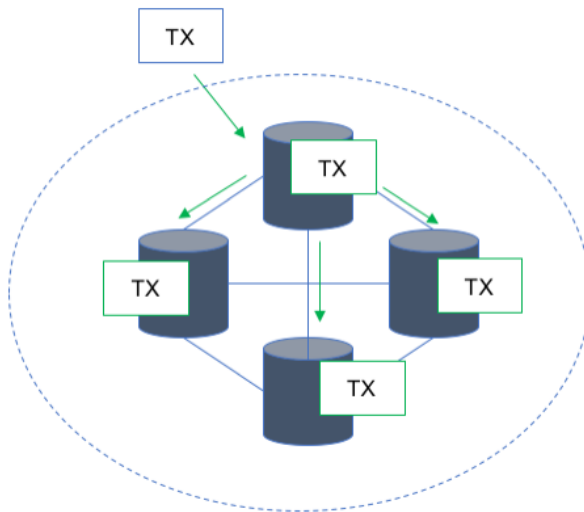


ZoKrates – I know, that I show nothing

Jacob Eberhardt

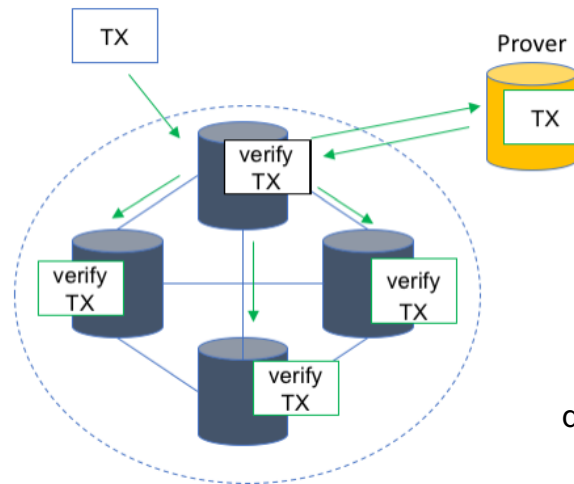
Delegated Computation

On-chain processing



Blockchain Network

Delegated computation



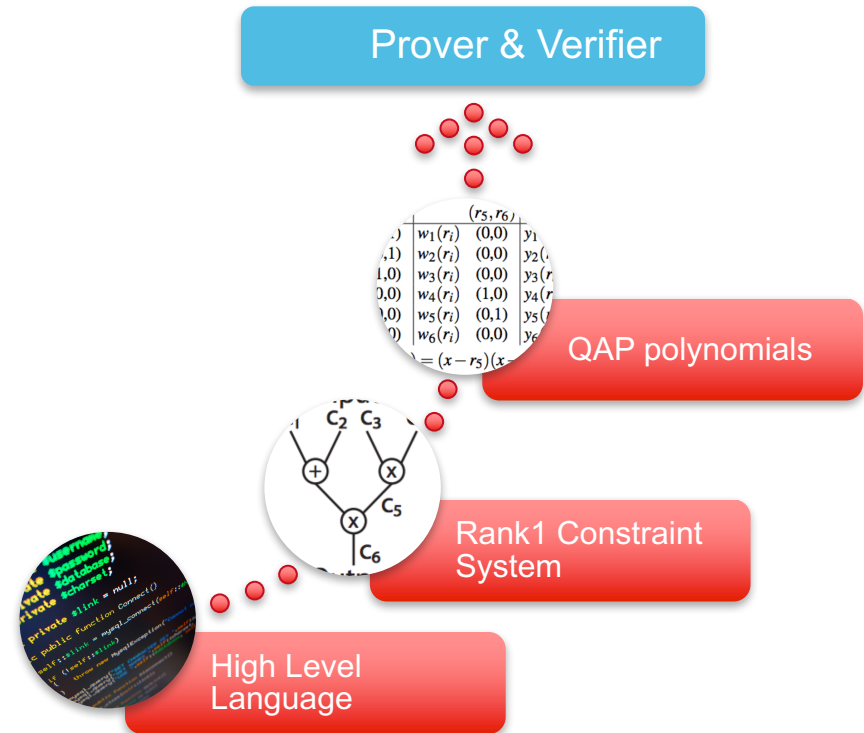
Blockchain Network

Problem:

Verifiable computations are complex to specify and require deep technological understanding

ZoKrates

- A higher-level language
- and compiler, which transforms a more convenient representation into verifiable programs based on zkSNARKS.
- Additionally, generates Ethereum Smart Contracts, which verify the results on-chain



Setup & Proof Implementation Options

Internal setup process:



Challenge:

- Process rather straight forward from R1CS on
- But: Code to R1CS conversion leads to huge amount of conditions with traditional languages

➔ Simple Language + Compiler to transform Code into R1CS
Also serves as prover

```
//Simple Code Example
def ifeq(x):
y = if (x + 2) == 3 then 1 else 5 fi
z = if y == x then x**3 else y**3 fi
return ((x + y) + z)
```

Demo


Verification on Ropsten Testnet

Overview

Event Logs

Transaction Information

Tools & Utilities

TxHash:	0xc8b957388627d49694a6cb9865bbf3d0418f7e49b7b487498c09fc31f0f1c9ce
Block Height:	1849266 (15 block confirmations)
TimeStamp:	4 mins ago (Oct-11-2017 12:27:47 PM +UTC)
From:	0xca5f75d4bff6d1e2f77812ff41d50414c335c20c
To:	Contract 0x3e561c8f9510bd61f86d281157dd73bf326f4bbc 
Value:	0 Ether (\$0.00)
Gas Limit:	1673418
Gas Used By Txn:	1670296
Gas Price:	0.00000009 Ether (90 Gwei)
Actual Tx Cost/Fee:	0.15032664 Ether (\$0.000000)
Cumulative Gas Used:	1670296
TxReceipt Status:	Success
Nonce:	12
Input Data:	<div>Function: verifyTx() *** MethodID: 0x6dae022f</div> <div>Convert To Ascii</div>

Verification on Ropsten Testnet

Transaction 0xc8b957388627d49694a6cb9865bbf3d0418f7e49b7b487498c09fc31f0f1c9ce

[Home](#) / [Transactions](#) / [Transaction Information](#)

Overview

Event Logs

Transaction Receipt Event Logs

[0] Address [0x3e561c8f9510bd61f86d281157dd73bf326f4bbc](#) 🔍

Topics [0] [0x3f3cfdb26fb5f9f1786ab4f1a1f9cd4c0b5e726cbdfc26e495261731aad44e39](#)

Data

Num ▾ → 32

Num ▾ → 34

Text ▾ → Transaction successfully verifie

Text ▾ → d.

Thank you!