FROST Federation

Kulpreet Singh
kp@opdup.com

Contents

- Use case
- Approach
- Plan

Use Case

- Replace centralised pool operator with a federation of pool operators
- A federation remains online and signs payouts for miners
- Membership decided by inputs into a UTXO

Approach

- FROST TSS

- FROST KeyGen with a BFT broadcast in KeyGen’s second round
  - Robustness is important for us
  - We can’t use a coordinator
  - Threshold requirement - if no honest majority, federation will disband with unilateral exits

Plan - Current focus on DKG

- Write KeyGen + BFT broadcast spec in TLA+

- As part of FROST Federation work we have built
  - reliable, secure and authenticated unicast
  - echo broadcast with t = 0 for now

- If KeyGen modification can work, we want to build it into our work
  - Remember, no coordinator 😢

- Measure time to completion of DKG

Help with reviews 🙏

It will be great to get some eyes on the modification to KeyGen

Thanks

Github: https://github.com/pool2win/frost-federation

Email: kp@opdup.com

Signal: jungly.01