# zk-TRISA

Eric Bert Jake

# The Security Problem

Our constraints:

- We want all VASPs to use TRISA
- Travel Rule: Counterparty PII recorded **before** a Tx is sent
- All ICOs accepting Fiat etc. are VASPs
- … How many ICOs in 2018 were Scams...

So we's have to bottleneck access to TRISA, but

- this limits adoption of TRISA
- This delegates trust to the TRISA gatekeepers
    - who may have different incentives than users & VASPs
    - Small Exchanges can be sold...

Could use public keys

- These can be compromised

# Can we save zk-TRISA from Sketchy ICOs?

If we add Seperate Endpoints to TRISA:

(1) DNS using Trisanyms `bert@kraken, 24601@vasp-loudon`
(2) Only one Initial Point where PII is shared between VASPs using zk
(3) User could be offered to approve/deny requests
(4) All Subsequent Steps are ZK

We will use Bit Commitments

& Bulletproofs

# Bit Commitment

Alice wants to commit to Bob a fact x

1. Agree on (Cryptographic) Hash to be used
2. Commitment Stage

   Alice --Hash[ x , salt ]---+ Bob

   (Bob Takes some action knowing Alice cannot reliably lie about x)

3. Reveal Stage

   Alice —( salt )----+ Bob

   (Bob takes some action now that Alice has proven)

# Zero-Knowledge for Cheap

Alice and Bob exchange PII and Trisanyms out-of-band,

Alice and Bob each

SNDR --Commit(SPII, salt)---+ RCVR: Now SNDR can’t fake knowledge of SPII

RCVR --Commit(RPII, salt’)--+ SNDR: Now RCVR can’t fake knowledge of RPII

SNDR ——-(salt)----------+ RCVR: Now SNDR can confirm SPII === RPII

SNDR ——-(salt)----------+ RCVR: Now SNDR can confirm SPII === RPII

Both

(1) SNDR and RCVR know eachother knows the same thing

(2) Without revealing that knowledge to eachother.

# zk-TRISA Saved from Sketchy ICOs!

If:

(1) DNS using Trisanyms `bert@kraken, 24601@vasp-loudon`
(2) Only one Initial Point where PII is shared between VASPs
(3) User could be offered to approve/deny requests
(4) All Subsequent Steps are ZK
(5) So long as the Initial Point is secure:

**⇒ Bad Actors can’t abuse TRISA to Harvest PII**

# Demo!

# Bulletproofs

- Composable: Can confirm M transfer-intents in *O(log M)* time
  - Downside: all fail or confirm together
- Save and Audtior can independently verify *without knowing PII*
  - Not true for Bit Commitments
- Can Prove Set Membership
  - Can test DOB / country x whitelist **without** revealing
- Minor: ZKPs acts as a PoW - could raise spammer costs
  - like hashcash for email