The XY Oracle Network: Proof of Eligibility Transactions and XYO Token Sale Logistics

Arie Trouw *

March 2018

Abstract

Most smart contracts only allow certain entities to be eligible to engage in transactions. There is an incurred burden and expense with the eligibility validation process of the contract caller that can expose contract holders to high drop-off rates and cost-based attacks. Traditionally, confirmation of eligibility verification is often saved only to external servers, not to the smart contracts themselves, leaving the potential for contract holders to incur future risks. The XYO Network (XY Oracle Network) provides a solution to the risk assumed by contract holders by establishing the architecture for **Proof of Eligibility (PoE)** transactions. The implementation of PoE allows the contract caller to validate their eligibility *after* initiating a smart contract, which confirms their position in contracts that are temporally sensitive and/or have limited availability. Additionally, transactions with Proof of Eligibility save affirmation of eligibility verification directly to the smart contract in order to prevent any further liability to the contract holder. The XYO Network employs Proof of Eligibility transactions to minimize liability and risk to Token buyers in its limited volume and variably priced XYO Token Sale. The XYO Network also adopts the Proof of Eligibility structure for all XYO Token Sale transactions due to its requirement for Token buyers to have KYC ("Know Your Customer") eligibility verification.

1 Introduction

The verification for Smart contract eligibility is most frequently implemented to selectively permit transactions between contract holders and eligible contract callers. The requirement of contract caller eligibility verification ensures safety and control for contract holders, but results in higher costs for contract holders who must pay to invoke this process. Eligibility verification is burdensome and complex for contract callers, which can lead to their decreased commitment and higher drop-off rate. Finally, contract holders can also be hurt by cost-based attacks, where entities interested in increasing costs to contract holders continuously provide irrelevant or false data in order to initiate the process of eligibility verification, without the intent to complete a transaction. This type of attack incurs very little cost to the attacker, but high costs to the contract holder.

*XYO Network, arie.trouw@xyo.network

Proof of Eligibility mitigates the dilemma involved with historical implementations of eligibility verification and potential cost-based attacks through a reorganization of the steps required to complete a transaction. Traditional transaction architecture prioritizes the process of eligibility verification over the initiation of the transaction, which negatively impacts both the contract caller and the contract holder. Contract callers are deterred sooner in the transaction for two reasons: the eligibility verification process is complex and laborious, and the duration of the third-party eligibility verification procedure threatens their opportunity to execute the contract. Contract holders experience greater contract caller drop-off rates while exposing themselves to cost-based attacks due to the low cost for the contract caller to input data for verification. The XYO Network's PoE model for transaction architecture prioritizes the *initiation* of the smart contract over the overall *process* of eligibility verification. Initiating a contract earlier in the overall transaction process both preserves the original transaction order in the blockchain and timestamps the initiation of the contract (which is particularly useful for contract callers in cases of smart contracts that are temporally sensitive and/or have limited availability). Additionally, initiation prior to verification increases the contract caller's commitment to the transaction earlier in the funnel, which decreases their drop-off rates and deters them from performing cost-based attacks.

The usage of Proof of Eligibility in smart contract transactions provides the benefits of preservation of transaction order, confirmation of contract initiation, and increased contract caller commitment.

---

2 Historical vs. XYO Network's Implementation of Transaction Architecture

Historical implementations of smart contract transaction architecture prioritize eligibility verification prior to smart contract initiation and ultimately save the eligibility verification data to a server. This approach is susceptible to cost-based attacks, higher drop-off rates, and loss of data (should the server be compromised). The XYO Network's implementation of Proof of Eligibility restructures transaction architecture and prioritizes transaction initiation over the eligibility verification process. The requirement of the contract caller to initiate the contract *before* the verification process increases their commitment to the contract and disincentivizes them to abandon or attack the contract holder. Additionally, PoE transaction architecture saves verification data directly to the smart contract itself, which is far more secure than a private server.

2.1 Diagram and Comparison

The following diagram emphasizes the prioritization of eligibility verification vs. smart contract initiation between the historical and XYO Network's transation architecture. The steps in each process are outlined in order and reveal that while a Proof of Eligibility transaction is more complex, it benefits from the separation of the smart contract execution into an initialization step and a completion step. This separation solidifies contract caller commitment earlier in the structure. For added security, a PoE transaction saves verification data directly to the smart contract instead of to a server.

Historical Architecture Process

1. Introduce Contract caller-facing platform
2. Begin eligibility verification
3. Send caller to third-party for eligibility verification
4. Store caller eligibility
5. Return to customer-facing platform with eligibility verification
6. **Execute contract**
7. **Save verification data to server**

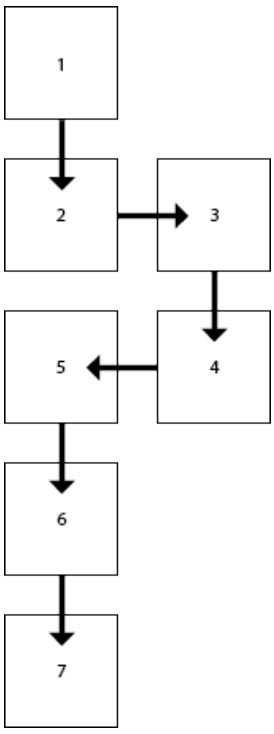

Figure 1. Historical Architecture

PoE Architecture Process

1. Introduce Contract caller-facing platform
2. **Initiate transaction**
3. Begin eligibility verification
4. Send caller to third-party for eligibility verification
5. Store caller eligibility
6. Return to customer-facing platform with eligibility verification
7. **Complete contract**
8. **Save verification data to smart contract**

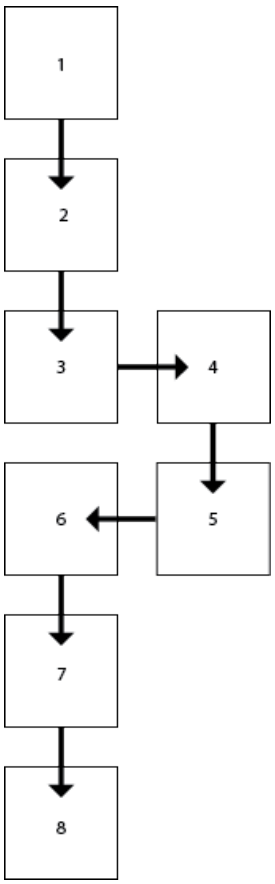

Figure 1. PoE Architecture

3 Example: XYO Token Purchase with Ether

A purchase of XYO Tokens with Ether exemplifies the benefits of a transaction utilizing Proof of Eligibility due to the complexity of the XYO Token Sale's pricing structure. The XYO Token Sale employs a pricing model that is calculated from a token availability-based equation designed by the XYO Network. This temporally sensitive and availability-based pricing makes a Proof of Eligibility-based transaction architecture particularly favorable to both the XYO Network and contract callers who wish to contribute Ether to purchase XYO Tokens. The dependence of price on real-time token availability renders confirmation of contract initiation and maintenance of transaction order crucial.

During any Token Sale that employs price variability and/or volume-sensitivity, it is imperative for a contract caller's position in the order of transactions to be maintained. When a Token price is contingent on the number of Tokens sold to-date, the longer a contract caller waits to purchase Tokens with Ether, the higher the Token price (unless the Token price became fixed at an earlier point). If the Token price in Ether becomes fixed, maintenance of transaction order in relation to others will still be important to contract callers, since a contract initiation that occurs after the final token is sold will result in a a zero-Token return.

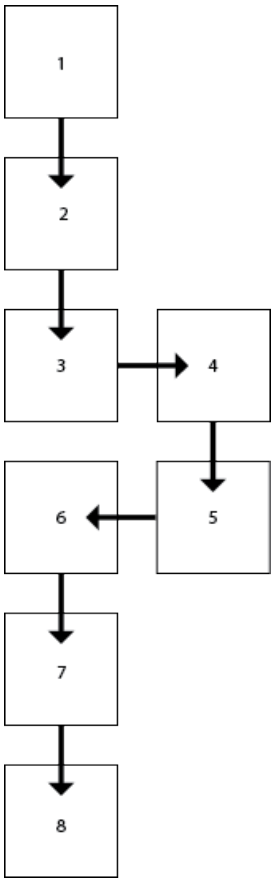

Figure 1. Contract Caller purchases XYO Tokens with Ether

Process

1. Customer sends Ether payment for XYO Tokens to the smart contract.

2. The smart contract records the transaction by adding the incoming address to a list and associates it with the number of XYO Tokens that are to be distributed to the customer. The contributed Ether is added to the value of the contract.

3. The customer completes the verification process (KYC and/or AML).

4. An authorized wallet calls the contract to confirm that the customer has passed eligibility verification.

5. The smart contract transfers the XYO Tokens due to the customer to their associated wallet address and the Ether that was given is sent to the company. Eligibility verification is saved directly to the smart contract.

6. At the conclusion of the XYO Token Sale, all remaining unverified Ether from unfinished contracts is forfeited to the company. (See Section 4.1-4.1.1 for mitigation to speculation)

---

4 Early Commitment and Resulting Risks of PoE

The transaction architecture established by Proof of Eligibility strengthens and solidifies user commitment earlier in the transaction process than in historical implementations. Earlier user commitment carries a significant benefit for contract holders, as it reduces user drop-off rates and disincentivizes contract callers from attempting cost-based attacks. While earlier commitment make the benefits to contract holders near absolute, this feature also makes it difficult for smart contract callers to withdraw from a contract, should they wish to withdraw at a later point in the transaction process. Contract callers may try to get around this loss of control by waiting to complete their eligibility verification after the contract has been initialized, maybe indefinitely. In cases where the output of an executed contract changes in value after initialization, this practice can lead to speculation. This is particularly relevant in transactions that have low initial costs to the contract caller or circumstances where there is an opportunity for return or transaction reversal after the eligibility verification process has occurred. The importance of contract initialization prioritization in PoE means smart contract callers are more dependent on contract holders, as smart contract holders control the implementation of any third-party eligibility verification provider. Thusly, increased and earlier commitment of smart contract callers requires a great deal of trust between the contract caller and contract holder.

4.1 Speculation in Future-Based Transactions

When smart contracts involve elements that change in value, size, or other qualities over time, contract callers and contract holders are often concerned about the speed of their contract execution. In cases involving tokens, coins, or equity, contract callers traditionally wish to execute a contract with the hopes of a future gain. However, when the market value of the element experiences short term fluctuations, contract callers may engage in speculation. Instead of executing a contract for a long-term market or intrinsic value gain,

these contract callers may prolong the execution of the smart contract in order to examine and capitalize on short term fluctuations.

Both historical and PoE transactions are susceptible to contract caller speculation, as contract callers can either wait to begin eligibility verification (maybe indefinitely), or initiate the contract and *then* prolong eligibility verification. Every implementation of transaction architecture will need to find a way to mitigate this possibility, each dependent on the individual nuances of the elements pertaining to the contract. The XYO Network's approach with Proof of Eligibility transactions lessens the potential for this speculation since contract callers are required to initiate a contract prior to eligibility verification.

4.1.1 Speculation Mitigation in XYO Token Sale

In the XYO Token Sale, Proof of Origin-based transactions allow contract callers to confirm their Token price at contract initiation, which is particularly alluring given the XYO Token's variable pricing structure and limited availability. However, the PoE structure also allows for the possibility of a contract caller to confirm their initiation position, contribute Ether, and then deliberately fail, prolong, or discontinue the eligibility verification process. To mitigate this possibility, the XYO Network has built step 6 in the XYO Token Sale Process (See Section 3), which states that, "all remaining unverified Ether from unfinished contracts is forfeited to the company." The XYO Network acknowledges that any incomplete contracts may be a result of speculation or cost-based attacks, so the the decision to keep any unverified Ether aims to deter this type of activity. Additionally, the XYO Network does not allow transaction reversal: once a contract has been initiated, contract callers will have 1 year from initiation date to complete eligibility verification.

The use of PoE transactions for the XYO Token Sale allows contract callers to establish and confirm their position relative to other Token purchasers, which is especially relevant due to the XYO Token's variable pricing structure and limited availability. To alleviate pressure on contract-callers, the eligibility verification completion window will extend past the date of conclusion of the the XYO Token Sale. This allows contract callers to initiate a contract during the XYO Token Sale, and be able to execute the contract after the Token Sale's end shall their eligibility verification process take longer than expected. Should a contract caller not complete their eligibility verification within the allotted 1 year window of time or fail to pass verification completely, the smart contract will not be executed and the Ether will be forfeited to the XYO Network.

4.2 Trust Between Contract Caller and Contract Holder

In situations where smart contracts require eligibility verification and there is no opportunity for transaction reversal, there must exist a great deal of trust between both the contract caller and contract holder. In many circumstances, the contract holder has the power to control the implementation of a third-party to process eligibility verification, so the contract caller must trust that the contract holder has no intent to manipulate the process.

---

5 Acknowledgements

This white paper for Proof of Eligibility is a corollary to the XYO Network white paper. We thank Jordan Trouw for her data sourcing and collaboration in her contributions to this paper. We also thank Christine Sako for her review and application of best-practices in her review of this work.

Glossary

contract caller An entity that initiates a smart contract, on the receiving end of the contract holder's input. 1–6

contract holder An entity that controls a smart contract, on the receiving end of the contract caller's input. 1, 2, 5, 6

cost-based attack A malicious attempt by one entity to increase incurred costs for another, often through high-volume data input for a costly process with little to no cost to the attacker. 1, 2, 5

PoE Proof of Eligibility. 1, 2, 5

Proof of Eligibility Addresses the dilemma of eligibility verification and potential cost-based attacks through a reorganization of the steps required to complete the transaction. 2, 4–7

Proof of Origin Proof of Origin is the key to verifying that ledgers flowing into the XYO Network are valid. A unique ID for source of data is not practical since it can be forged. Private key signing is not practical since most parts of the XYO Network are difficult or impossible to physically secure, thus the potential for a bad actor to steal a private key is too feasible. To solve this, XYO Network uses Transient Key Chaining. The benefit of this is that it is impossible to falsify the chain of origin for data. However, once the chain is broken, it is broken forever and cannot be continued, rendering it an island. 6

smart contract A protocol coined by Nick Szabo before Bitcoin, purportedly in 1994 (which is why some believe him to be Satoshi Nakamoto, the mystical and unknown inventor of Bitcoin). The idea behind smart contracts is to codify a legal agreement in a program and to have decentralized computers execute its terms, instead of humans having to interpret and act on contracts. Smart contracts collapse money (e.g. Ether) and contracts into the same concept. Being that smart contracts are deterministic (like computer programs) and fully transparent and readable, they serve as a powerful way to replace middle-men and brokers. 1, 2, 5, 6

transaction The necessary requirements and entire process involved in the execution of a smart contract. 1, 5, 6

transaction architecture The basic structure of a transaction, often a list of steps that result in an executed smart contract. 2, 4–6

XY Oracle Network XYO Network. 1

XYO Network XYO Network stands for "XY Oracle Network." It is comprised of the entire system of XYO enabled components/nodes that include Sentinels, Bridges, Archivists, and Diviners. The primary function of the XYO Network is to act as a portal by which digital smart contracts can be executed through real world geo-location confirmations. 2, 4, 6, 7