The XY Oracle Network: The Proof-of-Eligibility

Arie Trouw *

March 2018

Abstract

Some smart contracts require that only certain people or entities are allowed to transact with them, but they are often exposed to cost base attacks because the process of validating the eligibility of the caller has cost. In most cases, if determining eligibility prior to allowing the contract to complete, the risk is on the contract holder to absorb the cost of the check, and the caller burdens no risk. XYO's Proof of Eligibility (PoE) solves this problem by allowing the user to transact first and then validate eligibility afterwards, but prior to receiving the benefit of the transaction.

1 Introduction

Reducing the time to transaction for smart contracts is very important for customers and companies. PoE addresses this with a few benefits. Preserves order of transaction by having the initiation of the transaction be instant so that any verification delay does not report the transactions. Confirms to the user that they did not miss out in the case where the contract is temporal or has a limited capacity. Commits the user to the transaction, preventing cost based attacks.

2 architecture

3 process order

*XYO Network, arie.trouw@xyo.network

4 Acknowledgements

This white paper is the product of an inspiring team effort that was made possible through the belief in our vision from the following individuals: We thank Christine Sako for her exceptional work ethic and attention to detail in her review of our work. The consistency in structure and best-practices observed in our white paper is the product of Christine's efforts. We thank Johnny Kolasinski for his research and compilation of applicable use cases. Last, we thank John Arana for his careful review and creative input.

References

Glossary

. 1, 2, 4, 5, 7, 9

. 4, 5, 7, 14, 15

. 6, 7, 9, 11

. 7

. 1, 8, 9

. 4, 5, 12, 14, 15

. 1–4, 8, 9, 13, 16

. 3

. 15

. 4, 5, 7, 8, 11, 13–15

. 4, 5, 7–9, 11, 14

. 1, 3, 4, 8, 14

. 4, 6, 7, 11, 14

. 11

. 1, 4, 5, 8, 11, 12, 15

. 4, 7, 10–12, 14

. 5–7

. 3–5, 7, 9, 12–16

. 1–5, 7, 13, 16

. 11

. 1, 3–5, 8, 14, 16

. 1

. 2–5, 7, 11, 14–17

. 4–7, 14