

2019-05-29 Meeting Notes

1. Outstanding PRs: no code stuff, language binding stuff.
 - a. Suggestion: have a folder for draft RFCs to bring down RFC clutter.
2. Rust Signature API: rust developers have put a basic signature API together. Can we use it, or should we mimic it?
 - a. People need more time to go over it.
3. Zmix API discussion.
4. When do we want to shoot for 1.0?
 - a. Code audits?
 - b. Crypto code review questions. What's the best way to do it?
5. Try to get CII badge stuff soon. Talk to Dave?
6. What does everyone want out of Ursa v1.0?
 - a. DFINITY crowd: ZKlang.
 - b. We need to polish the Zmix spec.
 - c. Sawtooth: maybe some non-simple signatures and ZK stuff.
 - d. Code audits: best way to do for theoretical and non-theoretical stuff.
7. Other CI targets?