

2021-02-03 Meeting Notes

1. Introductions: we have a packed agenda!
2. Presentation from Avradip on ZK frameworks.
 - a. Introduction to ZK proofs (at a high level, theory-based).
 - b. Discussion of zkinterface.
 - c. Suitability for this type of interface for Ursa?
 - d. Discussion of what to do with any work in this area.
3. Discussion on what to do with pairing plus.
 - a. How to best handle?
 - b. Probably put in HL repo somewhere, but clearly designate as a fork.
4. Ursa HW interface.
 - a. Gauging interest in hardware.
5. Go implementation of BBS+: will be open-sourced soon.