ZF FROST Updates

Conrado Gouvea - Zcash Foundation

Main crates

- https://github.com/ZcashFoundation/frost

- 2.0.0-rc.0 is out, 2.0.0 to be released really soon
  - Some API adjustments related to serialization
  - no-std support

- Refresh shares functionality being worked on

- Taproot PR
  - Opened by contributors
  - Waiting for us to review, hopefully by the end of the month

Demo code and FROST server

- https://github.com/ZcashFoundation/frost-zcash-demo/

- FROST server
  - Helps participants to communicate with each other
  - Work in progress, currently adding encryption and authentication

- frost-client
  - CLI tool to run FROST using the server
  - Will also be a library

- trusted-dealer, dkg, participant, coordinator
  - CLI tools, might be integrated into frost-client

Our goals

- Have our ZF FROST crates be used by a Zcash-supporting wallet
  - Possibly using our FROST server
- Work with wallet developers towards that goal