Building On Bitcoin

Peter Todd

Mar 8th 2017

37EC 7D7B 0A21 7CDB 4B4E 007E 7FAB 1142 67E4 FA04

What are we accomplishing?

Most software development makes things *possible*.
But security is about making things *impossible*.

What kind of work are we doing?

"Blockchain" apps are cryptographic protocols.

What is "blockchain" cryptography?

"Blockchain" cryptography proves things.

Timestamps

What is proven: Message m existed before time t.

How: OpenTimestamps

Uniqueness

What is proven: Key *k* is maps to value *v* globally.

How: Transaction Outputs (Single-Use-Seals)

Proof-of-Publication

What is proven: Message *m* reached a large audience.

How: Hash-Lock Scripts

Proof-of-Burn

What is proven: Thing x cost v to create.

How: Bitcoin Sacrifices

Why use Bitcoin?

Stability

Why use Bitcoin?

Proof-of-Work

Thank you!