Andrey Sobol

All chains will be rollup after 10 years

Bitcoin

Segwit → single ZK proof

Bitcoin Script + Signatures (ecdsa, schnorr) can be proven

Ethereum and other EVM based chains

All EVM instruction + all signatures → single ZK proof

Before Universal Trusted Setup

	SNARKs	**STARKs**	**BulletProofs**
verification	O(1)	O(poly-log(N))	O(N)
proof size	O(1)	O(poly-log(N))	O(log(N))
trusted setup	Yes	No	No

After Universal Trusted Setup

	SNARKs	**STARKs**	**BulletProofs**	**SNARKs with Universal Trusted Setup**
verification	O(1)	O(poly-log(N))	O(N)	O(1)
proof size	O(1)	O(poly-log(N))	O(log(N))	O(1)
trusted setup	Yes	No	No	Universal

Recursion (Chain of proofs)

```
prove(statement[n] +
    + prove(statement[n-1] +
        + prove(statement[n-2] +
        + ...
        )
    )
)
```

Recursion == Turing Completeness

Matter labs

https://matter-labs.io/