MIT Bitcoin Expo, March 7, 2020

TAPRÖÖT

Who · How · Why

Andrew Poelstra

Director of Research, Blockstream

öne

What is Taproot?

Spending Conditions: Keys and Scripts

- To spend bitcoins one must satisfy the coins' spending conditions
- These conditions are specified using Bitcoin Script
- Conditions include: signature checks, hashlocks, timelocks
- Not included: velocity limits, spend destinations, refund mechanisms (future work?)

Spending Conditions: Scripts and Witnesses

- A script may specify a wide set of spending conditions, but ultimately only one is used
- For privacy and scalability, alternates should not be revealed
- Since 2012 this idea (MAST) has been floated, but never implemented. Why?

Spending Conditions: Keys Tricks

- Signature check (against a key) is the most common condition
- Keys can express much more than sig checks
- Multisignatures, threshold signatures, hashlocks, commitments
- $P \to P + H(P, m) \cdot G$

Spending Conditions: Taproot Assumption

Taproot Assumption

If all interested parties agree, no other conditions matter.

Taproot

- Use MAST to hide conditions behind a Merkle root. . .
- . . . then hide the Merkle root with a key-commitment. . .
- . . . and allow direct spends with the key

twö

Designing for Bitcoin

Is Bitcoin Dead?

- Public perception is that Bitcoin development is very slow
- *Deployment* on Bitcoin is indeed slow, with good reason
- (Is it slow enough?)
- The pace of research is overwhelming

The Unbearable Heaviness of Protocol Changes

- Every change must be accepted by the entire community
- Miners, protocol developers, wallet developers, HSM developers, retail users, institutional users, exchanges, custodians, etc., etc.
- If a change makes their lives meaningfully worse, it won't happen
- Requiring a software update is probably "making lives meaningfully worse"

The Unbearable Heaviness of Protocol Changes

- Bitcoin is worth about about $170bn
- Mistakes (probably) can't be undone

Tradeoffs Suck

- Cryptography lets us do many things with no additional resources
- But not everything (?)
- Even a few wasted bytes can be the difference when adopting a proposal (want a win for as many people as possible)
- There is also a complexity cost

Political Things

- Segwit saw some dramatic political posturing, but ordinary politics are less exciting
- Many participants are afraid of change or complexity for consensus risk
- Many developers do not want to learn and implement new crypto (increased cost, risk of mistakes, user confusion)
- Bikeshedding, demand for proofs, generating excitement, etc.

Andrew Poelstra
coronavirus@wpsoftware.net

Blockstream