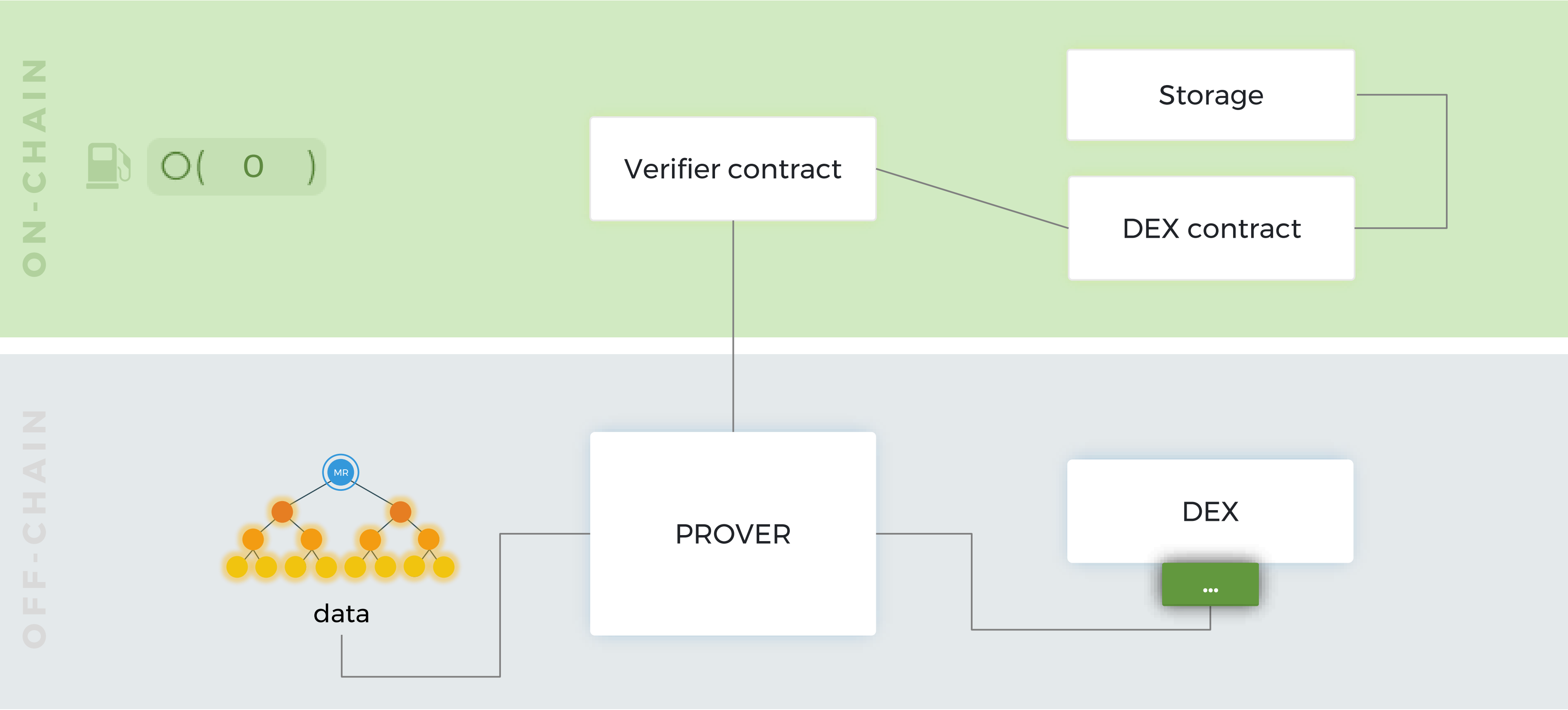


# StarkDEX – High Level



STARKWARE

# StarkDEX – High Level



ON-CHAIN

O( 0 )

Verifier contract

Storage

DEX contract

OFF-CHAIN

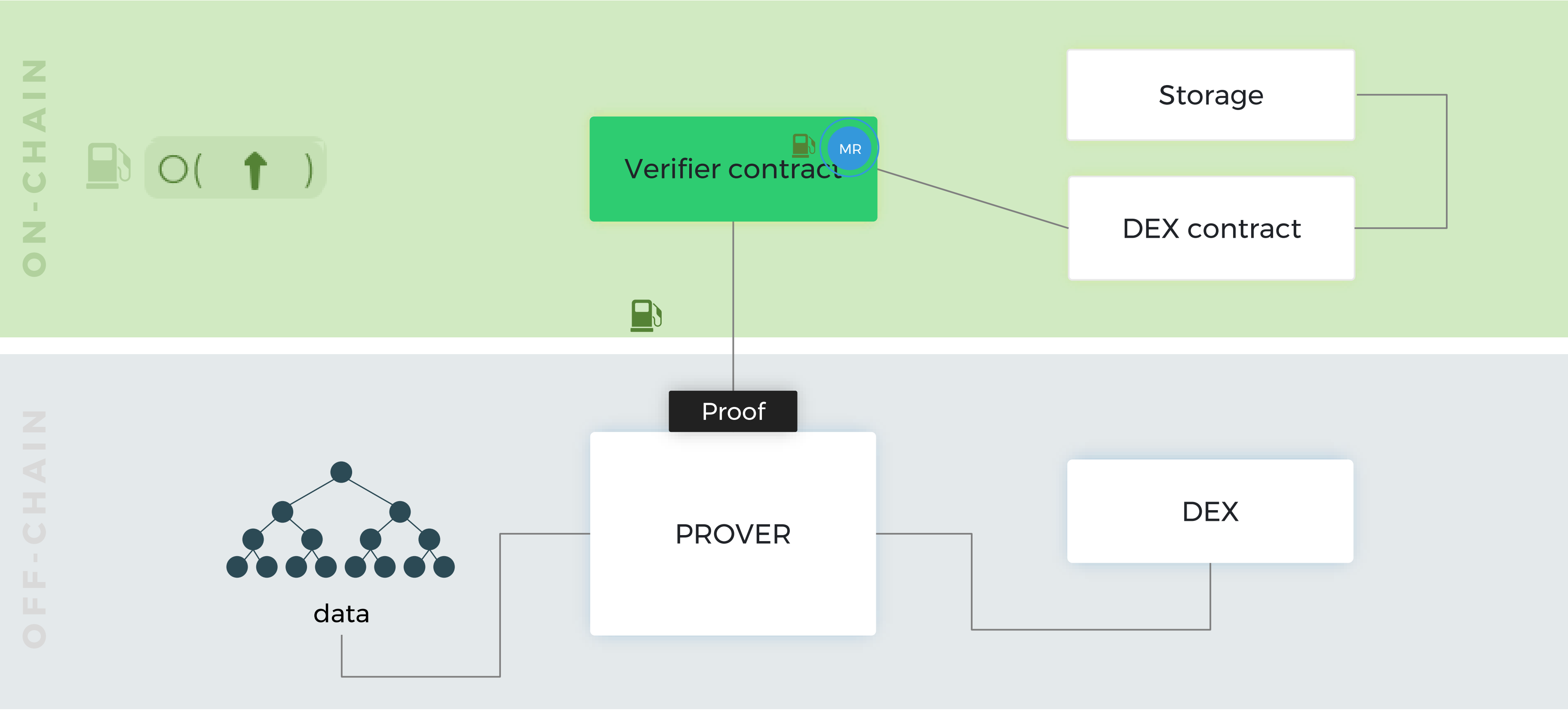
data

PROVER

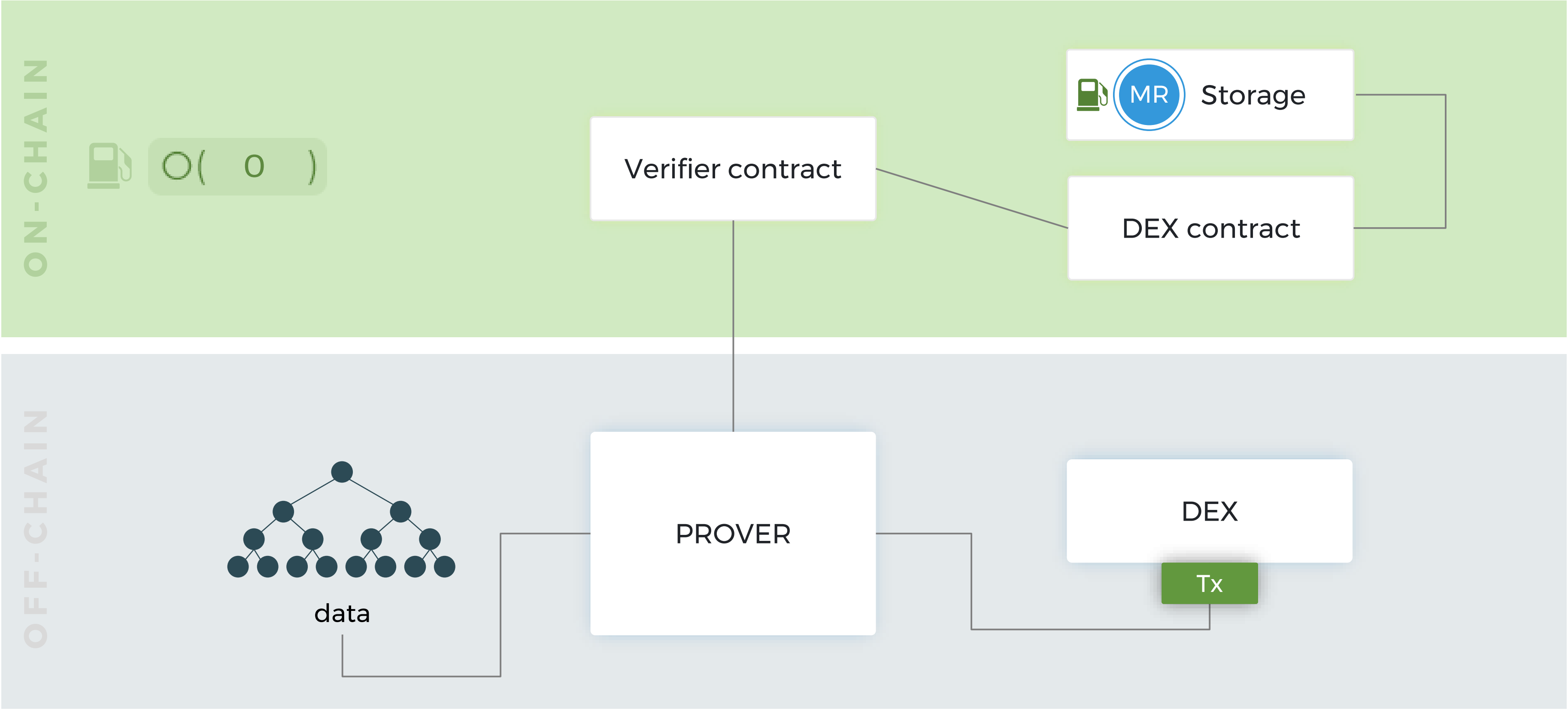
DEX

...

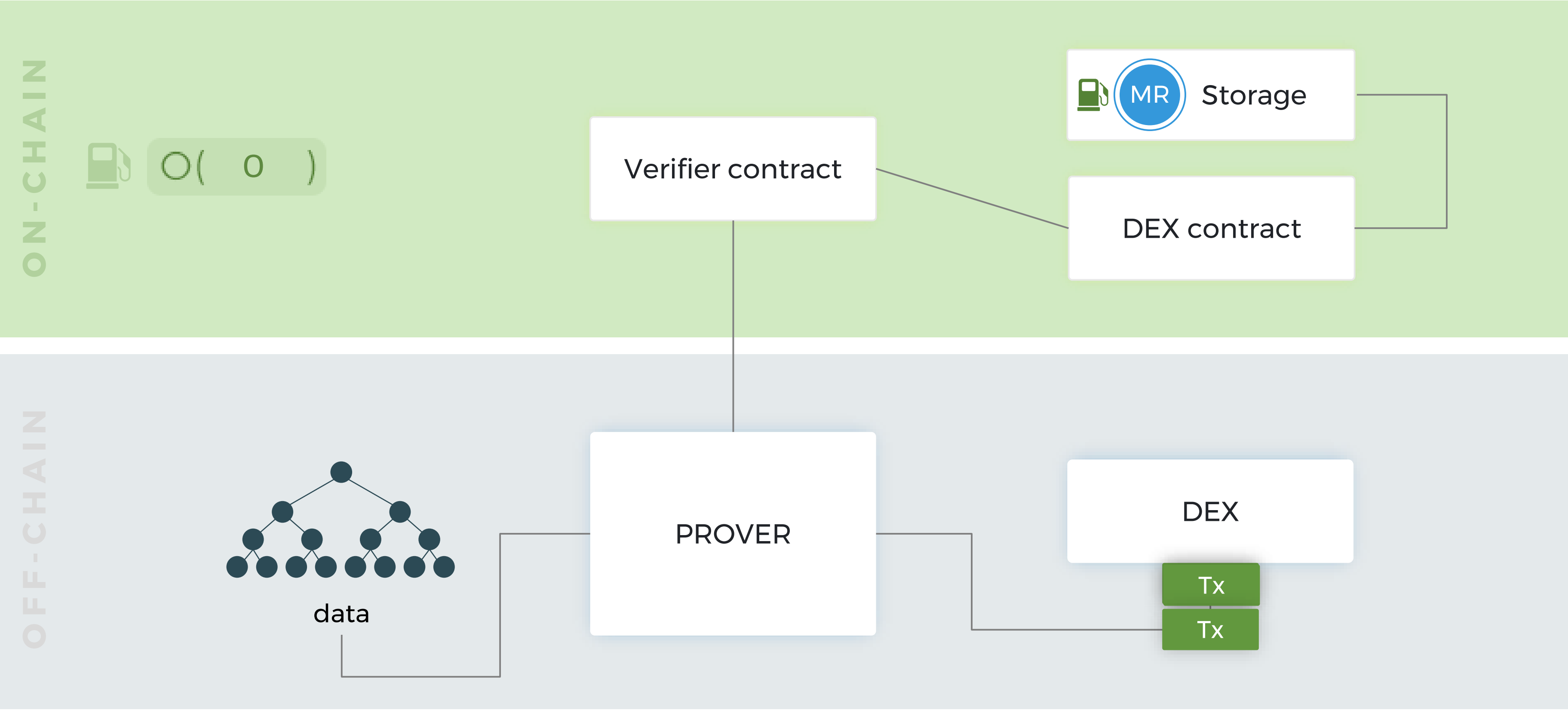
# StarkDEX – High Level



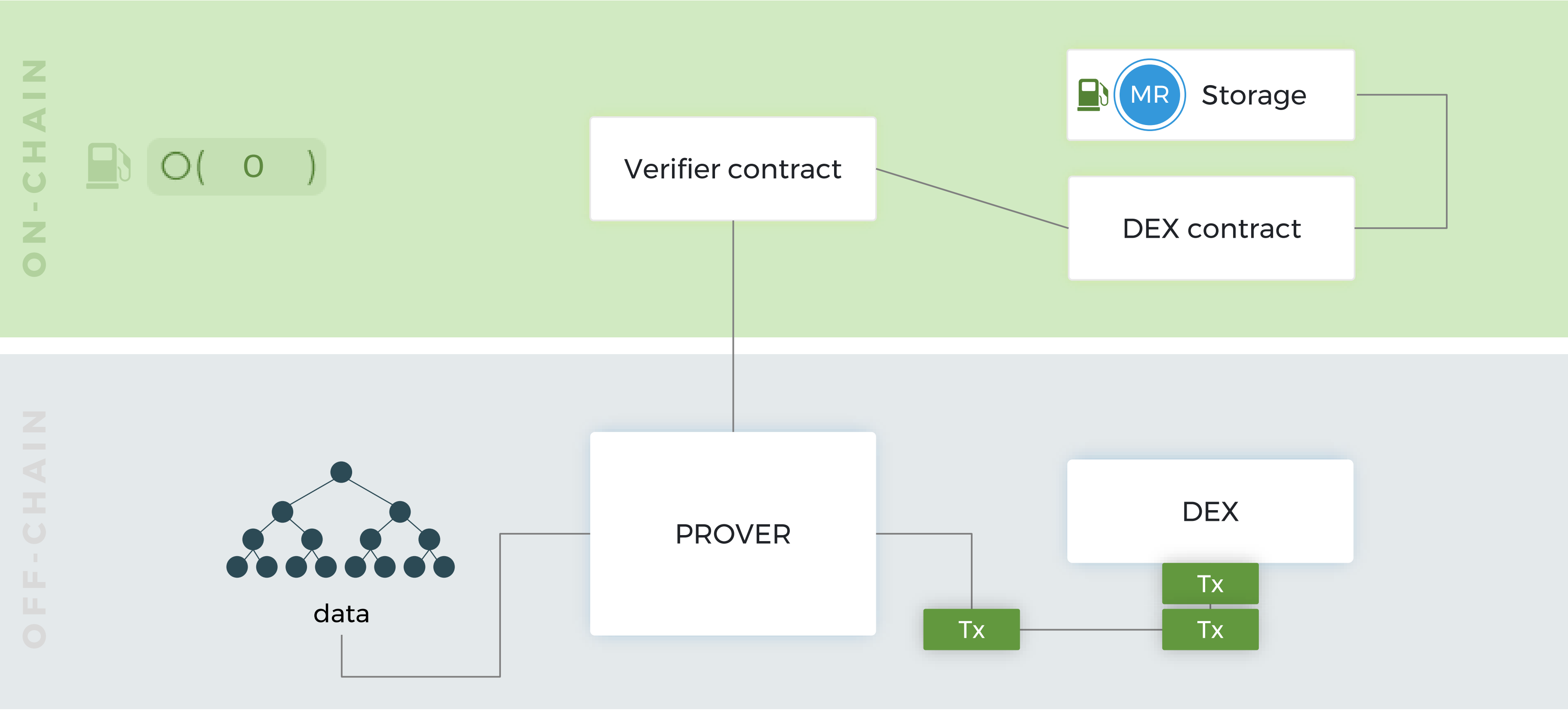
# StarkDEX – High Level



# StarkDEX – High Level

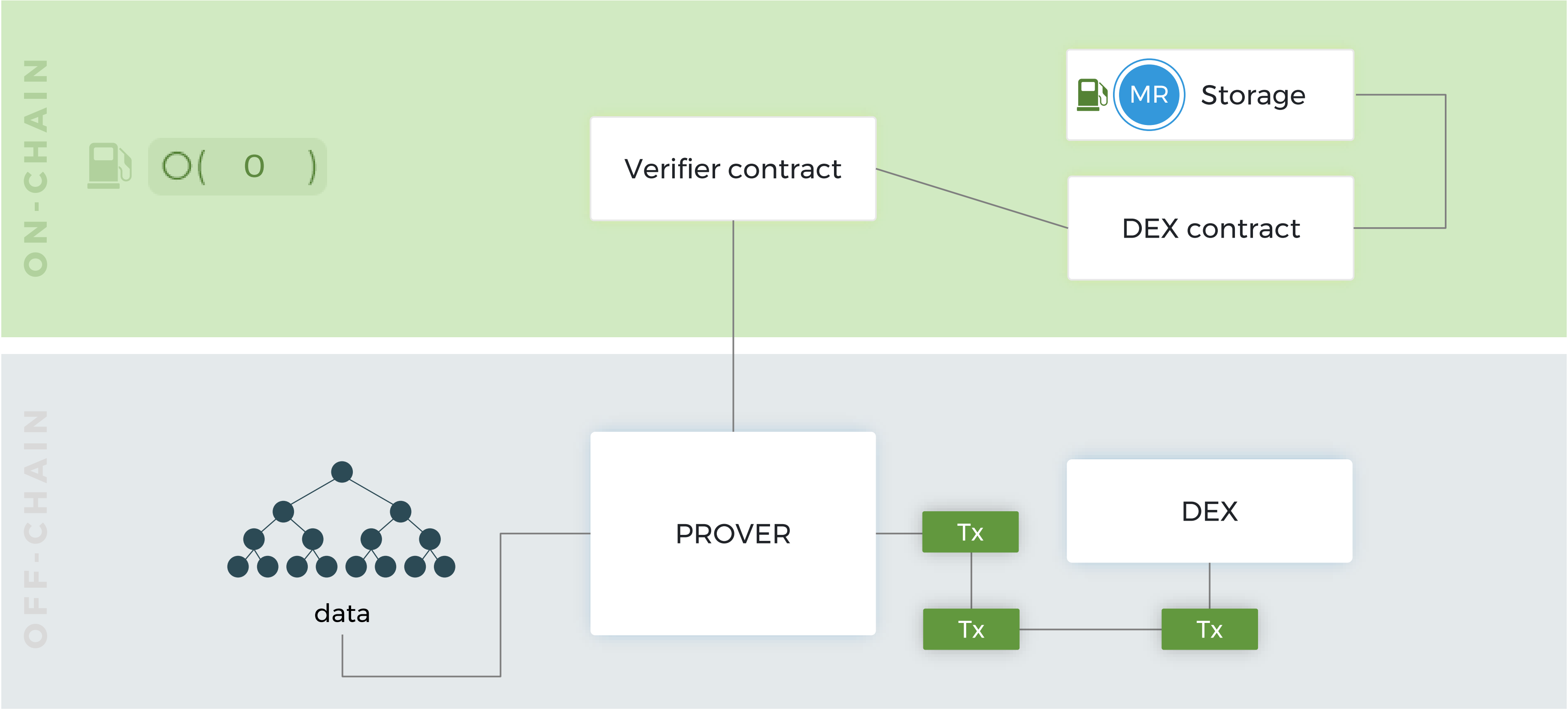


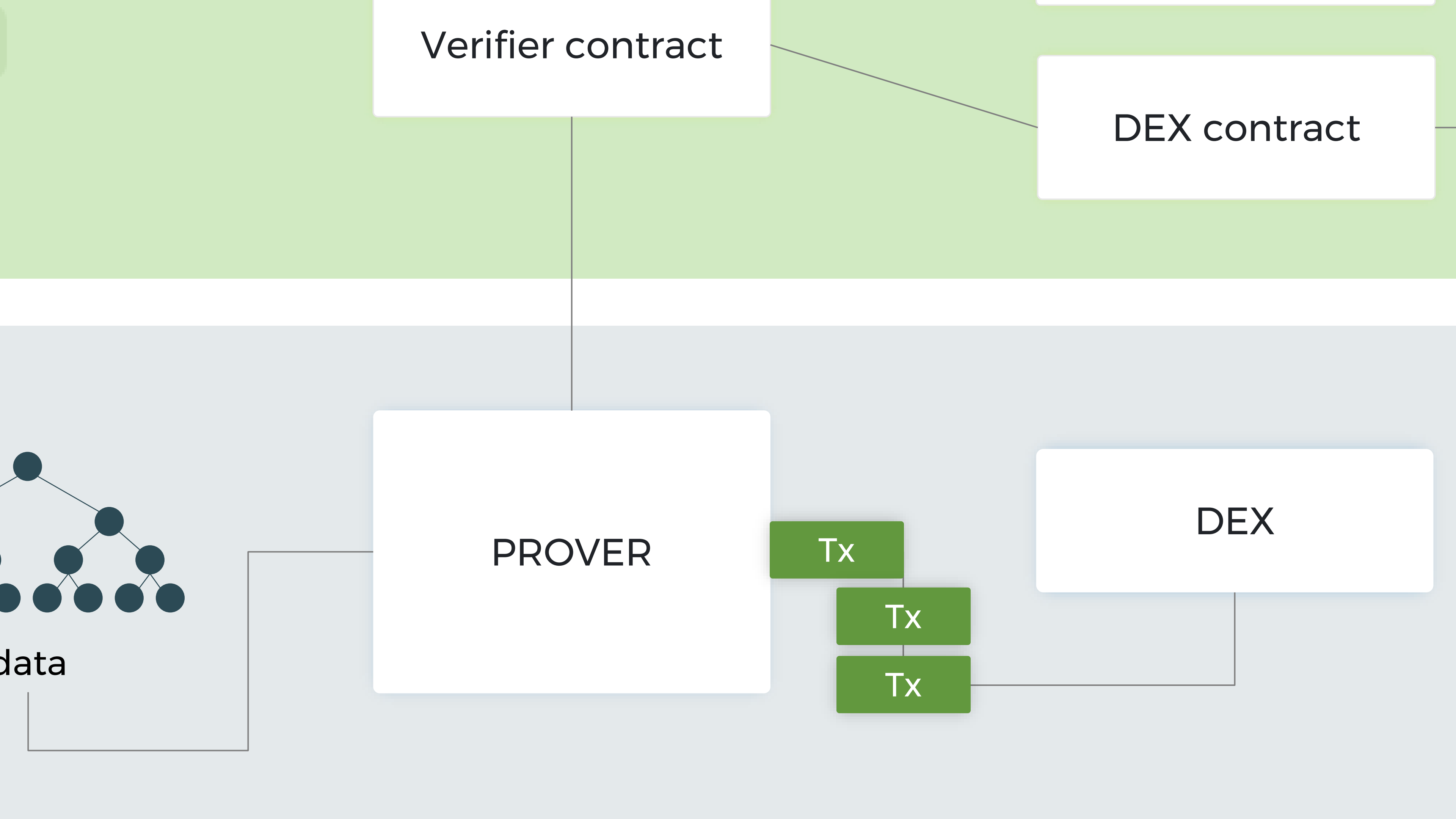
# StarkDEX – High Level



STARKWARE

# StarkDEX – High Level





Verifier contract

DEX contract

PROVER

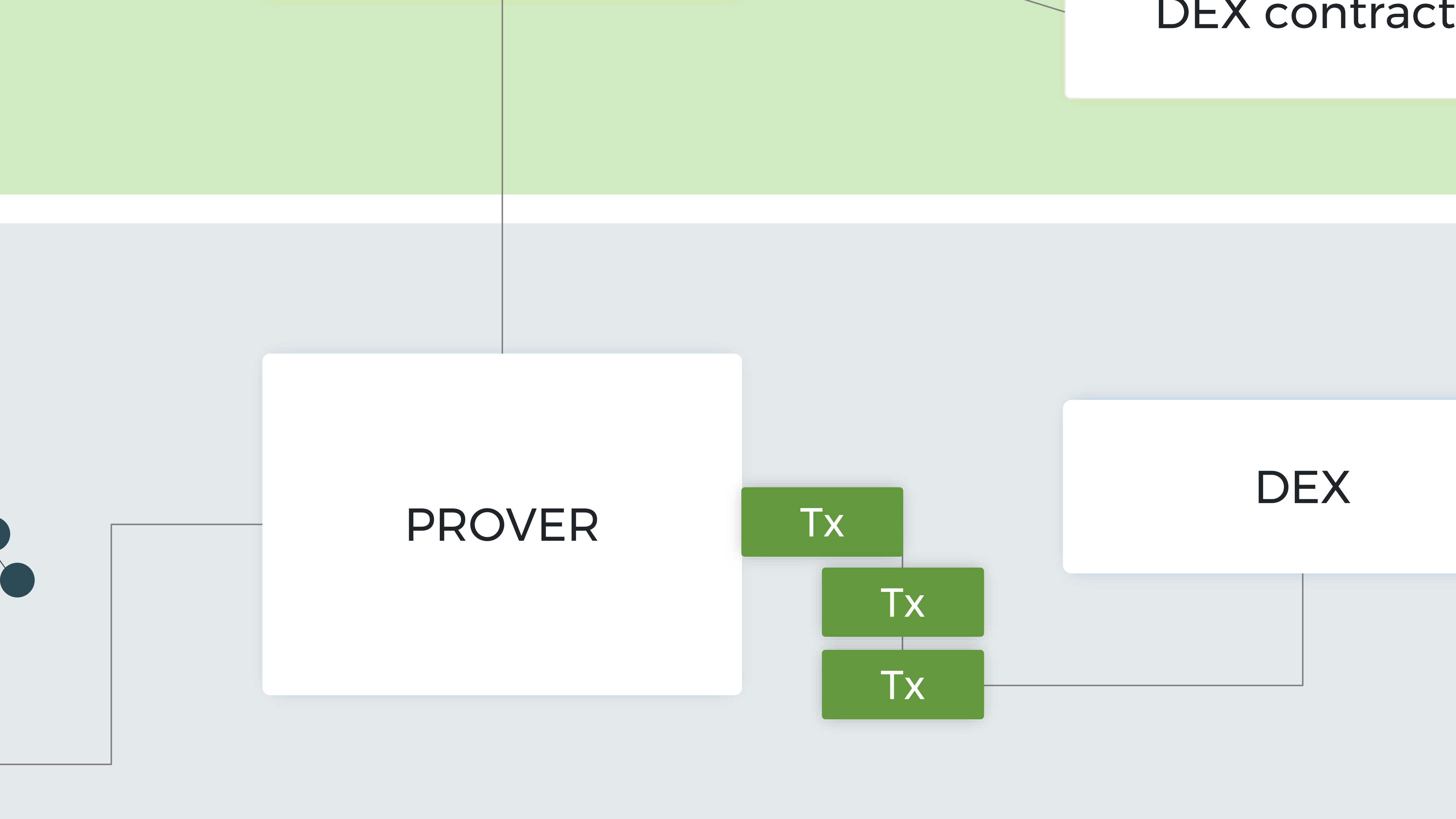
Tx

Tx

Tx

DEX

data



DEX contract

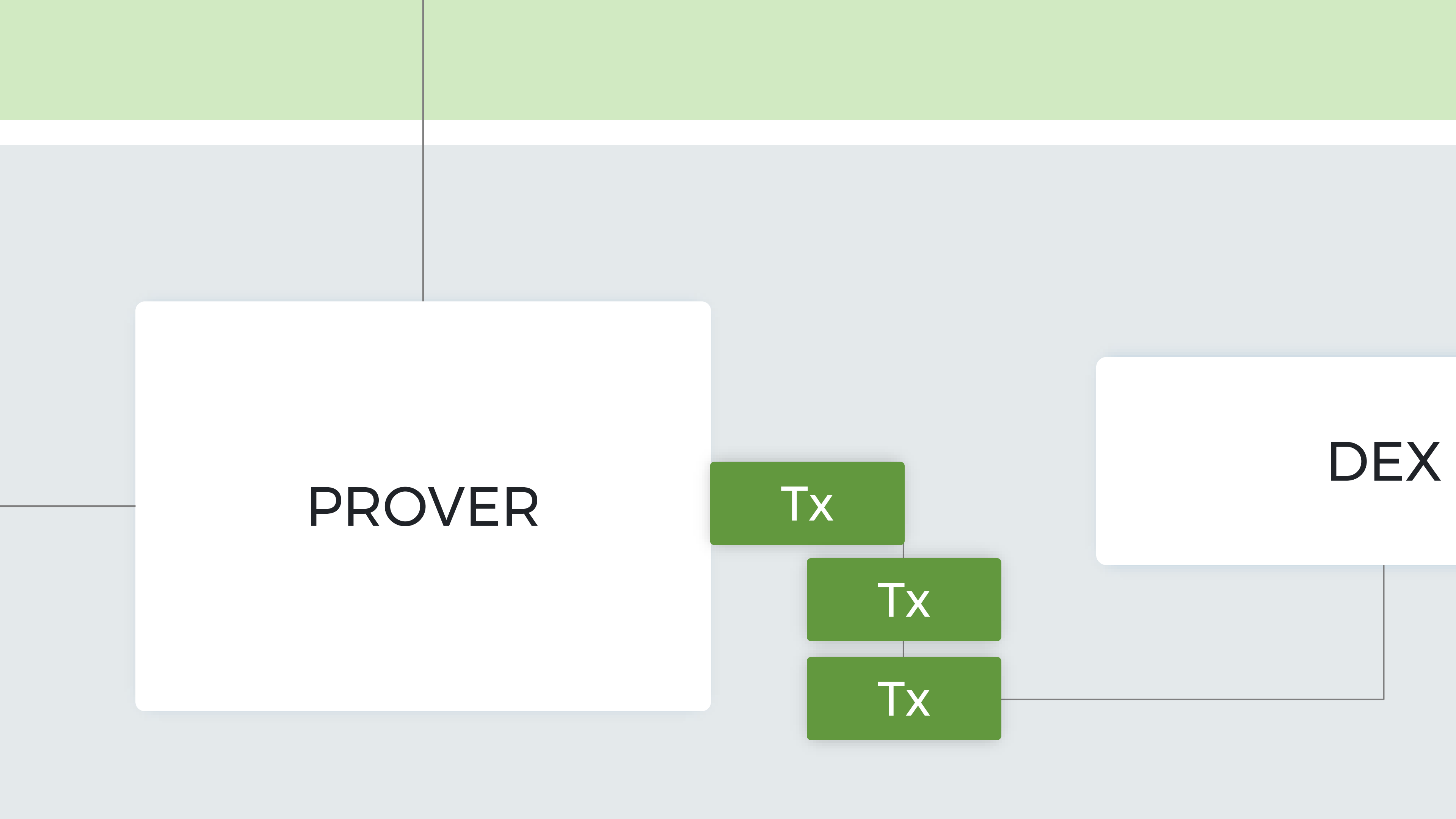
PROVER

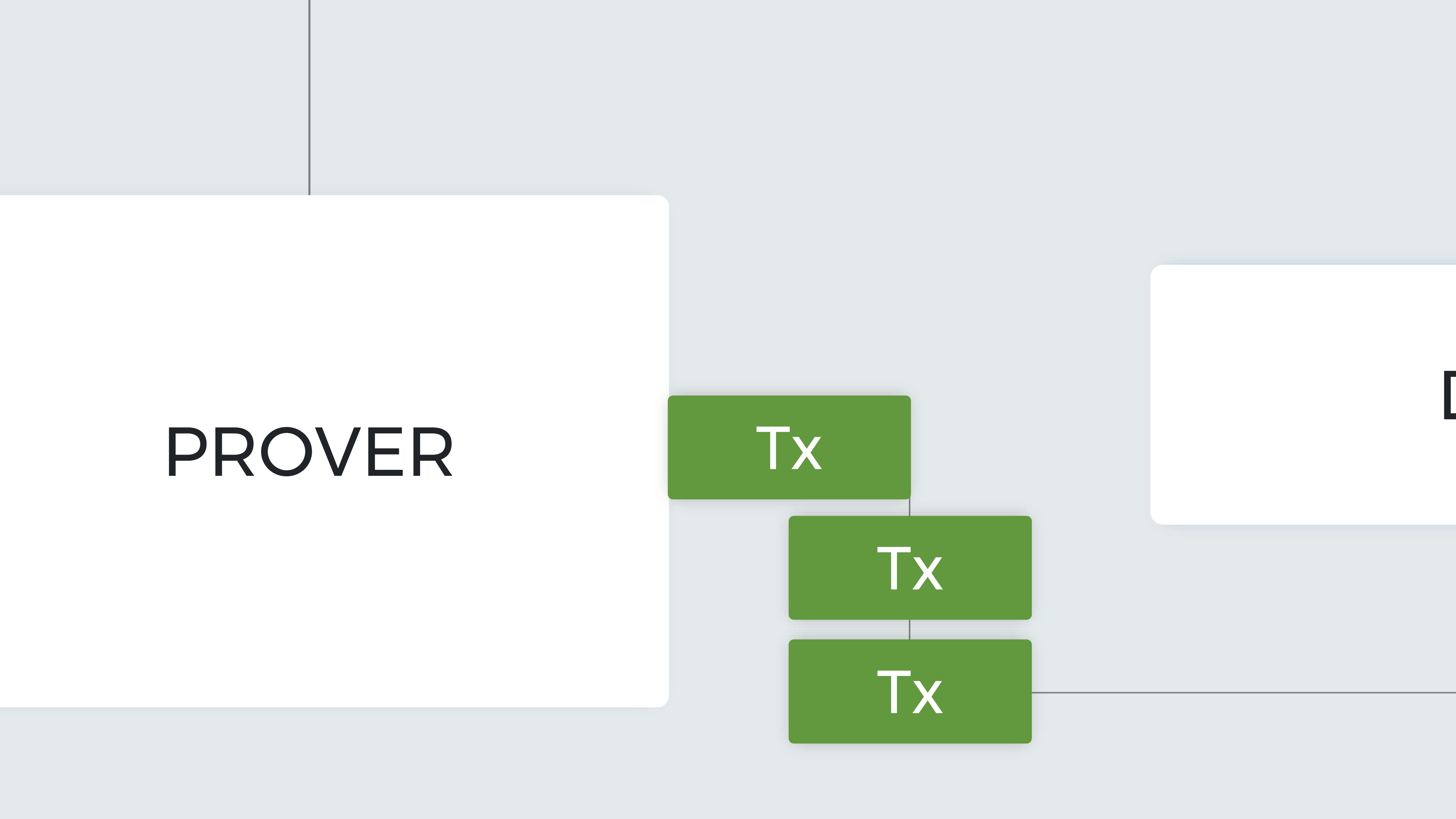
Tx

Tx

Tx

DEX


PROVER
Tx
Tx
Tx
DEX

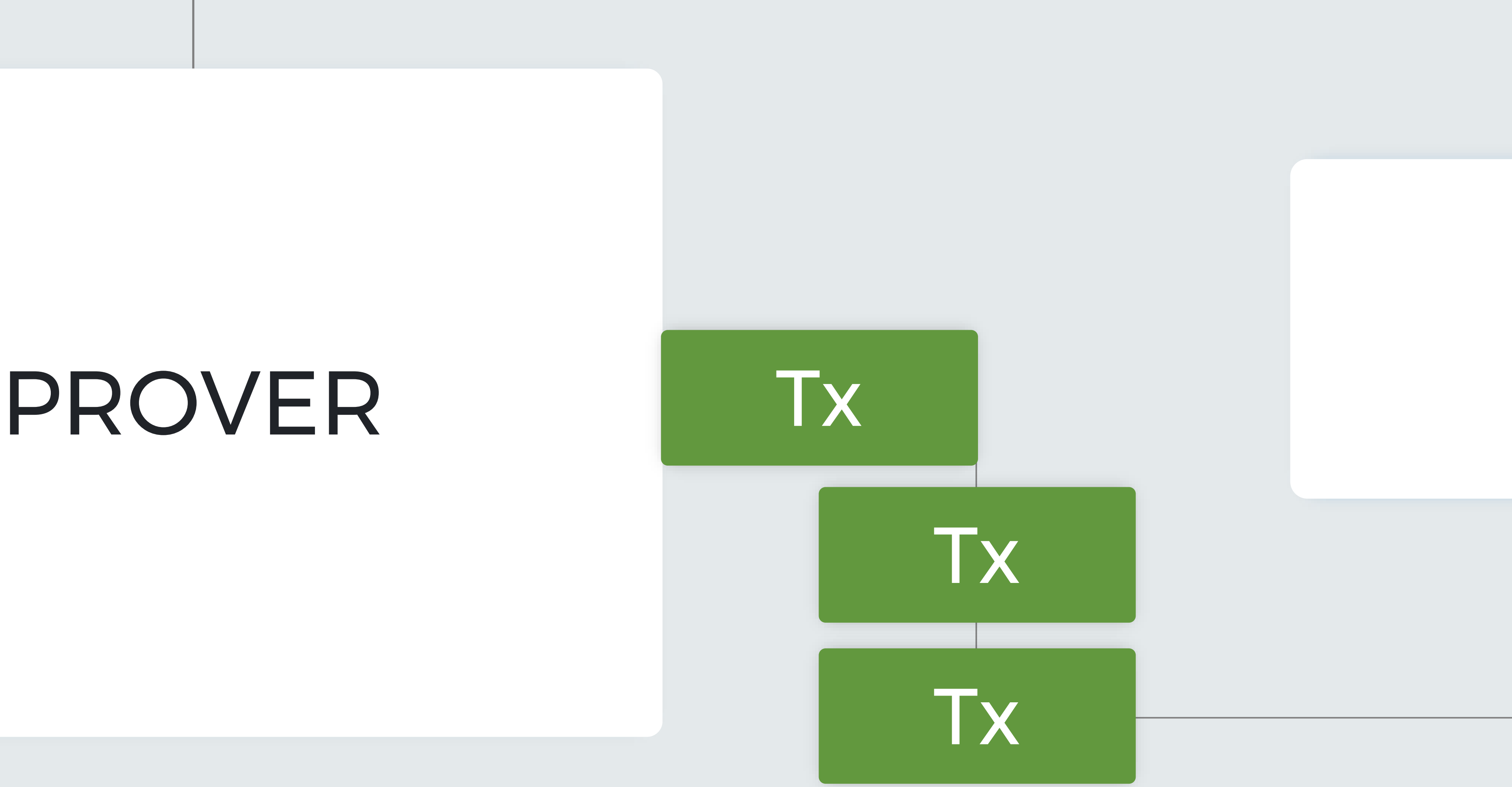


PROVER

Tx

Tx

Tx



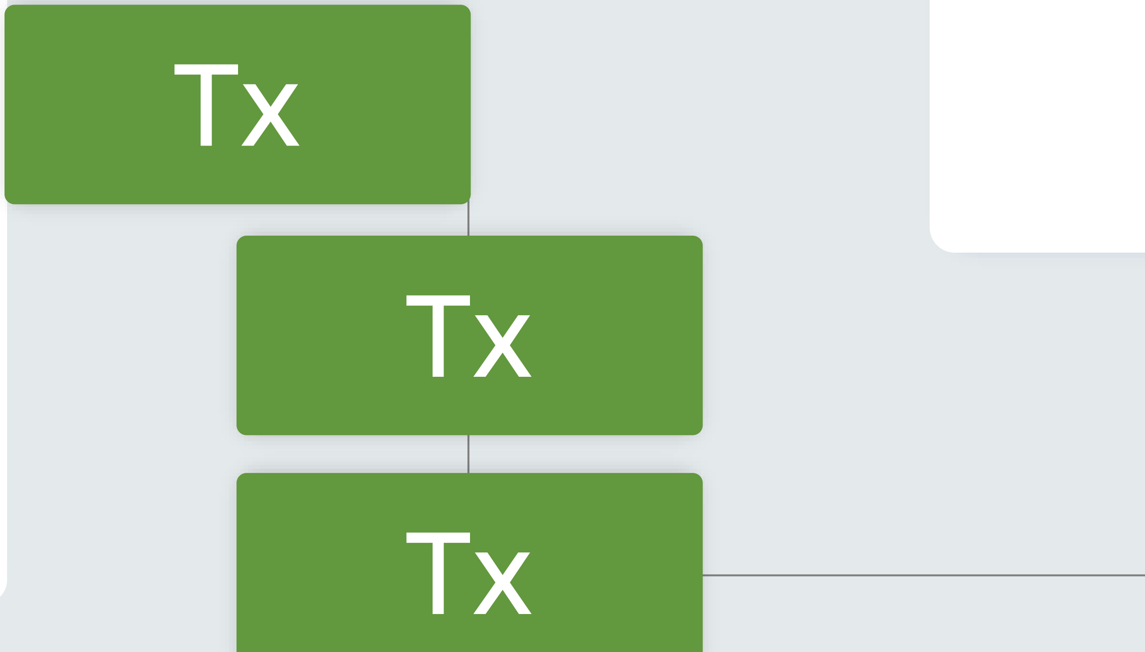
PROVER

Tx

Tx

Tx

OVER

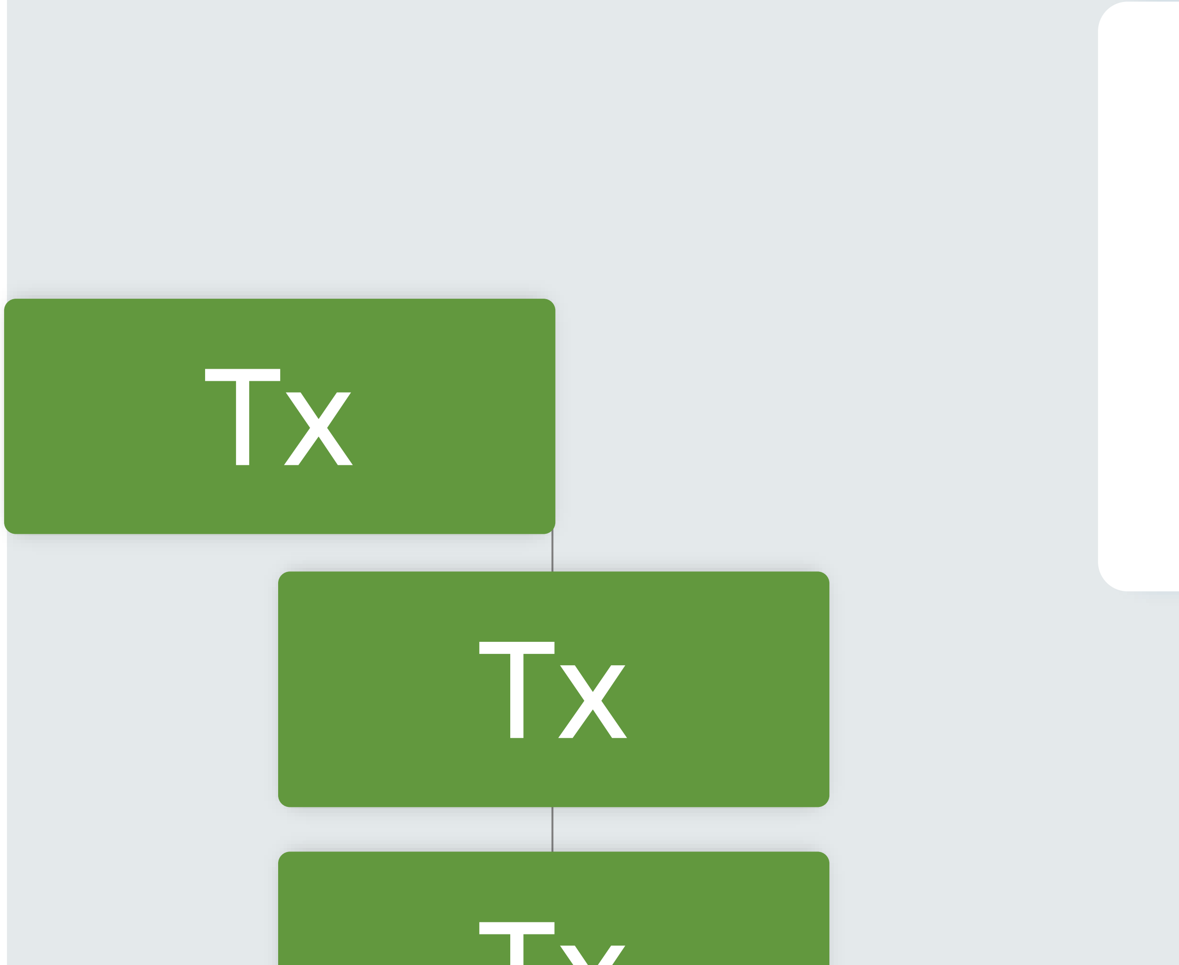


Tx

Tx

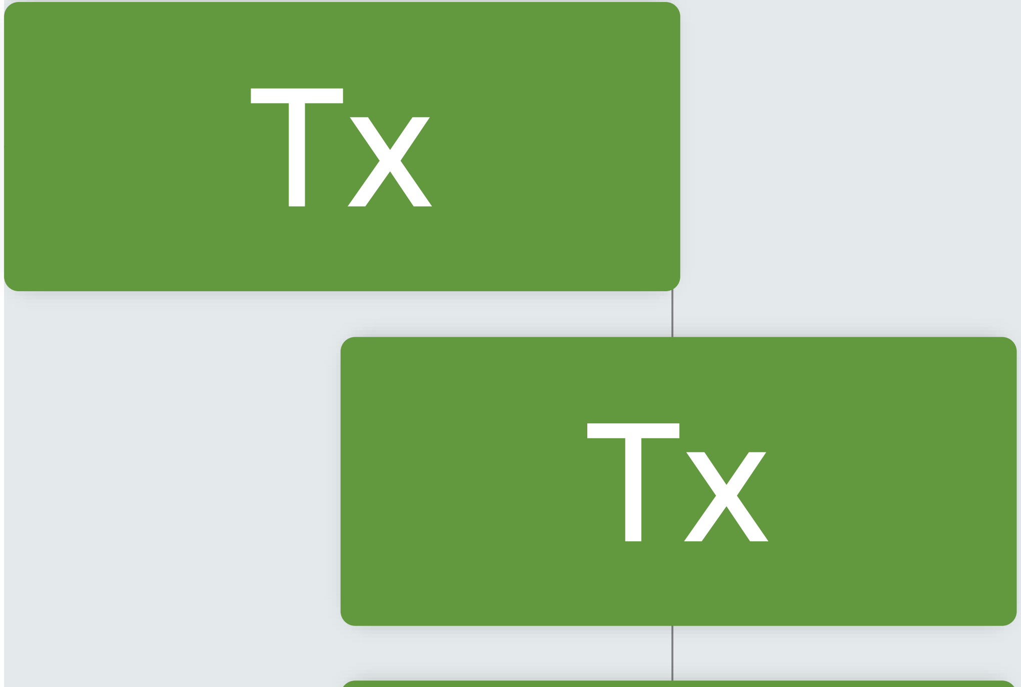
Tx

VER


Tx

Tx

Tx



Tx

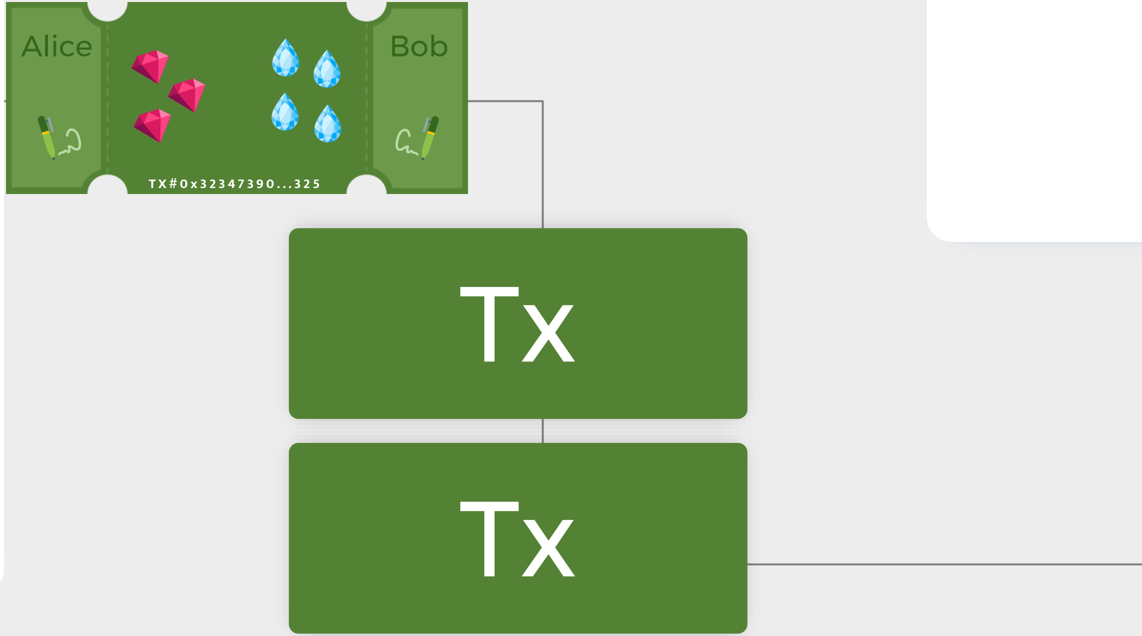
Tx

T

Alice
Bob
TX#0x32347390...325

Tx

OVER



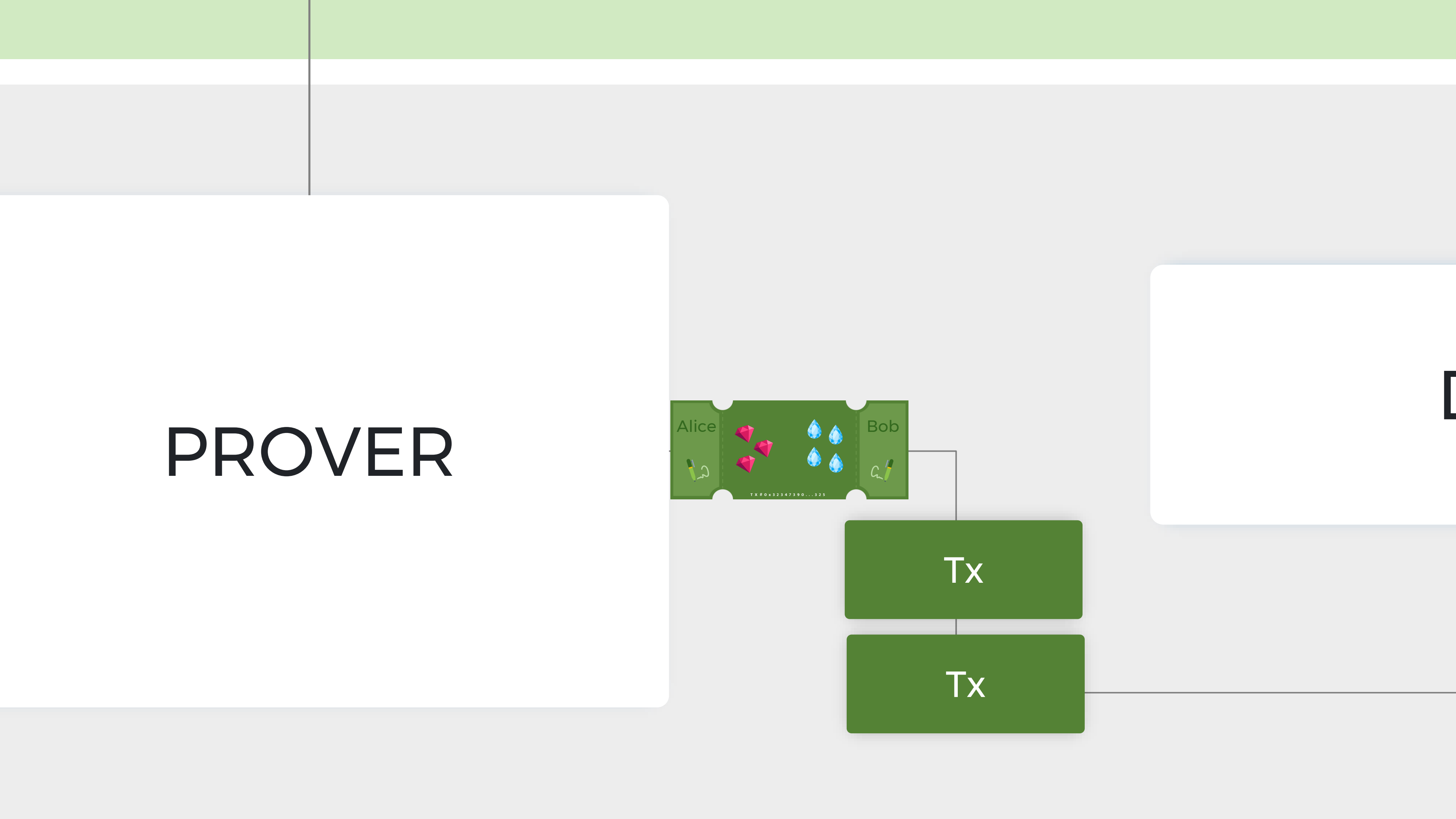
Alice

Bob

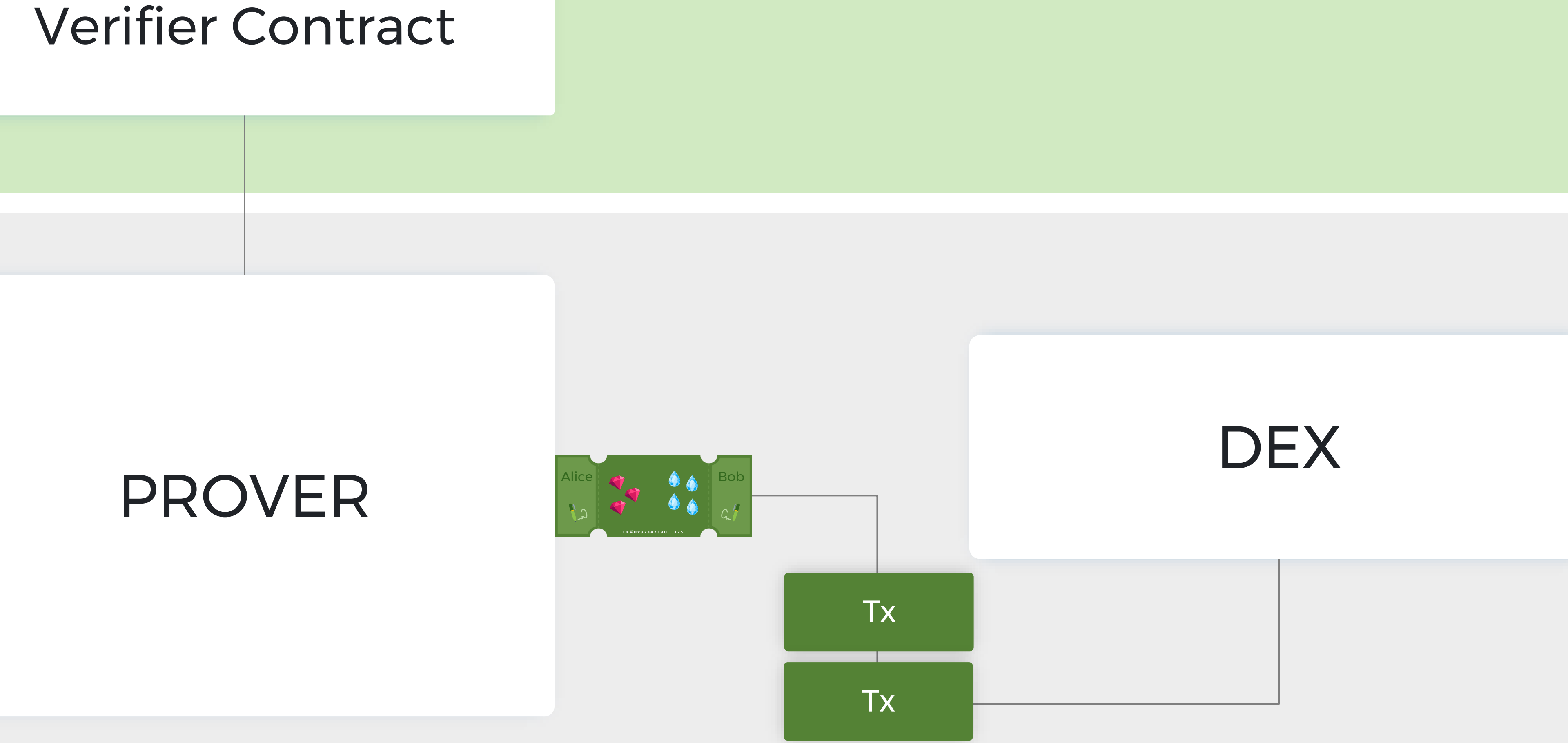
TX#0x32347390...325

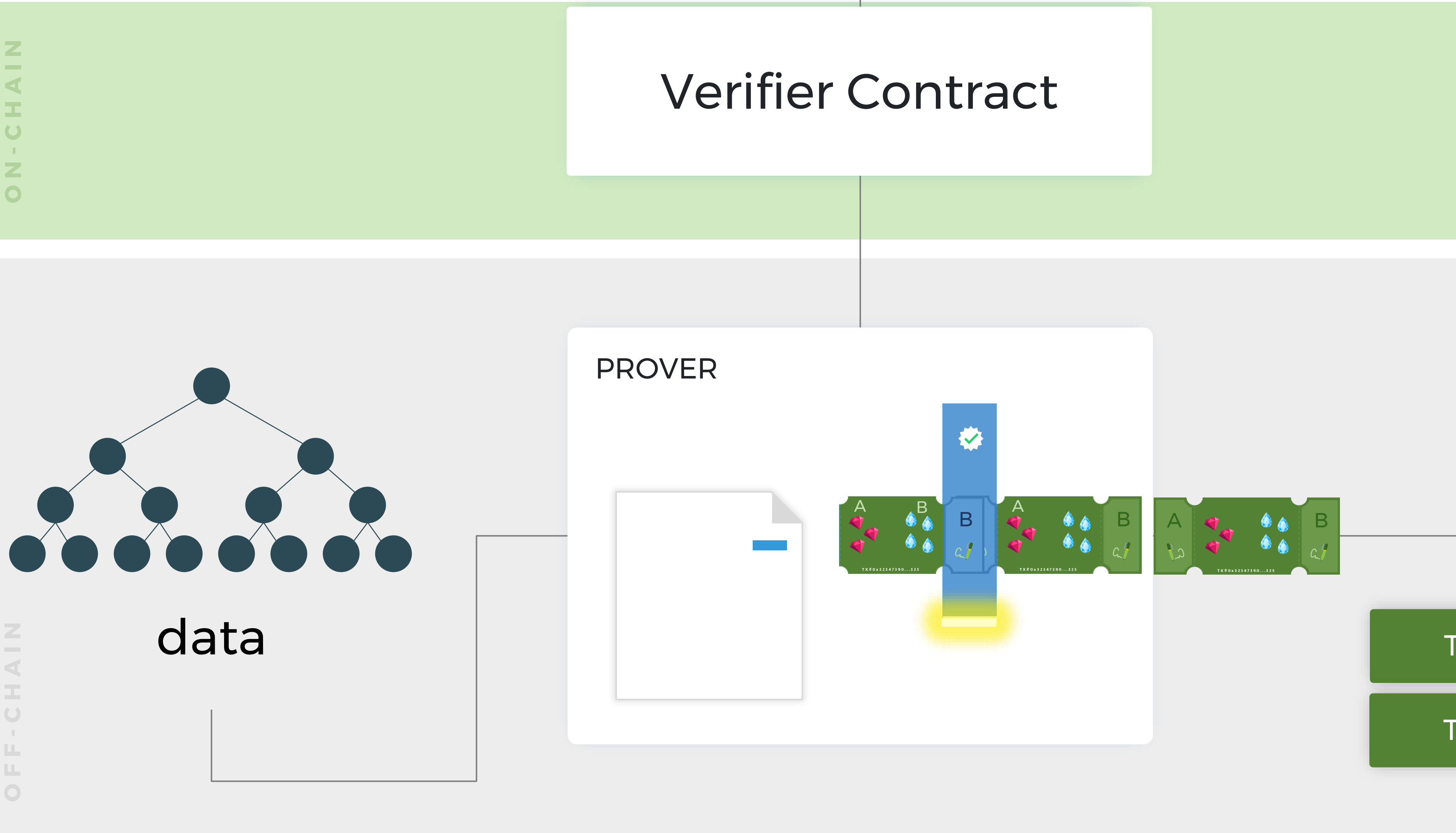
Tx

Tx



PROVER


Verifier Contract
PROVER
Alice
Bob
TX#0x32347390...325
DEX
Tx
Tx



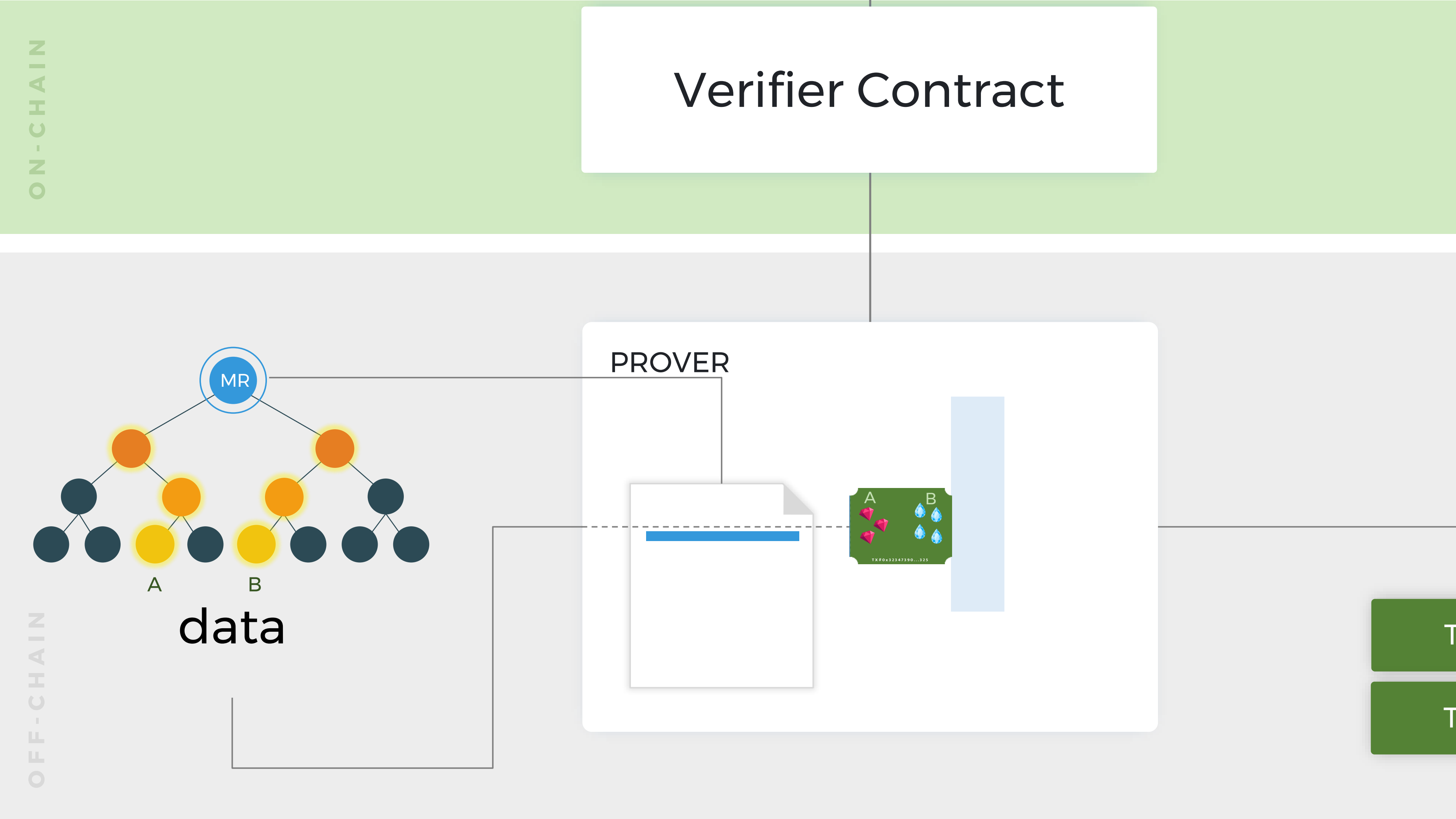
ON-CHAIN

Verifier Contract

OFF-CHAIN

data

PROVER



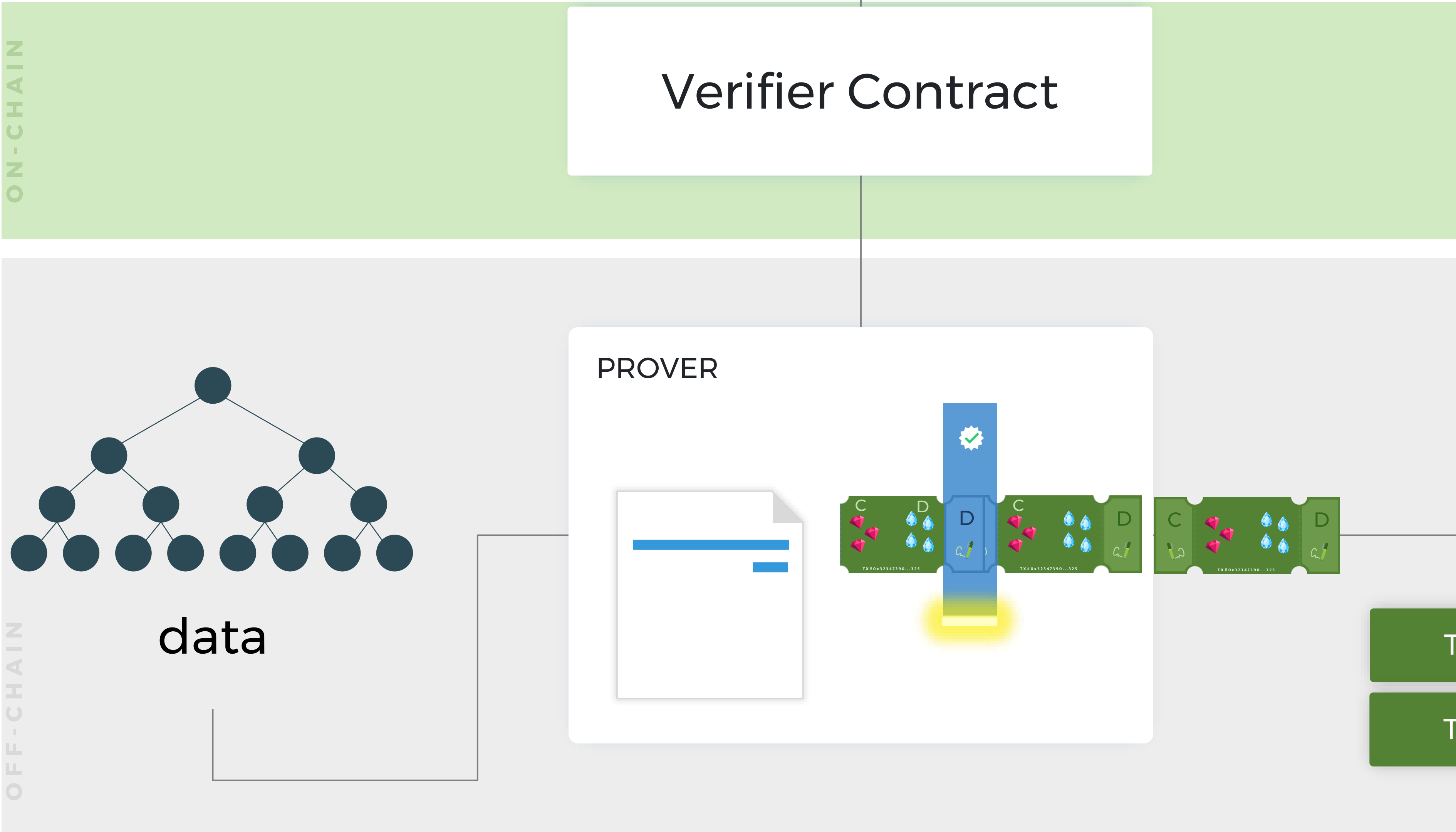
ON-CHAIN

Verifier Contract

PROVER

data

OFF-CHAIN



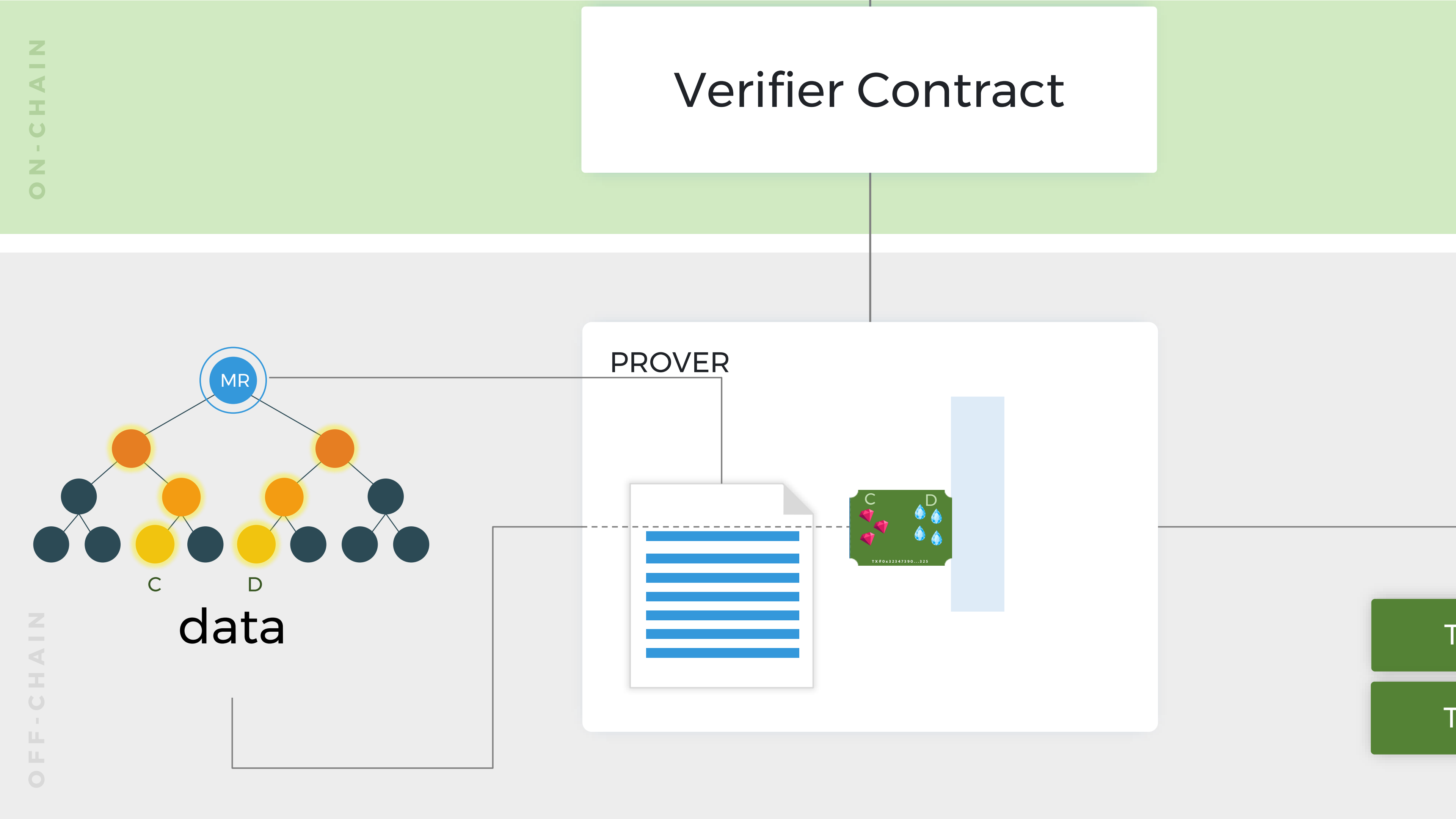
ON-CHAIN

Verifier Contract

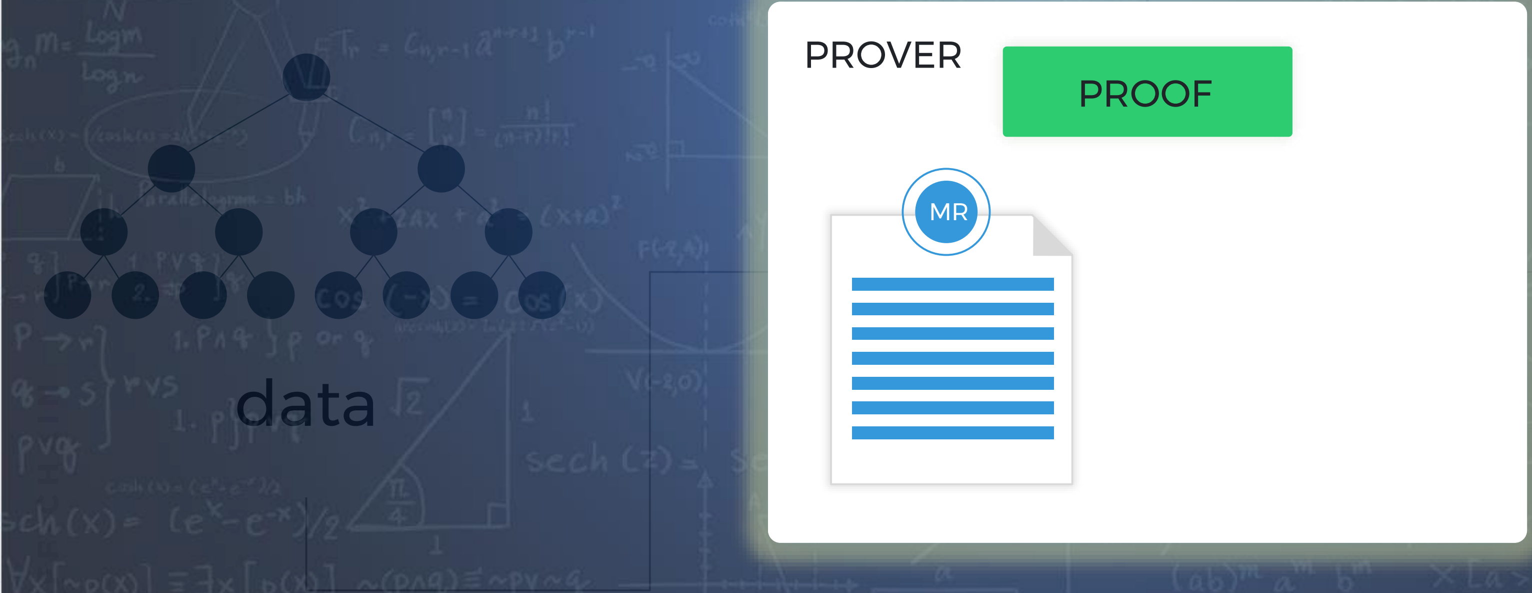
PROVER

data

OFF-CHAIN


ON-CHAIN
Verifier Contract
OFF-CHAIN
MR
C
D
data
PROVER
C
D
TX#0x32347390...325
T
T

# Verifier Contract

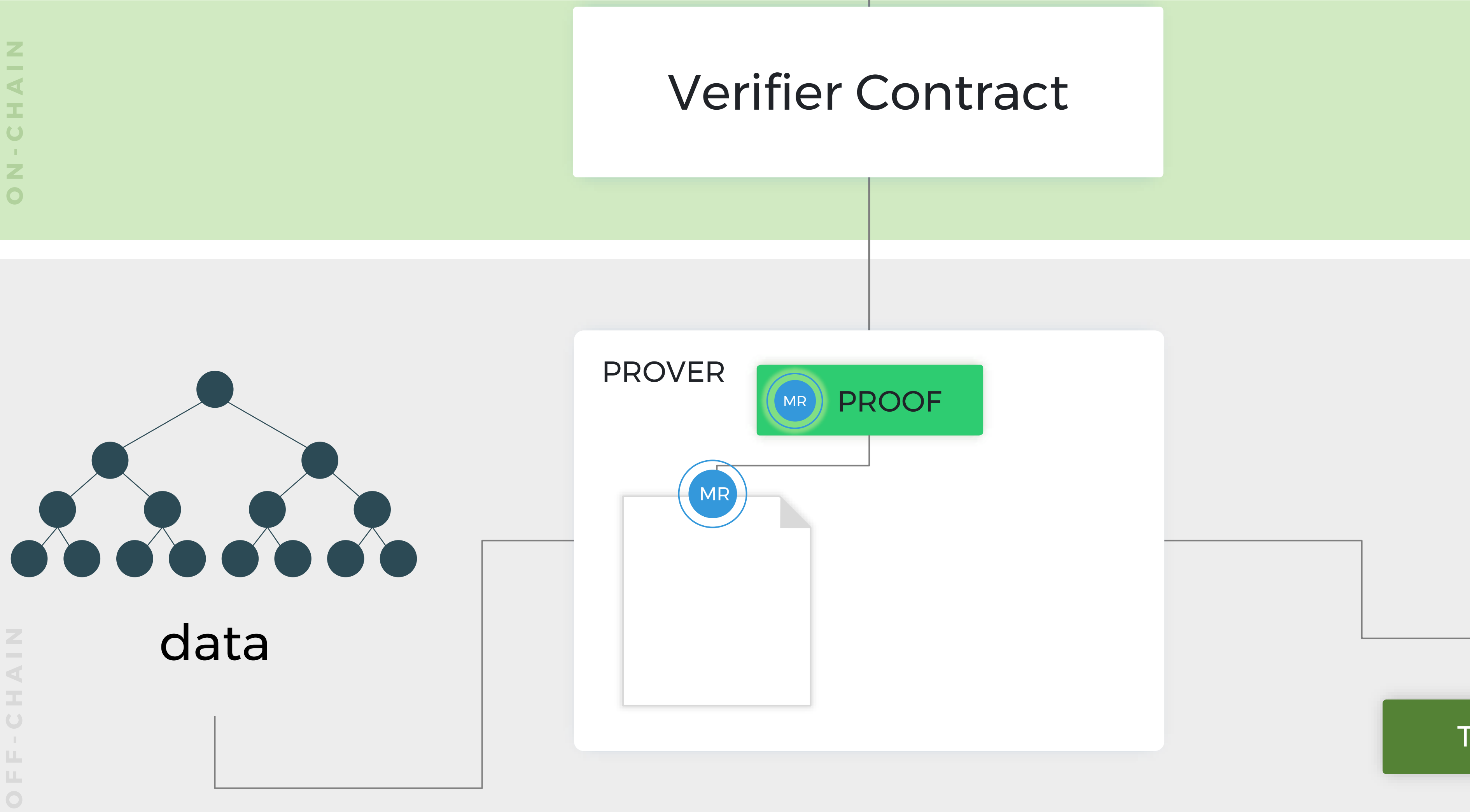


data

PROVER

PROOF

MR



ON-CHAIN

Verifier Contract

PROVER

MR

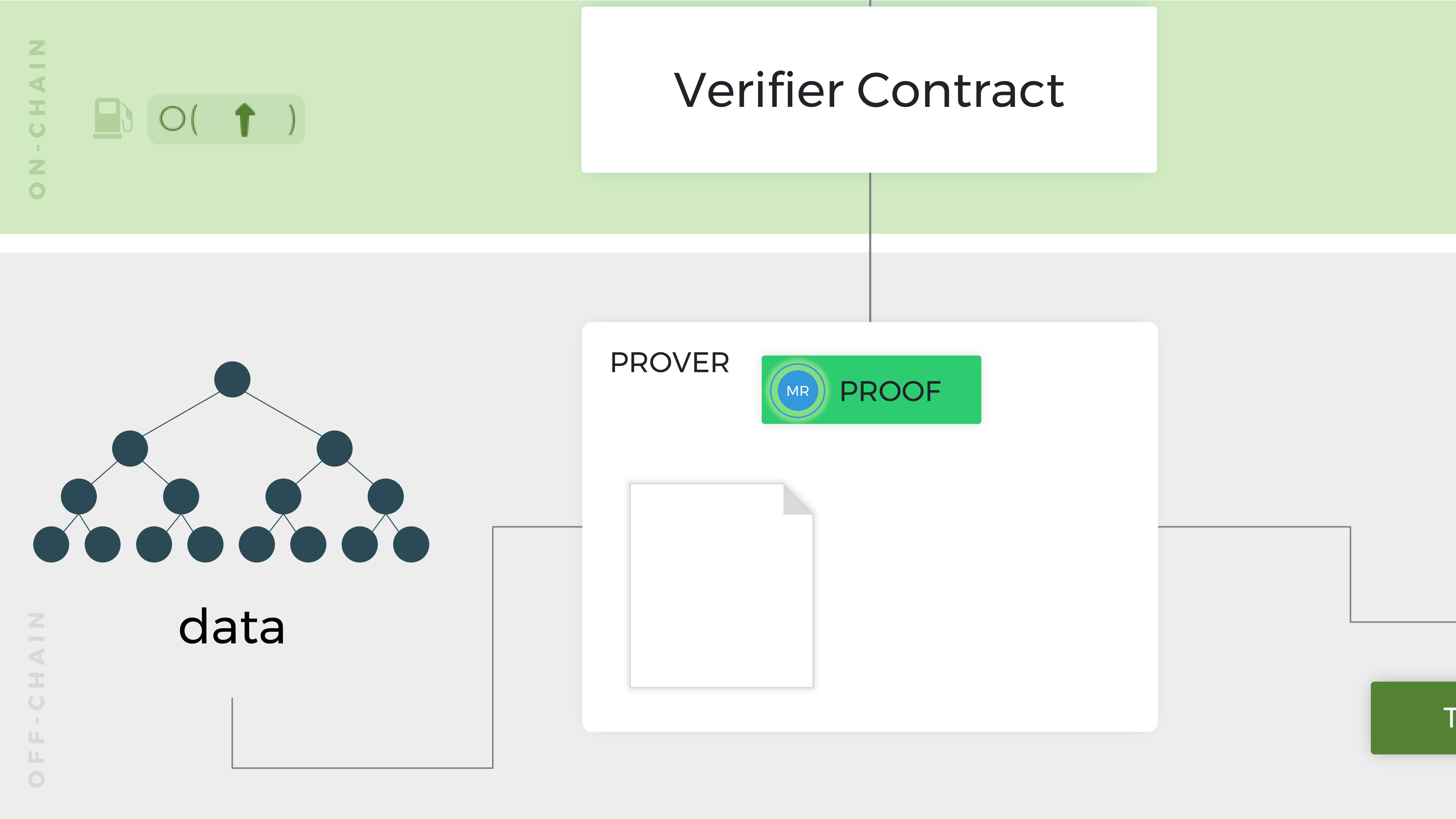
PROOF

MR

data

T

OFF-CHAIN



ON-CHAIN

O( ↑ )

Verifier Contract

PROVER

MR PROOF

data

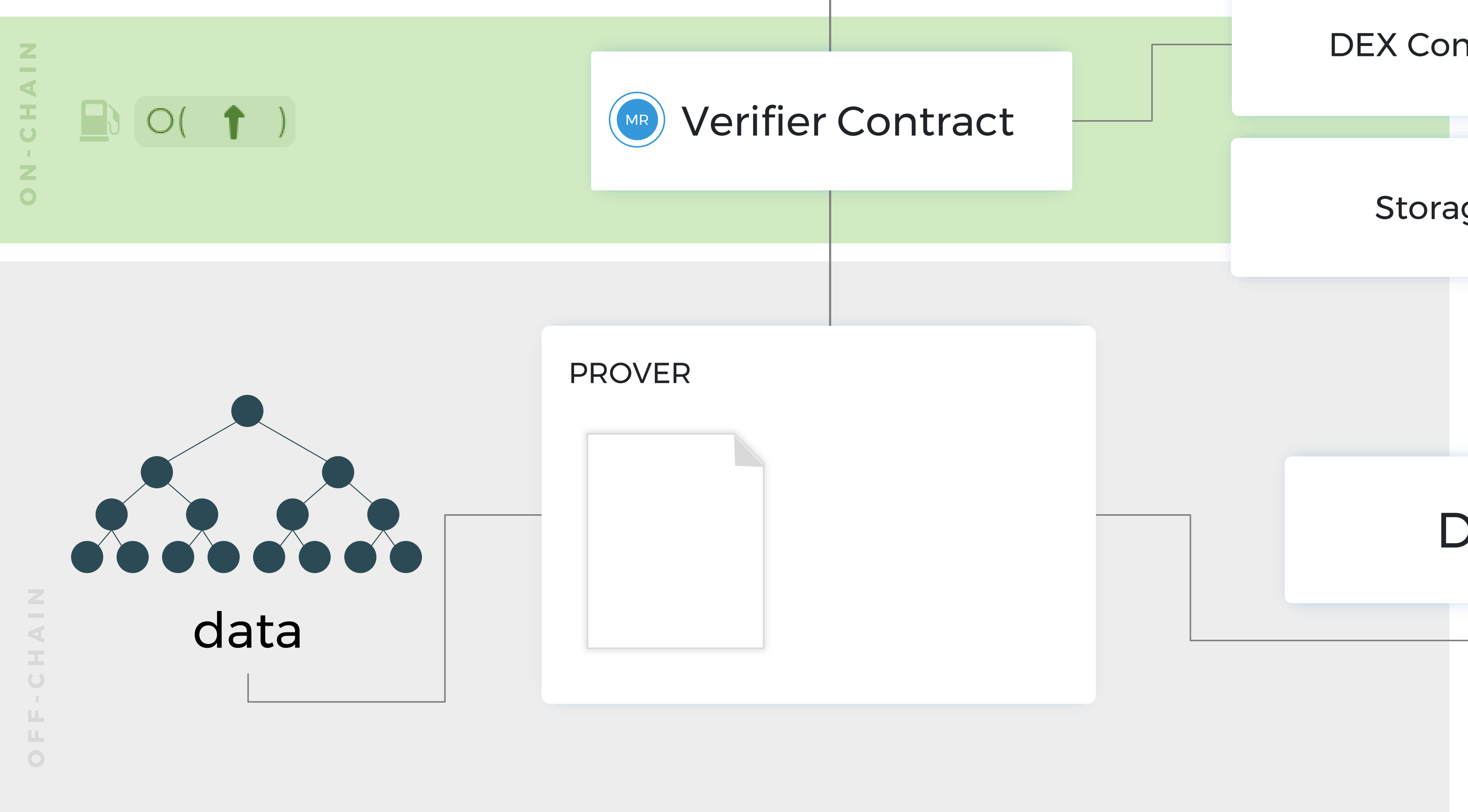
OFF-CHAIN

T

# Verifier Contract

PROVER

data



ON-CHAIN

O( )

MR

Verifier Contract

DEX Con

Storag

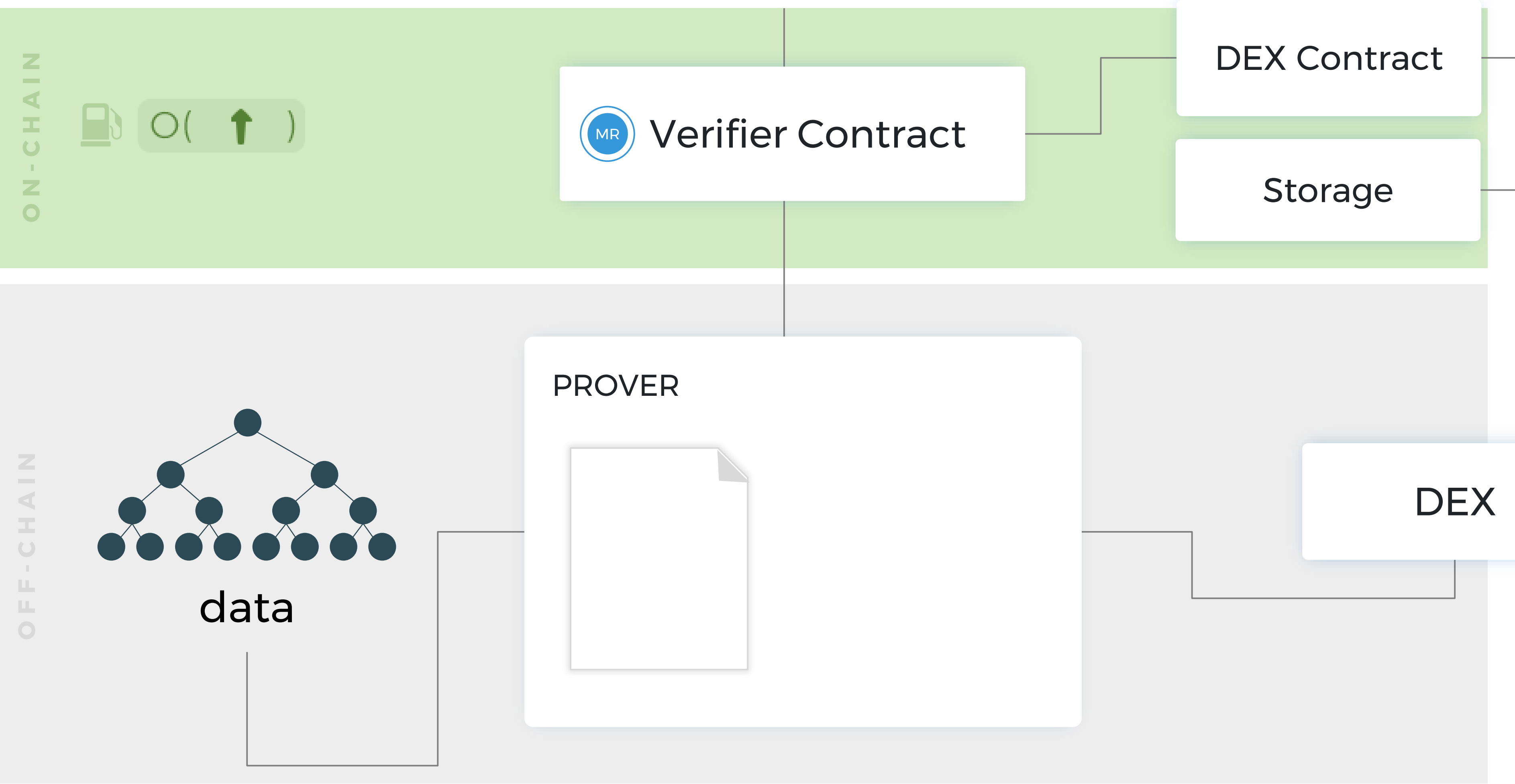
OFF-CHAIN

PROVER

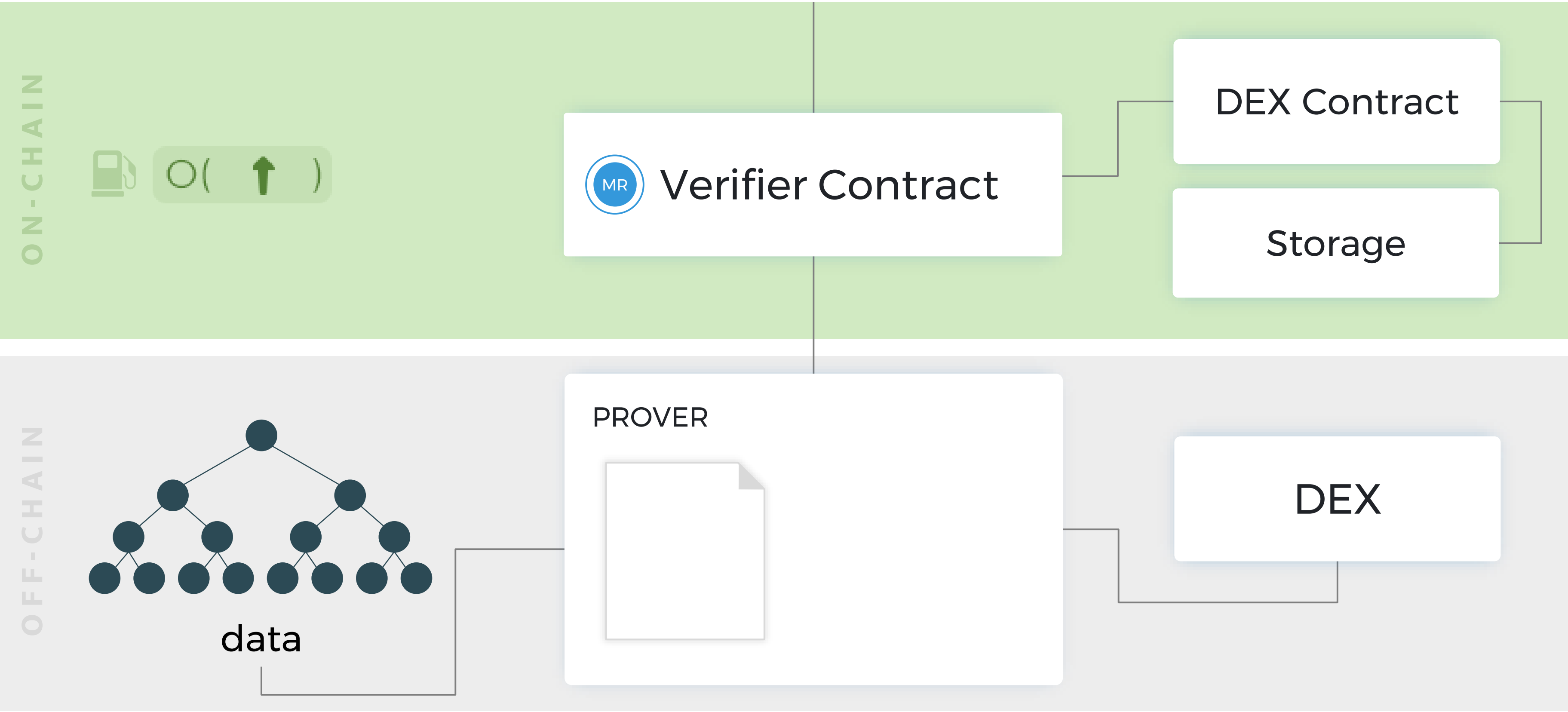
data

D

# Starked Dex – Tx Anatomy

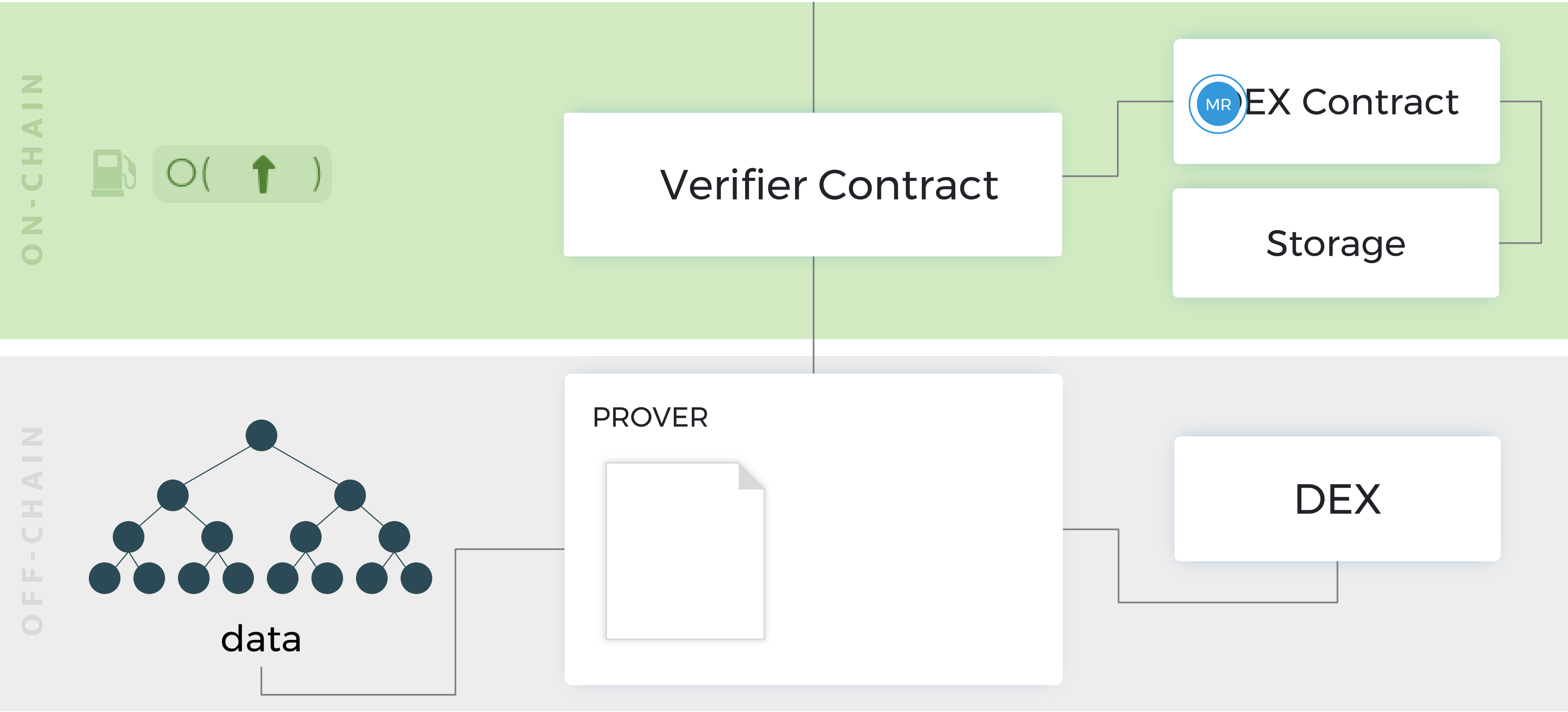


# Starked Dex - Tx Anatomy



STARKWARE

# Starked Dex - Tx Anatomy



ON-CHAIN

O( ↑ )

Verifier Contract

MR EX Contract

Storage

OFF-CHAIN

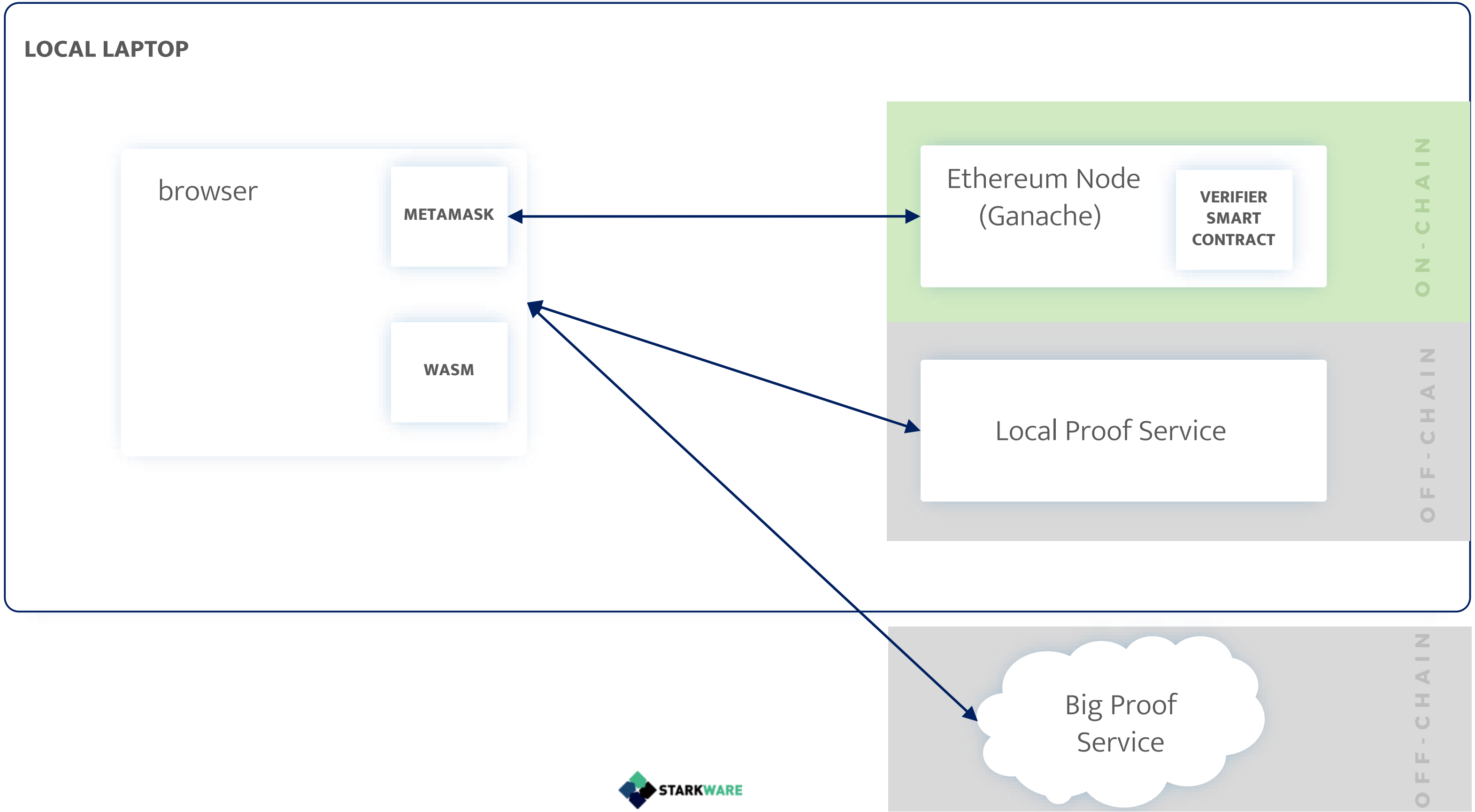
data

PROVER

DEX

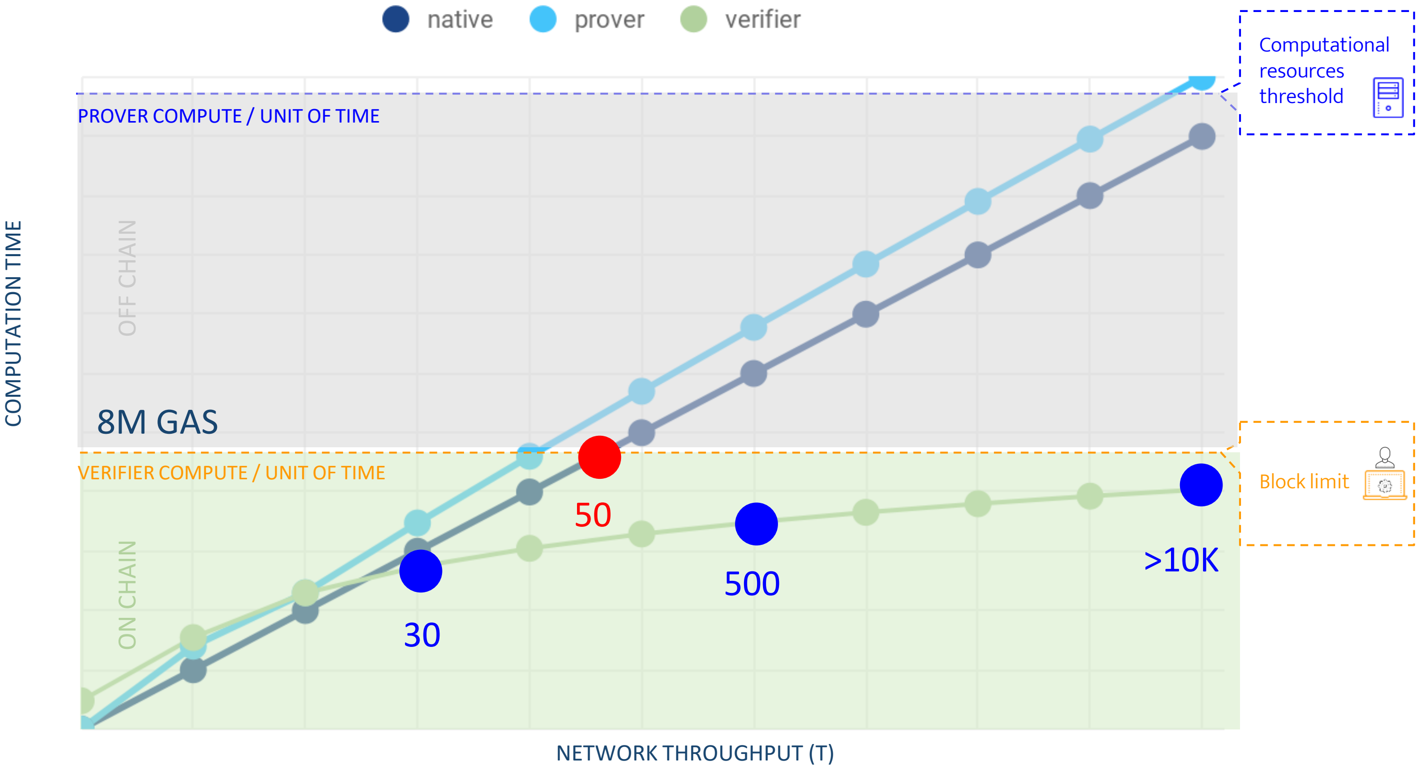
# ONE MORE THING...

# DEMO



STARKWARE

# STARK Scalability



WORK IN PROGRESS

## 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