RISE OF THE ZAPPS

ZoKrates

Jacob Eberhardt

Socrates: *I know that I know nothing*

ZoKrates: *I know that I tell nothing*

```
def add(a, b, c):
  return a + b + c
with add(1, 2, 3), call
./zokrates compile –i 'add.code_path'
./zokrates compute–witness –a 1 2 3
./zokrates setup
```

```
/zokrates setup
```

1. Improved setup phase:

Power of TAU

Sean Bowe, Ariel Gabizon and Ian Miers

Cheap, scalable, secure
To occur in 2018 HF
+ zapps

Zcash 2018 hardfork

- new elliptic curve for improved zk-snarks (ethereum would need to HF to include)

- Compulsory shielded addresses?

2. Zk-STARKS

Eli-Ben Sasson, Iddo Bentov, Ynon Horesh, Michael Riabzev

- No setup phase
- Computes in milliseconds
- Quantum resistant
- Ethereum compatible
- Weeks from publication

Further reading:

ZoKrates:
https://github.com/JacobEberhardt/ZoKrates

Power of Tau: https://eprint.iacr.org/2017/1050

Zk-STARKS first algorithm: https://eccc.weizmann.ac.il/report/2017/134/
Vitalik Buterin breakdown: http://vitalik.ca/general/2017/11/09/starks_part_1.html

coindesk.com/author/rachelroseoleary