Abstract

We propose a privacy-preserving version of Casper FFG, tentatively titled Casper EFG (Elusive Finality Gadget), using traceable ring signatures. Through the use of traceable ring signatures, validators are anonymous as long as they are honest and in the case of dishonest validators, they can be de-anonymized and penalized accordingly.

Note that this is a work-in-progress and I am seeking feedback on the idea.

Overview

We define a traceable ring signature scheme as follows:

Let L = (issue, pk_N)

denote a tag where pk_N

is the set of public keys of the ring of validators and issue

is say the id for a particular epoch voting period or blocks. Any validator in the ring can vote for blocks using their own private key and a verifier can verify a signature with respect to L

but doesn't know who generated the signature among validators in L

. If the same block is signed twice by the same validator, everyone can see that the signatures come from the same private key. In other words, they are linked. If two different blocks are signed within the same epoch at the same height with the same tag, then not only do we know that the signatures are linked, the anonymity of the validator is revoked.

Traceable ring signatures provide us with a few nice properties:

Public Traceability

: Anyone who votes for conflicting blocks (note: an extension to surround votes can be made) can be traced

Tag-Linkability

: Every two signatures made by the same validator with respect to the same tag are linked.

Anonymity

: As long as the validator is honest i.e. not signing the same block with respect to the same tag, they are indistinguishable from the other validators. Moreover, for different blocks (tags), signatures are unlinkable.

Exculpability

: An honest validator cannot be accused of signing twice with respect to the same tag.

These properties make it such that we should be able to still provide penalties and attribute faults to validators.

Penalization

In order for this scheme to work, we need to be able to penalize validators who vote for different blocks at the same height and/or surround votes. For now, consider the case where a dishonest validator votes for conflicting blocks. EDIT: Now that I had some sleep, I don't think it's possible to fit surround votes in this framework. It would perhaps have to be done outside of the protocol. More thought is needed.

Let L = (issue, validators_{pk})

where L is a tag, the issue is a vote on blocks and validators_{pk}

is the ring of validator public keys.

Let v_{dishonest} \in validators_{pk}

be the public key of a dishonest validator.

As per the traceable ring signature, once this validator votes on conflicting blocks at the same height, they will be de-anonymized. Now, we know who voted dishonestly and can penalized them. However, once they have been de-anonymized, they can no longer participate in Casper since we know who they are. Thus, we make penalize them such that they lose their entire deposit.

So, this added anonymity makes it such that a validator wants to stay anonymous so that they don’t lose their investment.

Future work

This was a very informal description of how Casper FFG can be made privacy-preserving using traceable ring signatures. Next steps would be to formalize this idea and show that the usual properties hold under these conditions.