Improve the explanation about our motivation regarding that today there is a privacy preserving problem in permissioned ledgers and the used of this architecture has been turning more popular, increasing the need to solve this open issue. Add more examples of real projects/services that are based on permissioned ledger like Ptwist for a close cryptocurrency (in a circular economy) and the use case of Maersk and IBM

Improve our explanation about our contribution regarding the differences between our protocol and the current one. It is important to state that know the user’s identity is crucial for BA consensus mechanism, because if not, they can be attacked using sibyl attacks. On the other hand, there is no literature that address this issue, so our model is a novel proposal.

Explain better when the CA and for what the CA gets involve in the transactional process

Define better the roles and functions of each network member

Unlink our paper with Fabric PBFT (just generates confusion)

Explicitly state that the user privacy is achieved by unlink the transaction with the user ID that by default is associated with the user credentials generated by the CA

Explain WHY Okamoto-schnorr signature was selected and no David Chaum’s one. Basically, we are looking for just for the blind signature and not blind message. The idea is kept information public but unlink the transactions with the user that generated it. This is well address by Okamoto changing the original Zero Knowledge Proof Authentication scheme proposed by Schnorr and turn it in blind signature scheme under random oracle model.

Improve the definition of Consistency by adding that refers to the property of record a transaction and kept it immutable in time.

Improve typos