Scaling Bitcoin 2018 Workshop Proposal

Andrew Poelstra

2 July 2018

Summary. A workshop to focus on scriptless scripts, adaptor signatures and their applications. Topics covered are: Schnorr signatures and their relation to ECDSA, adaptor signatures, and their application to atomic swaps. A detailed agenda is as follows:

1. (5-10 minutes) Schnorr multisignatures using MuSig [1], and their comparison to ECDSA and multisignature ECDSA. How Schnorr sigantures may be integrated into Bitcoin, including Taproot [2].

2. (5-10 minutes) Introduction to *adaptor signatures*, an extension of Schnorr multisiganatures which can be used for several smart contract applications [3] including atomic swaps.

3. (Remainder.) Introduction to the libsecp256k1 MuSig API. This can be found at [4] and is subject to change in the months preceding the conference. How to use this API to design an interactive multiparty protocol for multisignatures, and to extend this to include support for adaptor signatures. How to use this protocol to implement an atomic swap using a modified Bitcoin Regtest network if sufficient code support is available by the time of the conference, or the Elements [5] blockchain platform if not.

[1] `https://eprint.iacr.org/2018/068`

[2] `https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html`

[3] `https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2018-05-12/slides.pdf`

[4] `https://github.com/apoelstra/secp256k1/blob/2018-04-taproot/src/modules/musig/musig.md`

[5] `https://github.com/elementsproject/elements`