1 Blinded Channel Announcements (BCA)

1.1 Abstract

This protocol is designed to announce lightning channels without linking of onchain utxo and lightning node id.

1.2 Protocol

Let there be n paritcipants wanting to announce $k < n$ lightning channels, each with a capacity $\geq C$. Each lightning channel is an already signed (perhaps not broadcasted) Taproot 2 of 2 utxo (created with MuSig2). We define the set of all the utxos $U_{\geq C} := \{utxo_1, \ldots, utxo_k\}$. The i-th utxo $utxo_i$ has a public key P_i and a secret key S_i.

The n paritcipants now communicate in a *group chat* (via tor). All participants report their utxos. Additionally the 2 participants belonging to 1 utxo open 1 *pair chat* with each other (via tor), such that there are k *pair chats*.

The i-th *pair chat*:

1. generates a private key Z_i, with a public key Q_i
2. The message $m_i := (Q_i)$ is (RSA) blinded and the blinded message M_i is announced to all participants linking $utxo_i \leftrightarrow M_i$

The blinded message M_i will now be (RSA) signed by all participants with their secret keys S_i, resulting in signatures $(S_1^{M_i}, \ldots, S_k^{M_i})$. Each participant will sign only 1 message from each other participant.

The i-th *pair chat*:

1. Unblinds the signatures $(s_1^{m_i}, \ldots, s_k^{m_i})$ and combines them to a token $t_i := (m_i, U_{\geq C}, P_0, \ldots, P_k, s_1^{m_i}, \ldots, s_k^{m_i})$ proving m_i is assigned to some (unknown) utxo in $U_{\geq C}$. The token ownership of t_i can be proven by signing t_i with the secret key Z_i, resulting in a signature s^{t_i}.
2. Announces their channel: minimum capacity C, both node ids, t_i and s^{t_i}

1.3 Summary

With this protocol the owners of a lightning channel can announce their channel without revealing which utxo is the basis for their channel, only that their utxo is one of the otxos in $U_{\geq C}$.

1.4 Downsides

1. Similar to coinjoin this protocol needs an annonymity pool of utxos of a minimum capacity C, and interaction between participants before channel are announced. One could for example standardize that $C \in \{0.01 \text{ BTC}, 0.05 \text{ BTC}, 0.1 \text{ BTC}\}$

2. The exchange of the signatures $S_1^{M_i}$ is not atomic. So the protocol is incomplete if some participant stops cooperating, giving some participants perhaps a sull set of signatures, while other participants have an incomplete set.

3. I am not a cryptographer, so there could be plenty of security holes in this protocol. Looking for feedback!