2021-01-20 Meeting Notes

1. Introductions/welcome. We had one new participant–Andreas. Welcome!
2. Discussion on zero knowledge framework (Avradip). General discussion.
    a. Dan M: we could use a little bit more information and precision.
    b. Avradip: will come back with more info next time.
3. Discussion on signature interface.
    a. Mike lost a bunch when his computer crashed.
    b. Some slight issues with Pairing+: using old hash to curve.
    c. Discussion of blind signatures.
        i. Tricky to get public interface right.
        ii. Excellent explanation by Mike in detail.
        iii. This took up most of the meeting time, and was well worth it.
        iv. TODO: Come up with better blind signature interface that is more misuse resistant.