XY Oracle Network: La Rete di Localizzazione Crittografica basata su Proof-of-Origin

Arie Trouw *, Markus Levin †, Scott Scheper ‡

Gennaio 2018

Abstract

Con la crescente presenza di tecnologie connesse che dipendono dalla localizzazione, la nostra privacy e sicurezza dipendono fortemente dall'accuratezza e dalla validità dei dati di posizione. Si sono compiuti diversi sforzi per rimuovere la necessità del ricorso a soggetti centralizzati che controllino il flusso di tali dati, ma ognuno di questi tentativi si è basato sull'integrità dei dispositivi che raccolgono le informazioni sul piano fisico. Noi proponiamo una rete di localizzazione crittografica priva di terze parti fiduciarie (trustless) che utilizza una nuova formulazione basata su una catena di dimostrazioni a conoscenza zero (zero-knowledge proof) per stabilire un grado elevato di certezza sui dati di posizione. XYO Network (XY Oracle Network) è un'astrazione che permette la verifica stratificata della localizzazione attraverso molte categorie di dispositivi e protocolli. Al suo nucleo ospita un insieme di originali meccanismi crittografici conosciuti come Proof of Origin e Bound Witness, che collegano il potere della tecnologia blockchain con la raccolta dati sul piano fisico, creando un sistema con applicazioni dirette nel mondo attuale.

1 Introduzione

Con l'avvento degli smart contract trustless basati su blockchain, è cresciuta significativamente la necessità di servizi oracle che gestiscano l'esito di un contratto. Per stabilire la conclusione del contratto, la maggior parte delle attuali implementazioni di smart contract si basa su un insieme singolo o aggregato di oracle autorevoli. Nei casi in cui entrambe le parti possono trovarsi d'accordo riguardo all'autorità e all'incorruttibilità di un determinato oracle, questo metodo risulta sufficiente. Tuttavia, in molti casi non esiste un oracle idoneo oppure non può essere considerato autorevole a causa della possibilità di errore o di danneggiamento.

Gli oracle di localizzazione ricadono in questa categoria. La predizione della posizione di un oggetto nel mondo fisico si basa sui componenti di segnalazione, trasmissione, archiviazione e processamento di un dato oracle, tutte attività che comportano errore e possono risultare corrotte. I rischi includono la manipolazione dei dati, così come la loro contaminazione, perdita nonché fenomeni di collusione.

*XYO Network, arie.trouw@xyo.network
†XYO Network, markus.levin@xyo.network
‡XYO Network, scott.scheper@xyo.network

Sussiste pertanto il seguente problema: **sia la certezza che l'accuratezza della localizzazione ricevono un impatto negativo dalla mancanza di un oracle di posizione che sia decentralizzato e trustless**. Piattaforme come Ethereum ed EOS sono state ampiamente usate per il loro potere di mediare le interazioni online in modo sicuro con i casi d'uso principali che implicano garanzie per la raccolta di fondi secondo le modalità delle ICO. Tuttavia, finora ogni piattaforma si è focalizzata interamente sul mondo online, lasciando da parte il mondo fisico a causa della rumorosità e della corruttibilità dei dati dei canali di informazione attuali.

XYO Network ha lavorato tenendo a mente l'idea di permettere ai developer, come ad esempio coloro che sviluppano smart contract per piattaforme blockchain, di interagire con il mondo fisico come se fosse una API. XYO Network è il primo protocollo oracle al mondo che rende possibile a due soggetti di effettuare transazioni nel mondo reale senza una terza parte centralizzata. Le nostre astrazioni ci permettono di rendere trustless la verifica della posizione, creando un protocollo con nuovi casi d'uso fino ad oggi impossibili da mettere in pratica.

XYO Network sarà costruito su un'infrastruttura già esistente composta da oltre 1.000.000 di dispositivi circolanti nel mondo, distribuiti attraverso le imprese che vendono al pubblico dispositivi findable. I dispositivi Bluetooth e GPS della XY permettono ai normali consumatori di posizionare dei beacon di tracciabilità fisica sugli oggetti che desiderano monitorare (come chiavi, bagagli, biciclette e persino animali domestici). Nel caso perdano o non riescano più a trovare un oggetto, possono verificare esattamente dove si trovi visualizzando la sua posizione con un'applicazione per smartphone. In soli sei anni, XYO Network ha creato una delle più grandi reti Bluetooth e GPS consumer esistente al mondo.

2 Contesto storico e approcci precedenti

2.1 Proof of Location

Il concetto di posizione dimostrabile circola sin dagli anni ‘60 e si può far risalire addirittura agli anni ‘40, con i sistemi di radionavigazione terrestre come il LORAN [1]. Ora esistono servizi di localizzazione che impiegano molteplici mezzi di verifica uno sull'altro per creare una Proof of Location attraverso la triangolarizzazione e il GPS. Tuttavia, tali approcci risultano ben lontani dall'affrontare la sfida più critica che si pone alle tecnologie di localizzazione attuali, ovvero la progettazione di un sistema che rilevi i segnali fraudolenti e vada a disincentivare lo spoofing dei dati di posizione. Per questa ragione, riteniamo che al giorno d'oggi la piattaforma di cripto-localizzazione più significativa sarà quella che si focalizzerà maggiormente sulla verifica dell'origine dei segnali di ubicazione fisica.

Sorprendentemente, l'idea di applicare la verifica della posizione alle tecnologie blockchain è apparsa la prima volta nel settembre del 2016 all’evento DevCon 2 di Ethereum, introdotta da Lefteris Karapetsas, uno sviluppatore Ethereum di Berlino. Il progetto di Karapetsas, *Sikorka*, ha permesso l'esecuzione istantanea degli smart contract nel mondo reale, usando quella che denominò “*Proof of Presence*”. La sua applicazione, volta a creare un ponte fra posizionamento e mondo della blockchain, si è incentrata principalmente su casi d'uso in ambito di realtà aumentata, introducendo inoltre degli originali concetti che pongono ardue questioni in merito alla verifica della posizione di una persona o un oggetto [2].

Il 17 settembre 2016, l'espressione "*Proof of Location*" è formalmente emersa nella comunità Ethereum [3], per essere poi ulteriormente esposta da Matt Di Ferrante, sviluppatore dell'Ethereum Foundation:

> *"In tutta onestà, la Proof of Location di cui ci si può fidare è una delle cose più difficili da implementare. Anche se si hanno molti partecipanti in grado di attestare la posizione di ognuno degli altri, non c'è alcuna garanzia che questi non possano creare soltanto ambiguità in futuro; siccome ci staremo sempre e solo basando su ciò che dichiara la maggioranza, ciò rappresenta una debolezza enorme. Se si potesse dotare qualche tipo di dispositivo hardware specializzato con una tecnologia anti-manomissione, come ad esempio la distruzione della chiave privata quando qualcuno tenta di aprirlo o di modificarne il firmware, allora si potrebbe forse avere maggiore sicurezza, ma allo stesso tempo questo non renderebbe impossibile lo spoofing dei segnali GPS. Per ottenere una qualsiasi garanzia di accuratezza, un'implementazione idonea di questi concetti richiede talmente tante alternative e fonti di dati differenti che sarebbe realizzabile solo con un progetto davvero ben finanziato." [3]*
>
> —Matt Di Ferrante, Developer, Ethereum Foundation

2.2 Proof of Location: limiti

Per riassumere, la Proof of Location può essere intesa come il far leva sulle potenti proprietà della blockchain, come la marcatura temporale (*time-stamping*) e la decentralizzazione, combinandole con dispositivi off-chain dotati di localizzazione che *ci si augura* siano resistenti allo spoofing. Ci riferiamo all'ambito della tecnologia di localizzazione crittografica come "*cripto-localizzazione*". Inoltre, in modo simile a come la debolezza degli smart contract è incentrata sugli oracle che si affidano a una singola fonte di verità (e perciò hanno una singola fonte di fallimento), i sistemi di cripto-localizzazione fronteggiano lo stesso problema. La vulnerabilità delle attuali tecnologie di cripto-localizzazione si basa sui dispositivi off-chain che restituiscono la posizione di un oggetto. Negli smart contract, la fonte di dati off-chain è un oracle. Nel caso di XYO Network, invece, si tratta di una tipologia specializzata di oracle che chiamiamo Sentinel. L'innovazione fondamentale di XYO Network si concentra su una prova anonima dell'ubicazione alla base dei componenti del nostro sistema, per creare un protocollo trustless di cripto-localizzazione.

---

3 XY Oracle Network

> *"La necessità di un sistema difficile da perturbare che vada a complementare il GPS è ben nota da anni. Il GPS è eccezionalmente accurato e affidabile, ma il jamming, lo spoofing, i cyber attack ed altre forme di interferenza sembrano essere crescenti in frequenza e gravità. Questo ha il potenziale di generare effetti devastanti sulle nostre vite e l'attività economica."*[4]
>
> —Dana Goward, Presidente della RNT Foundation

3.1 Introduzione

L'obiettivo di XYO Network è creare un sistema decentralizzato e trustless di oracle di localizzazione che sia resistente agli attacchi e, alla richiesta di dati disponibili, restituisca la più elevata certezza possibile. Questo lo otteniamo attraverso un insieme di astrazioni che riducono egregiamente il rischio di spoofing della posizione tramite una catena di dimostrazioni a conoscenza zero lungo i componenti del sistema.

3.2 Panoramica della Rete

Il nostro sistema fornisce un punto d'accesso a un protocollo di dispositivi connessi che restituisce elevata certezza sui dati di posizione attraverso una catena di prove crittografiche. Gli utenti sono in grado di emettere transazioni, chiamate "query", al fine di consultare dati di localizzazione su qualsiasi piattaforma blockchain dotata di funzionalità smart contract.[1] Gli aggregatori su XYO Network si occupano poi di ricevere tali query emesse al contratto e di andare a prendere le risposte che hanno la maggiore accuratezza presso un insieme decentralizzato di dispositivi, che restituisce prove crittografiche agli aggregatori stessi. Poi, dopo aver raggiunto un consensus sulla risposta dal punteggio migliore, gli aggregatori inseriscono tali risposte all'interno dello smart contract. Questa rete di componenti rende possibile determinare se un oggetto si trovi a delle specifiche coordinate XY in un dato momento, con la maggior certezza dimostrabile possibile e in maniera trustless.

XYO Network si compone di quattro elementi primari: le **Sentinel** (Raccoglitori di Dati), i **Bridge** (Trasmettitori di Dati), gli **Archivist** (Memorizzatori di Dati) e i **Diviner** (Aggregatori di Risposte). Le Sentinel raccolgono le informazioni di posizione attraverso sensori, radio nonché altri metodi. I Bridge prendono questi dati dalle Sentinel e li passano agli Archivist, che salvano l'informazione mettendola a disposizione dei Diviner. Questi ultimi analizzano le euristiche di posizione rese disponibili dagli Archivist al fine di generare risposte alle query assegnandovi un punteggio di accuratezza. I Diviner ritrasmettono poi queste risposte all'interno di uno smart contract (pertanto, i Diviner servono da oracoli). Il punteggio di accuratezza, chiamato **Origin Chain Score**, è determinato attraverso un insieme di dimostrazioni a conoscenza zero conosciuto come **Proof of Origin Chain**. Questa catena garantisce che due o più insiemi di dati siano stati originati dalla medesima fonte senza rivelare altre informazioni sottostanti. Lungo il percorso della query, ogni componente genera la propria Proof of Origin, che viene poi collegata a quella di ciascun componente a cui inoltra i dati. La Proof of Origin è una nuova formulazione che costruisce una catena di garanzie crittografiche lungo un percorso di trasmettitori all'interno della rete al fine di offrire elevata sicurezza dei dati del mondo fisico. Questa **Proof of Origin Chain** condensa tutta la fiducia che possiamo trarre dai dati di posizione lungo tutto il sentiero che riconduce ai primi dispositivi che hanno rilevato le informazioni. Esamineremo in dettaglio come lavora la Proof of Origin nella sezione seguente.

Per istituire un meccanismo di consensus decentralizzato tra i Diviner, XYO Network si affiderà a una blockchain pubblica e immutabile nota come **XYOMainChain**, che archivia le operazioni di query insieme ai dati raccolti dai Diviner e al loro relativo punteggio di origine. Prima di immergerci nei dettagli di funzionalità dell'intero sistema, andremo a definire con chiarezza le responsabilità di ciascun componente della nostra rete.

3.2.1 Sentinel

Le Sentinel sono testimoni della posizione. Osservano le euristiche e ne garantiscono la certezza e l'accuratezza generando dei ledger (registri) temporali. L'aspetto più importante delle Sentinel è il fatto che producono dei ledger che altri componenti possono essere certi che provengano dalla medesima fonte. Fanno questo aggiungendo la Proof of Origin a una catena di trasmissione di prove crittografiche. Dato che XYO Network è un sistema trustless, le Sentinel devono essere incentivate a fornire informazioni di localizzazione veritiere.

1 Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counterparty, Monax e altri.

Questo è compiuto attraverso la combinazione di un elemento di reputazione con un elemento di pagamento. Una Sentinel è remunerata con Token XYO Network (XYO) quando le informazioni da lei raccolte sono impiegate per rispondere a una query. Per incrementare le probabilità di remunerazione, una Sentinel deve generare dei ledger coerenti con quelli delle altre Sentinel e fornire la Proof of Origin per identificarsi come la fonte dei dati di posizione.

3.2.2 Bridge

I Bridge trascrivono le informazioni di localizzazione, trasmettendo in sicurezza i ledger dalle Sentinel agli Archivist. L'aspetto più importante è che un Archivist può essere certo che i dati riportati sui ledger di euristica ricevuti da un Bridge non hanno subito alcuna alterazione. Un altro aspetto importante è il fatto che un Bridge fornisce un'ulteriore Proof of Origin. Dato che XYO Network è un sistema trustless, i Bridge devono essere incentivati a fornire una genuina trasmissione delle euristiche. Questo è compiuto attraverso la combinazione di un elemento di reputazione con un elemento di pagamento. Un Bridge è remunerato con Token XYO Network (XYO) quando le informazioni da lui trasmesse sono impiegate per rispondere a una query. Per incrementare le probabilità di remunerazione, una Sentinel deve generare dei ledger coerenti con quelli delle altre Sentinel e fornire la Proof of Origin per identificarsi come il trasmettitore dell'euristica.

3.2.3 Archivist

Gli Archivist salvano le informazioni di posizione trasmesse dai Bridge in una forma decentralizzata con l'obiettivo di mantenere registrato tutto lo storico dei ledger. Anche se qualche dato dovesse andare perso o diventare temporaneamente non disponibile, il sistema continuerebbe a funzionare, seppur con minore accuratezza. Gli Archivist si occupano anche di indicizzare i ledger, così che, quando necessario, possano restituire agilmente una stringa di dati. Si occupano di archiviare soltanto dati grezzi e ricevono in pagamento dei Token XYO Network esclusivamente per la consultazione e il successivo uso di tali informazioni. L'archiviazione è sempre gratuita.

Gli Archivist risultano collegati in una rete, quindi se uno di loro non contiene certi dati, effettuerà una richiesta agli altri Archivist. In forma opzionale, un Archivist può salvare ogni informazione del ledger che gli viene restituita. Questo porterà in maniera estremamente probabile ad avere due tipologie di Archivist: quelli che operano al bordo del "cloud" che si occupa della produzione dei dati e quelli che si concentrano più sul loro sfruttamento. Ci saranno poi gli Archivist in una posizione più centrale, che saranno ibridi. Salvare i dati non è obbligatorio, ma può essere fatto in modo semplice attraverso IPFS o un'altra soluzione di storage decentralizzato. Ogni dato temporale è passato da un Archivist all'altro, con l'aggiunta di una Proof of Origin al fine di tracciare il pagamento, dato che tutti gli Archivist vengono pagati. Per una consultazione, è possibile impostare un livello minimo di Proof of Origin per incrementare la validità. Per prevenire l'aumento sproporzionato dei dati, gli interessi di Sentinel, Bridge ed Archivist devono essere allineati.

3.2.4 Diviner

I Diviner rappresentano la parte più complessa di XYO Network. Il loro obiettivo generale è recuperare per una query i dati più accurati da XYO Network, per poi ritrasmetterli all'emittente di tale interrogazione. I Diviner condividono la piattaforma blockchain applicabile (per es. Ethereum, Stellar, Cardano, IOTA, ecc.) per le query emesse per lo smart contract XYO. Dopodiché, trovano la risposta interagendo direttamente con la rete di Archivist per identificare quella con il più alto punteggio di accuratezza/sicurezza. Questo lo fanno giudicando il testimone in base alla miglior catena di Proof of Origin. I Diviner che hanno recuperato la risposta dal punteggio migliore con un intervallo di tempo

minore avranno la capacit× di generare un blocco sulla blockchain XYO principale (XYOMainChain) tramite Proof of Work. L'ordine di priorit× delle query ß stabilito in base alla dimensione della ricompensa e alla complessit×, pertanto pið XYO saranno offerti per una risposta, maggiore sar× la priorit× della query.

Altri Diviner raggiungono il consenso sulla validit× di un blocco e lo firmano digitalmente. A quel punto, il Diviner che per quel blocco era l'indirizzo coinbase invier× allo smart contract una transazione contenente la risposta con il relativo punteggio di accuratezza. Al fine di prevenire un attacco che comporti l¸immissione di informazioni false all'interno della blockchain ad opera di soggetti fingano di essere Diviner, si invier× anche una lista delle firme degli altri Diviner. Lo smart contract potr× poi verificare l'integrit× delle informazioni controllando tale lista di firme.

3.3 End-to-End Functionality

Now that the responsibilities of each component are detailed, here is an end-to-end example of how the system will work:

1. **Sentinels Gather Data**
   - Sentinels gather real world location heuristics and prepare their own Proof of Origin to be chained to nodes above them
2. **Bridges Gather Data From Sentinels**
   - Bridges gather necessary data from online sentinels and append Proof of Origin to their chain. Bridges then make themselves available to Archivists in the Network.
3. **Archivists Index/Assemble Data from Bridges**
   - Bridges constantly send information to Archivists that are then kept on decentralized stores along with a location heuristic index.
4. **Diviner Fetches a User's Query**
   - Diviners poll for queries sent to the Ethereum smart contract and decide to begin the answer formulation process
5. **Diviner Collects Data From Archivists**
   - Diviners then decide to take on a query by fetching the appropriate information needed from the Archivist network.
6. **Diviner Formulates Answer**
   - Diviners choose the Best Answer to the query from the Archivist Network that contains the best Origin Chain Score.
7. **Diviner Proposes Block**
   - Diviners then propose blocks on the XYOMainChain containing the answer contents, the query, and the XYO Tokens (XYO) paid through Proof of Work. Other Diviners on the network digitally sign the block's content, then the coinbase Diviner's account nonce is updated to showcase its Proof of Work in the system once a consensus on a valid block is reached.
8. **Diviner Returns Result to Query Initiator**
   - Diviners package the answer, its Origin Chain Score, and its set of digital signatures and send them to an adapter component that securely connects to the XYO smart contract. The adapter is in charge of making sure the integrity of the Diviner has not been compromised and sends the set of digitally signed answers to the smart contract. This happens right after the block creation process. The coinbase Diviner is then paid for its efforts.

9. **XYO Network Components Get Rewarded for Their Work**

    - The components along the Proof of Origin Chain get paid for their involvement in fetching the answer to the query. Sentinels, Bridges, Archivists, and Diviners are all rewarded for their work.

In the case that the same query is asked more than once, more than one answer may be produced since the answer that is produced at a given moment is based on the available heuristics the system can offer at that time. Submitting an answer to the blockchain takes two steps. First, an analysis must be done to determine the Best Answer to a query. If multiple answers are generated by the system, then nodes will compare the answers and always choose the better answer. An example of a simple query would be: "*Where was a node on the network at a specific time in the past*"

3.4 Blockchain As a Single Source of Truth

At their core, Diviners simply transform relative data into absolute data. They are able to explore the entire Archivist network to concretize an absolute answer to a query on the XYO Network. Diviners are also the nodes that propose and add blocks to the XYOMainChain, and get rewarded for their Proof of Work. Because the Archivist network is a store of unprocessed data and the blockchain is a store of absolute, processed data, the network can eventually use the latest information on the XYOMainChain to answer future queries instead of relying on expensive computation through the Archivist Network.

Since blocks on the XYOMainChain store the Proof of Origin Chain and graph of components that were used to answer queries, future Diviners can explore this absolute data to achieve accurate results with lower bandwidth usage. As such, the XYOMainChain will gradually become the most important source of truth of the system. However, an Archivist network will still be required in order to maintain the most up-to-date information on location heuristics gathered by Sentinels.

3.5 XYO Network's Framework For Selecting The Best Answer Candidate

We define the *Best Answer* as the single answer, amongst a list of Answer Candidates, that returns the highest validity score and has a higher accuracy score than the minimum required accuracy. The validity score is based on the Origin Chain Score. The system knows what the highest record Origin Score is, which would be the 100 percent until a higher score is achieved, which then becomes the new 100 percent. The XYO Network allows selection of the Best Answer Algorithm for determining the Best Answer. This creates expansion for future research into alternative algorithms.

When data is excluded from an answer due to it being considered bad or incorrect, it will be circulated to archivists so that they can purge that data from their decentralized stores.

3.6 Initial Integration With Public Blockchains

The XYO Network is designed to be an abstraction that can interact with any smart contract capable, public blockchain such as Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano and others. To interact with the XYO Network, users on Ethereum, for instance, can issue

queries to our XYO smart contract and pay in XYO Tokens (ERC20). The nodes in our own XYO Blockchain, called Diviners, would constantly be polling Ethereum for these queries and be reward in the native currency of our own XYO Blockchain (also called XYO Tokens). In the future, we will do a one-to-one conversion from holders of our ERC20 token into our own blockchain's native currency in order to provide our platforms with transaction fees that support micropayment requirements necessary for scalable IoT use cases. In these cases, we will allow users to issue queries directly to our blockchain instead of interacting through a public smart contract.

---

4 Proof of Origin

With a physical network comprised of untrusted nodes it is possible to determine the certainty of data that has been provided by edge nodes based on a zero-knowledge proof that two or more pieces of data originated from the same source. Using these data sets, combined with a number of similar data sets and the knowledge of at least one node's absolute location, the absolute location of the other node can be ascertained.

4.1 Proof of Origin Introduction

Traditional trustless systems rely on a private key for signing transactions or contracts in a system. This works very well with the assumption that the node on the network that signs the data in question is physically and virtually secure. However, if the private key is compromised, then the ability to prove origin falters.

When applying trustless concepts to the Internet of Things, it must be assumed that edge nodes on the network are not physically or virtually secure. This brings forth the need to identify edge nodes without the use of unique IDs and to instead judge the data produced by them as being honest and valid without any knowledge from outside the network.

4.2 The Core of Proof of Origin: Bound Witnesses

Proof of Origin relies on the concept of a *Bound Witness*. Given that an untrusted source of data used to resolve a digital contract (an oracle) is not useful, we can substantially increase the certainty of the data provided by first establishing the existence of a bidirectional proof of location. The primary bidirectional location heuristic is proximity, since both parties can validate the occurrence and range of an interaction by cosigning the interaction. This allows for a zero-knowledge proof that the two nodes were in proximity of each other.

We then need to determine the certainty that an oracle witness node in a trustless system gathered the data that it is sharing. In a trustless system, a witness node can either by defect or corruption produce false data. Invalid data can be detected and removed simply if it falls outside the allowed range for that heuristic. Valid but incorrect data (i.e. false data) is much more difficult to detect.

4.3 Unidirectional vs. Bidirectional Location Heuristics

Most data related to the physical world (a heuristic) is unidirectional. This means that the element being measured cannot measure back, making unidirectional heuristic data very

difficult to validate. A bidirectional heuristic is one where the measured element can report its own measurement back to the other party, which makes validation possible. Location is a rare heuristic in that it can be bidirectional, with two edge nodes reporting on each other. **A real-world example of this would be two people who are near each other taking a selfie, printing a copy for each party, and then both signing the selfie. This process would give both parties Proof of Proximity. The only way for these two people to have gotten this "data" would be from them having been together in the same location.**

Next, let us discuss network effects: Imagine a system where every edge node is expected to constantly produce these "selfies" as they travel around, and store them in a binder. They are also expected to keep that binder in time-sequential order and are never allowed to delete one. This establishes a proximity recorder for each edge node that can be cross referenced with the recorders of the other edge nodes.

4.4 Non-Edge Nodes

All nodes are considered "witnesses," including bridge, relay, storage, and analysis nodes. This allows for any data that is relayed from one node to the next to be bound. This is the concept of the **Bound Witness**.

4.5 Cross Reference

Analyzing every set of "selfies" that is produced and chained together by every edge node allows the system to produce the Best Answer from the relative proximity of all the nodes that are in the network. If every node reports honestly and accurately, the mapping of all the relative positions of the edge nodes will achieve the maximum certainty and accuracy possible: 100 percent. Conversely, if every node is either dishonest or flawed, the certainty and accuracy both can approach the minimum of 0 percent.

Given a set of reported data and a query for a relative position of one of the edge nodes, an approximation of the position can be generated along with coefficients for certainty and accuracy.

Given the same set of data and the same analysis algorithm, every calculation should arrive at the same position approximation and the same coefficients for certainty and accuracy.

4.6 Diagram

S' and *S"* (Figure 1.) are each a Sentinel (edge node) that collect heuristics. When in contact with each other, they exchange heuristic data and public keys. Both build a full record of the interaction and sign the resulting interaction. That signed record then becomes the next entry in both of their local ledgers (`16` for *S'* and `3` for *S"*). This action binds these two witnesses as being within proximity of each other.

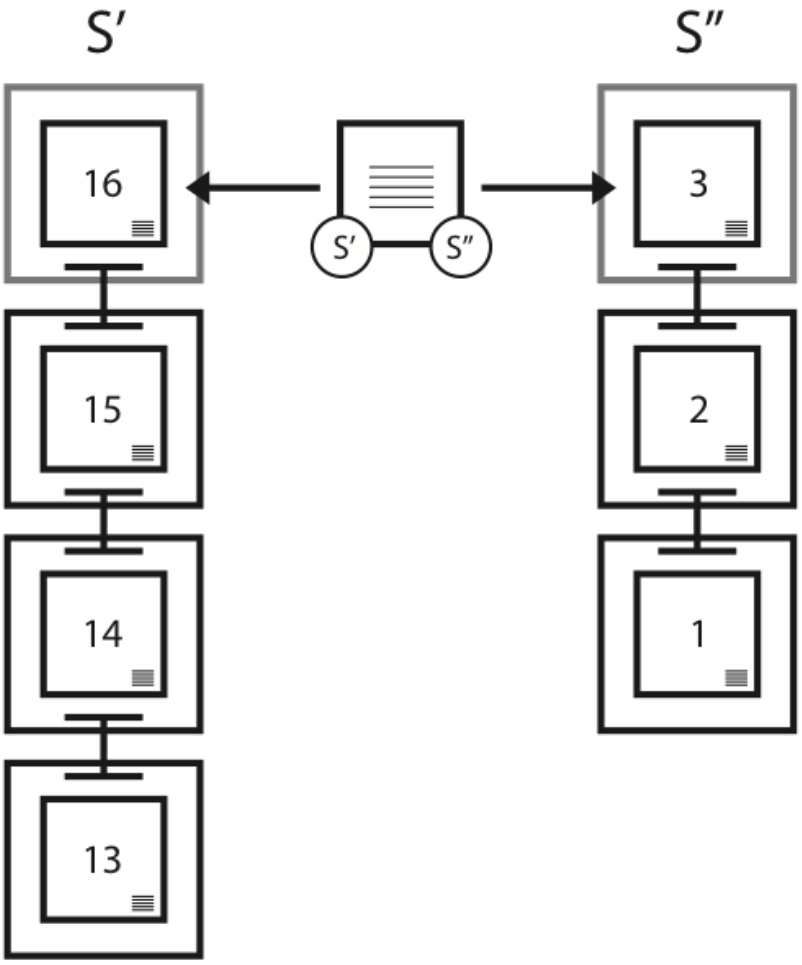

Figure 1. Witness Binding Example Between Two Sentinels

4.7 Origin Chains

Each origin maintains its own ledger and signs it to make a Proof of Origin Chain. Once information on the Proof of Origin Chain has been shared, it is effectively permanent. This is because the fork that happens after the share ends the chain and makes all future data from the witness to be treated as if it were from a new witness. To generate a link in a Proof of Origin Chain, the origin generates a public/private key pair. It then signs both the previous and next blocks with the same pair after including the public key in both blocks. Immediately after the signature is made, the private key is deleted. With the immediate deletion of the private key, the risk of a key being stolen or reused is greatly minimized.

Proof of Origin Chains are 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 ability for a bad actor to steal a private key is too feasible. To solve this, XYO Network utilizes Transient Key Chains. The benefit of their usage 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.

Every time a heuristic ledger is handed off in XYO Network, the receiver appends their own Proof of Origin, which makes the Proof of Origin Chain longer and generates a Proof of Origin Intersection. Proof of Origin Chains and Proof of Origin Intersections are the primary indicators used by Diviners to verify validity of ledgers. The equation for a Ledger Reputation is effectively what percent of the XYO Network was involved in making the Proof of Origin Ball associated with it. In theory, if 100 percent of the XYO Network records are linked with Proof of Origin and then fully analyzed, the odds of it being valid is 100 percent. If 0 percent of XYO Network records are available for analysis, then validity drops to 0 percent.

For added security, the public key for a Chain Link is not provided until the second entry for it is made available. This also allows for the time interval between entries or other data to be stored in the previous or next link.

4.8 Origin Chain Score

Origin Chain Score is calculated as follows (default algorithm):

- PcL = Proof of Origin Chain Length
- PcD = Proof of Origin Chain Difficulty
- Pc' Pc'' O = Proof of Origin Chain Overlap for Pc' and Pc''

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O} \tag{1}$$

4.9 Origin Tree

An Origin Tree is used to calculate the approximate validity of an answer. It uses the data gathered to generate an Ideal Tree, which is the tree that best fits that data for a given asserted answer. If node N is located at X,Y,Z,T location, the error across all the data in the set must hold a certain value. To compute this error, we would calculate the MIN, MAX, MEAN, MEDIAN, and AVERAGE DISTANCE FROM THE MEAN.

Given a set S of all scores s, a Proof of Origin Chain Difficulty PcD, and an error factor $error$, the Best Answer determined as follows:

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)] \tag{2}$$

In other words, the asserted answer that has the highest Best Answer Score is the Best Answer. Using the Proof of Origin Tree, we can identify and prune impossible branches (outliers).

4.10 Transient Key Chaining

A series of data packets can be chained together by using temporary private keys to sign two successive packets. When the public key paired with the private key is included in the data packets, the receiver can verify that both packets were signed by the same private key. The data in the packet cannot be altered without breaking the signature, assuring that the signed packets were not altered by a third party, such as a Bridge or storage node.

4.11 Link Depth

At a minimum, a node generates a new public/private key pair for every link in the Proof of Origin Chain, which has a Link Depth of `1`. There may be `N` entries in the link table for a given *Ledger Entry*, with each entry specifying the distance in the future when part two of the link will be added. No two links may have the same order of magnitude on a base 2 scale. For example, the entry `[1,3,7,12,39]` would be allowed, but `[1,3,7,12,15]` would not.

The depth `1` link is created, used and deleted when the previous block is published. However, links of depth greater than `1` have their pair generated as the previous block is being signed, and the second signing does not happen until `N` blocks later, after which the private key is deleted. For this reason, links of depth greater than 1 are always considered to be less secure than links of depth `1`, but they can be used to improve performance and reduce data loss at the cost of that security.

4.12 Fixed Order

The key element in determining the sequence of ledgers is the order in which they were reported. Given that it is not possible for a device to change the order of any Proof of Origin signed ledger, an absolute order can be established by looking at all the ledgers collectively.

4.13 Second-to-Last Publishing

A primary method for establishing Proof of Origin is based on the fact that a Sentinel always reports its second to last block without reporting the last block. This allows the last block to have the signed link to its predecessor as evidence of the link.

4.14 Empty Links

To make a Proof of Origin Chain more secure, it is required that the chain is updated no more than once every ten seconds and no less than once every sixty minutes. In the case that no new data is available, an empty block will be added to the chain.

4.15 Diagram

As time travels from left to right (Figure 2.), the Proof of Origin Chain that is being built gets longer. At any given time, the producer of the chain will only provide to the caller the entries with darkened borders, waiting for the second signing of the entry before making it available. For example, in the 3rd column, only entries `2` and `1` will be returned as being part of the chain.

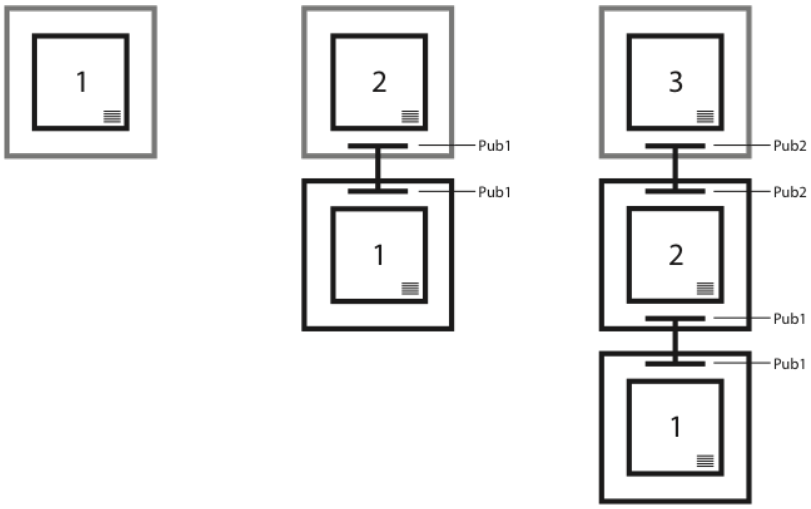

Figure 2. Link inclusion example in a Proof of Origin Chain

4.16 Summary

Given a series of data packets that are signed in sequential pairs with temporary private keys and include the paired public keys, it can be determined with absolute certainty that the packets came from the same origin.

---

5 Security Considerations

5.1 Fake Diviner Attack

A set of digital signatures are sent to the XYO smart contract because the contract needs to verify the integrity of the Diviner that sent the answer. The contract can then verify the other Diviners that signed this list within a high confidence interval. Without this, the relaying oracle would be the single source of failure and risk within the system.

5.2 Sentinel DDoS Attacks

Another attack to consider is a Distributed Denial of Service (DDoS) among Sentinel nodes in a particular region. An attacker could attempt to establish a large number of connections

to Sentinels in order to prevent them from relaying the correct information or relaying any information at all to the Bridges. We can circumvent this problem by requiring a small cryptographic puzzle to be solved by anyone attempting to connect to a Sentinel. Since a query won't involve a very large number of connections to Sentinels, this will not impose a heavy bearing on the XYO relay system, and will require an attacker to spend a large amount of resources to execute a successful DDoS our network. At any given point in time, an Proof of Origin Chain can be verified by anyone as it is stored on the XYOMainChain. This ensures that if a single entity along the chain was compromised, the accuracy of the query's answer (Origin Chain Score) will drop to 0.

---

6 XYO Token Economy

Oracles stand as a significant portion of the power and infrastructure needs for decentralized applications, with most of the focus revolving around the connectivity and aggregation of authoritative oracles. We believe that the need for a fully decentralized and trustless system of oracles is needed for decentralized applications to reach their maximum potential.

6.1 XYO Network Cryptoeconomics

We use XYO Tokens to incentivize the desired behavior of providing accurate, reliable location heuristics. XYO Tokens can be thought of as "gas" needed to interface with the real world in order to verify the XY-coordinate of a specified object.

The process works like this: A token holder first queries the XYO Network with a query (e.g. *"Where is my eCommerce order package with XYO Address* `0x123456789...`"). The query then gets sent into a queue, where it waits to be processed and answered. A user can set their desired confidence level and XYO gas price at query creation. The cost of a query (in XYO Tokens) is determined by the amount of data required to provide an answer to the query as well as market dynamics. The more data needed, the more expensive the query and higher the XYO gas price. Queries to the XYO Network have the potential to be very large and expensive. For instance, a trucking and logistics company could query the XYO Network to ask, "*What is the location of every single car in our fleet?*"

Once the XYO Token holder queries the XYO Network and pays the requested gas, all Diviners working on the task call out to the relevant Archivists to retrieve the pertinent data needed to answer the query. The data returned is derived from the Bridges, who originally gathered the data from the Sentinels. Sentinels are essentially the devices or signals that verify the location of objects. These include entities such as Bluetooth trackers, GPS trackers, geo-location tracking built into IoT devices, satellite tracking technology, QR-code scanners, RFID scanning and many others. XY Findables has pioneered and launched its consumer Bluetooth and GPS business, which has allowed it to test and process real-world location heuristic. All efforts in developing the XY Findables consumer business have served to help significantly in designing the XYO Network Blockchain Protocol.

If the data provided by a Sentinel device (such as a Bluetooth Beacon) is used to answer a query, then all four components involved in the transaction receive a portion of the XYO gas paid by the token holder: the Diviner (who searched for the answer), the Archiver (who stored the data), the Bridge (who transmitted the data) and the Sentinel (who recorded the location data). The distribution of the gas between 3 of the 4 components of the

XYO Network is always given in the same proportion. The exception is that of Diviners, whose involvement in the process of providing an answer is more extensive. Within each component, gas gets distributed evenly.

6.2 Rewards for Independence

Location-gathering devices are the atomic blocks of the network, and a single device may act as one or more of the four components of the system. However, it would be rare, especially in a large XYO Network, that devices would be more than two of these components. Furthermore, a blockchain ledger that has more independent Proof of Origin will hold higher regard, so there is a cryptoeconomic penalty for a device acting as multiple components.

6.3 Rewards for Stationarity Integrity

Sentinels in the XYO Network are assigned a stationarity coefficient for their quantity of movement throughout their lifecycle. The less a Sentinel moves in a period of time, the more its data can be trusted. Archivists keep track and analyze these stationarity coefficients when considering which Sentinels to route queries to.

6.4 Incentivizing Token Usage

A system in which token holders are encouraged *not* to use their tokens creates a long-term problem for the underlying economy. It creates an ecosystem with very scarce stores of value and triggers a natural impulse to invent reasons for *not* using the token, instead of boosting utility and liquidity.

The problem most cryptoeconomic incentives have is that the focus is placed too strongly on the token miners (e.g. Sentinels, Bridges, Archivists, Diviners), and not at all on the token users. The XYO Token takes both into account.

The XYO Token model incentivizes the miner to not just provide accurate data, but to also know when to not provide data at all. The end user is rewarded to transact more when network liquidity is low, compared to when network liquidity is high. Thus the ecosystem of the XYO Token has the ability to remain well-balanced, fluid and robust.

6.5 XYO Token Specifications

The public token sale has a tiered pricing structure that starts at 1 ETH: 100,000 XYO and maxes out at 1 ETH: 33,333 XYO. Details regarding our volume and time based pricing structure will be announced soon.

- Smart contract platform: Ethereum
- Contract Type: ERC20
- Token: XYO
- Token Name: XYO Network Utility Token
- Token Address: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Total issuance: Finite and capped at the amount reached after the Token Main Sale

- Amount issued during the main sale: Unlimited
- Unsold and Unallocated tokens: Burned after the token sale event. No further XYO tokens will be generated after the Main Sale ends.

---

7 XYO Network Use Cases

The XYO Network's usage has vast applications that span a multitude of industries. Take for example an eCommerce Company that could offer its premium customers payment-upon-delivery services. To be able to offer this service, the eCommerce company would leverage the XYO Network (which uses XYO Tokens) to write a smart contract (i.e. on Ethereum's platform). The XYO Network could then track the location of the package being sent to the consumer along every single step of fulfillment; from the warehouse shelf to the shipping courier, all the way into the consumer's house and every location in between. This could enable eCommerce retailers and websites to verify, in a trustless way, that the package not only appeared on the customer's doorstep, but also safely inside their home. Once the package has arrived in the customer's home (defined and verified by a specific XY-Coordinate), the shipment is considered complete and the payment to the vendor gets released. The eCommerce integration of the XYO Network thusly enables the ability to protect the merchant from fraud and ensure consumers only pay for goods that arrive in their home.

Consider an entirely different integration of the XYO Network with a hotel review site, whose current problem is that their reviews are often not trusted. Naturally, hotel owners are incentivized to improve their reviews at any cost. What if one could say with extremely high certainty that someone was in San Diego, flew to a hotel in Bali and stayed there for two weeks, returned to San Diego, and then wrote a review about their hotel stay in Bali? The review would have a very high reputation, especially if it was written by a serial reviewer who has written many reviews with verified location data.

---

8 XYO Network Expansion

We are fortunate to have a consumer business that has successfully built a real-world network with over one million (1,000,000) Bluetooth and GPS devices in the world. Most location networks fail to reach this phase and attain the critical mass necessary to build out an extensive network. The Sentinel network we have created is only the starting point. The XYO Network is an open system that any operator of location devices can plug into and begin earning XYO Tokens.

Generally, the greater the Sentinel cardinality in the XYO Network, the more reliable the it is. To further grow its network, the XYO Network is engaging with other businesses to expand its network of Sentinels beyond its own network of XY Findables beacons.

9 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: Raul Jordan (Harvard College, Thiel Fellow and XYO Network Advisor); for his contributions in making our white paper more concise and helping us elegantly communicate its technical details to the world. 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

[1] Blanchard, Walter. *Hyperbolic Airborne Radio Navigation Aids*. Journal of Navigation, 44(3), September 1991.

[2] Karapetsas, Lefteris. *Sikorka.io*. `http://sikorka.io/files/devcon2.pdf`. Shanghai, September 29, 2016.

[3] Di Ferrante, Matt. *Proof of Location*. `https://www.reddit.com/r/ethereum/comments/539o9c/proof_of_location/`. September 17, 2016.

[4] Goward, Dana. *RNT Foundation Testifies Before Congress*. US House of Representatives Hearing: "Finding Your Way: The Future of Federal Aids to Navigation," Washington, DC, February 4, 2014.

Glossary

accuracy A measure of confidence that a data point or heuristic is within a specific margin of error. 1, 2, 4, 5, 7, 9

Archivist An Archivist stores heuristics as a part of the decentralized data set with the goal of having all historical ledgers stored, but without that requirement. Even if some data is lost or becomes temporarily unavailable, the system continues to function, just with reduced accuracy. Archivists also index ledgers so that they can return a string of ledger data if needed. Archivists store raw data only and get paid solely for retrieval of the data. Storage is always free. 4, 5, 7, 14, 15

Best Answer We define the Best Answer as the single answer, amongst a list of Answer Candidates, that returns the highest validity score and has a higher accuracy score than the minimum required accuracy.. 6, 7, 9, 11

Best Answer Algorithm An algorithm used to generate Best Answer Scores when a Diviner chooses an answer. The XYO Network permits the addition of specialized algorithms and allows the customer to specify which algorithm to use. It is required that this algorithm will result in the same score when run on any Diviner given the same data set. 7

Bound Witness Bound Witness is a concept achieved by the existence of a bidirectional heuristic. Given that an untrusted source of data for the use of digital contract resolution (an oracle) is not useful, there is a substantial increase in certainty of the data provided by the establishment of such a heuristic. The primary bidirectional heuristic is proximity since both parties can validate the occurrence and range of an interaction by cosigning the interaction. This allows for a zero-knowledge proof that the two nodes were in proximity of each other.. 1, 8, 9

Bridge A Bridge is a heuristic transcriber. It securely relays heuristic ledgers from Sentinels to Diviners. The most important aspect of a Bridge is that a Diviner can be sure that the heuristic ledgers that are received from a Bridge have not been altered in any way. The second most important aspect of a Bridge is that they add an additional Proof of Origin metadata. 4, 5, 12, 14, 15

certainty A measure of the likelihood that a data point or heuristic is free from corruption or tampering. 1–4, 8, 9, 13, 16

crypto-location The realm of cryptographic location technology. 3

cryptoeconomics A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols. 15

Diviner A Diviner answers a given query by analyzing historical data that has been stored by the XYO Network. Heuristics stored in the XYO Network must have a high level of Proof of Origin to determine the validity and accuracy of the heuristic. A Diviner obtains and delivers an answer by judging the witness based on its Proof of Origin.

Given that the XYO Network is a trustless system, Diviners must be incentivized to provide honest analyses of heuristics. Unlike Sentinels and Bridges, Diviners use Proof of Work to add answers to the blockchain. 4, 5, 7, 8, 11, 13–15

heuristic A data point about the real world relative to the position of a Sentinel (proximity, temperature, light, motion, etc...). 4, 5, 7–9, 11, 14

oracle A part of a DApp (decentralized application) system that is responsible for resolving a digital contract by providing an answer with accuracy and certainty. The term "oracle" originates from cryptography where it signifies a truly random source (e.g. of a random number). This provides the necessary gate from a crypto equation to the world beyond. Oracles feed smart contracts information from beyond the chain (the real world, or off-chain). Oracles are interfaces from the digital world to the real world. As a morbid example, consider a contract for a Last Will & Testament. A Will's terms are executed upon confirmation that the testator is deceased. An oracle service could be built to trigger a Will by compiling and aggregating relevant data from official sources. The oracle could then be used as a feed or end-point for a smart contract to call out to in order to check whether or not the person is deceased. 1, 3, 4, 8, 14

Origin Chain Score The score assigned to an Origin Chain to determine its credibility. This assessment takes length, tangle, overlap, and redundancy into consideration. 4, 6, 7, 11, 14

Origin Tree A data set of ledger entries taken from various Origin Chains to establish the origin of a heuristic ledger entry with a specified level of certainty. 11

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

Proof of Origin Chain A Transient Key Chain that links together a series of Bound Witness heuristic ledger entries. 4, 7, 10–12, 14

Proof of Work Proof of Work is a piece of data that satisfies certain requirements, is difficult to produce (i.e. costly, time-consuming), but easy for others to verify. Producing a Proof of Work can be a random process with a low probability of generation so that rigorous trial and error is required on average before a valid Proof of Work is created. 5–7

Sentinel A Sentinel is a heuristic witnesses. It observes heuristics and vouches for the certainty and accuracy of them by producing temporal ledgers. The most important aspect of a Sentinel is that it produces ledgers that Diviners can be certain came from the same source by adding Proof of Origin to them. 3–5, 7, 9, 12–16

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. 1–5, 7, 13, 16

Transient Key Chain A Transient Key Chain links a series of data packets using Transient Key Cryptography. 11

trustless A characteristic where all parties in a system can reach a consensus on what the canonical truth is. Power and trust is distributed (or shared) among the network's stakeholders (e.g. developers, miners, and consumers), rather than concentrated in a single individual or entity (e.g. banks, governments, and financial institutions). This is a common term that can be easily misunderstood. Blockchains don't actually eliminate trust. What they do is minimize the amount of trust required from any single actor in the system. They do this by distributing trust among different actors in the system via an economic game that incentivizes actors to cooperate with the rules defined by the protocol. 1, 3–5, 8, 14, 16

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 geolocation confirmations. 2–5, 7, 11, 14–17

XYOMainChain An immutable blockchain in the XYO Network that stores query transactions along with data gathered from Diviners and their associated origin score. 4–7, 14