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 fanno affidamento sulla localizzazione, la nostra privacy e sicurezza dipendono fortemente dall'accuratezza e dalla validità dei dati di posizione. Si sono compiuti diversi sforzi per eliminare il 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 la conclusione di un contratto. Per definire l'esito 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 subiscono 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 con l'obiettivo 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 la nostra impresa che vende 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 elaborata 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 gli uni 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 di 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 procedure di fallback 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. Otteniamo questo 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 oracle). 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 trasmissione veritiera 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, un Bridge deve generare dei ledger coerenti con quelli degli altri Bridge 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 all'edge 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. Fanno questo 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 capacità di generare un blocco sulla blockchain XYO principale (XYOMainChain) tramite Proof of Work. L'ordine di priorità delle query è stabilito in base alla dimensione della ricompensa e alla complessità, pertanto più XYO saranno offerti per una risposta, maggiore sarà la priorità della query.

Altri Diviner raggiungono il consenso sulla validità di un blocco e lo firmano digitalmente. A quel punto, il Diviner che per quel blocco era l'indirizzo coinbase invierà 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 che fingano di essere Diviner, si invierà anche una lista delle firme degli altri Diviner. Lo smart contract potrà poi verificare l'integrità delle informazioni controllando tale lista di firme.

3.3 Funzionalità End-to-End

Ora che sono state esposte in dettaglio le responsabilità di ciascun componente, ecco un esempio end-to-end di come funzionerà il sistema:

1. **Le Sentinel raccolgono i dati.**
   - Le Sentinel raccolgono euristiche di localizzazione nel mondo reale e preparano la propria Proof of Origin da incatenare ai nodi successivi.
2. **I Bridge riuniscono i dati raccolti dalle Sentinel.**
   - I Bridge raggruppano i dati necessari dalle Sentinel online e aggiungono la Proof of Origin alla loro catena. Dopodiché, si rendono disponibili agli Archivist all'interno del Network.
3. **Gli Archivist indicizzano/assemblano i dati trasmessi dai Bridge.**
   - I Bridge inviano costantemente agli Archivist informazioni che sono poi mantenute in archivi centralizzati insieme a un indice delle euristiche di posizione.
4. **I Diviner recuperano una query degli utenti.**
   - I Diviner selezionano fra le query inviate allo smart contract Ethereum e decidono di avviare il processo di formulazione della risposta.
5. **I Diviner raccolgono i dati dagli Archivist.**
   - I Diviner decidono poi di occuparsi di una query prendendo le informazioni idonee necessarie presso la rete degli Archivist.
6. **Il Diviner formula la risposta.**
   - I Diviner selezionano la Best Answer per la query dalla rete di Archivist che contiene l'Origin Chain Score migliore.
7. **Il Diviner propone il blocco.**
   - I Diviner propongono poi i blocchi per la XYOMainChain, che includeranno i contenuti della risposta, la query e i Token XYO (XYO) pagati tramite Proof of Work. Gli altri Diviner sulla rete firmeranno digitalmente il contenuto del blocco e, una volta raggiunto il consenso sulla validità di un blocco, il nonce dell'account del Diviner coinbase sarà aggiornato per mostrare la sua Proof of Work.

8. **Il Diviner restituisce il risultato al promotore della query.**

   • I Diviner impacchettano la risposta, il suo Origin Chain Score e il suo insieme di firme digitali, dopodiché inviano il tutto a un componente adattatore collegato in forma sicura allo smart contract XYO. Tale adattatore si occupa di accertare che l'integrità del Diviner non sia stata compromessa, quindi invia l'insieme di risposte firmate digitalmente allo smart contract. Ciò avviene subito dopo il processo di creazione del blocco. A questo punto, il Diviner coinbase viene remunerato per i suoi sforzi.

9. **I componenti di XYO Network ricevono la remunerazione per il loro lavoro.**

   • I componenti lungo la Proof of Origin Chain ricevono il pagamento per il loro coinvolgimento nella ricerca della risposta alla query. Che si tratti di Sentinel, Bridge, Archivist o Diviner, tutti sono remunerati per il loro lavoro.

Nel caso in cui la stessa query si proponesse più di una volta, sarebbe possibile produrre più di una risposta, dato che una risposta generata in un dato momento risulterà basata sulle euristiche disponibili nel sistema a quel tempo. L'inoltro di una risposta alla blockchain consta di due fasi: prima di tutto, deve essere condotta un'analisi per determinare la Best Answer a una query. Poi, se il sistema genera risposte multiple, allora i nodi le confronteranno per scegliere sempre la risposta migliore. Un esempio di una semplice query potrebbe essere: "*Dov'era un nodo sulla rete in uno specifico momento passato?*"

3.4 Blockchain come singola fonte di verità

Fondamentalmente, i Diviner trasformano dati relativi in dati assoluti. Sono in grado di esplorare l'intera rete di Archivist per generare una risposta assoluta a una query su XYO Network. I Diviner costituiscono anche i nodi che propongono e aggiungono blocchi alla XYOMainChain, ottenendo una remunerazione per la loro Proof of Work. Poiché la rete di Archivist è un archivio di dati non processati mentre la blockchain è un archivio di dati elaborati ed assoluti, per rispondere a query future la rete potrà utilizzare le ultime informazioni riportate sulla XYOMainChain, invece che basarsi su dispendiosi calcoli tramite il Network di Archivist.

Siccome i blocchi sulla XYOMainChain archiviano la Proof of Origin Chain e il diagramma dei componenti utilizzati per rispondere alle query, i Diviner futuri potranno esplorare questi dati assoluti per ottenere risultati accurati con un utilizzo di banda minore. Di conseguenza, la XYOMainChain diventerà gradualmente la fonte più importante di verità del sistema. Tuttavia, si renderà sempre necessaria una rete di Archivist che mantengano quanto più aggiornate le informazioni sulle euristiche di localizzazione raccolte dalle Sentinel.

3.5 La struttura di XYO Network per la selezione della possibile Best Answer

Definiamo come Best Answer all'interno di una lista di Answer Candidates quella singola risposta che restituisce il punteggio di validità maggiore e possiede un punteggio di accuratezza superiore al valore minimo necessario. Il punteggio di validità è basato sull'Origin Chain Score. Il sistema conosce qual è il valore più alto di tale punteggio, che costituirebbe il 100% fino al raggiungimento di un punteggio più alto, il quale diventa poi a sua volta il nuovo 100%. Per determinare la Best Answer, XYO Network permette di selezionare il Best Answer Algorithm. Questo apre lo spazio per una futura attività di ricerca su algoritmi alternativi.

Qualora dei dati siano esclusi da una risposta poiché considerati scorretti o invalidi, questi saranno girati agli Archivist in modo che possano eliminarli dai loro archivi decentralizzati.

3.6 Integrazione iniziale con blockchain pubbliche

XYO Network è progettato per costituire un'astrazione in grado di interagire con qualsiasi blockchain pubblica abilitata agli smart contract, come Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano e altre. Per esempio, per interagire con XYO Network, gli utenti su Ethereum possono inoltrare delle query al nostro smart contract XYO e pagare in Token XYO (ERC20). I nodi all'interno della nostra XYO Blockchain, i Diviner, sonderebbero costantemente Ethereum per tali query ricevendo la ricompensa nella valuta nativa della nostra XYO Blockchain (i cosiddetti Token XYO). In futuro, al fine di integrare nelle nostre piattaforme delle commissioni di transazione che supportino i requisiti di micropagamento necessari per casi d'uso scalabili nell'ambito IoT, effettueremo una conversione alla pari fra il nostro token ERC20 e la valuta nativa della nostra blockchain. In tali casi, permetteremo agli utenti di generare delle query dirette alla nostra blockchain, invece di interagire attraverso uno smart contract pubblico.

---

4 Proof of Origin

Con una rete fisica costituita da nodi untrusted risulta possibile determinare la certezza dei dati forniti dai nodi edge basati sulla base di una dimostrazione a conoscenza zero riguardante il fatto che due o più dati siano stati originati dalla medesima fonte. Usando tali insiemi di dati, combinati con vari dataset simili e la conoscenza della posizione assoluta di almeno un nodo, è possibile determinare la localizzazione assoluta dell'altro nodo.

4.1 Introduzione della Proof of Origin

I sistemi trustless tradizionali si affidano a una chiave privata per validare transazioni o contratti in un sistema. Questa procedura funziona davvero bene fintanto che resta valida l'ipotesi secondo cui il nodo sulla rete che firma i dati in questione è sicuro sia a livello fisico che virtuale. Se, tuttavia, la chiave privata risulta compromessa, decresce la capacità di provare l'origine.

Quando si applicano i concetti trustless all'Internet of Things, bisogna assumere che in nodi edge sulla rete non sono fisicamente o virtualmente sicuri. Questo fa emergere la necessità di identificare nodi edge senza il ricorso a ID univoci, giudicando invece dati da loro prodotti come se fossero genuini e validi senza alcuna conoscenza esterna alla rete.

4.2 Il nucleo della Proof of Origin: il Bound Witness

La Proof of Origin si basa sull'idea di un Bound Witness. Dato che una fonte di dati untrusted non è utile alla risoluzione di un contratto digitale (un oracle), possiamo incrementare in modo sostanziale la certezza dei dati forniti dimostrando prima di tutto l'esistenza di una Proof of Location bidirezionale. La principale euristica di localizzazione bidirezionale è la prossimità, dato che entrambe le parti possono validare l'occorrenza e l'intervallo di un'interazione firmandola congiuntamente. Questo permette di compiere una dimostrazione a conoscenza zero del fatto che i due nodi fossero in prossimità l'uno all'altro.

Abbiamo poi la necessità di determinare la certezza con cui un nodo testimone di un oracle in un sistema trustless ha raccolto i dati che sta condividendo. In un sistema trustless, un nodo testimone può generare dati falsi per difetto o corruzione.

I dati non validi possono essere rilevati e rimossi in modo semplice, se ricadono all'esterno dell'intervallo concesso per quell'euristica. I dati validi ma scorretti (es. dati falsi) sono molto più difficili da individuare.

4.3 Euristiche di localizzazione unidirezionali vs. bidirezionali

La maggior parte dei dati relativi al mondo fisico (una euristica) è unidirezionale. Questo significa che l'elemento che viene misurato non può a sua volta misurare, quindi i dati di una euristica unidirezionale sono veramente difficili da validare. Abbiamo invece un'euristica bidirezionale quando l'elemento misurato può riferire all'altra parte la propria misurazione, rendendo quindi possibile la validazione. La localizzazione è un'euristica rara in quanto può essere bidirezionale, con due nodi edge che riferiscono l'uno all'altro. **Un esempio di questo nel mondo reale potrebbe essere quello di due persone vicine che si fanno un selfie, ne stampano una copia per ognuno e poi entrambi le firmano. Questo processo darebbe a entrambe le parti una Proof of Proximity. L'unico modo in cui queste due persone abbiano potuto ottenere questo "dato" sarebbe il fatto di essersi trovate insieme nella stessa ubicazione.**

Andiamo quindi a discutere degli effetti di rete: immaginiamo un sistema in cui si prevede che durante i suoi movimenti ogni nodo edge vada a produrre costantemente questi "selfie", archiviandoli in un raccoglitore. Si prevede anche che si occupino di mantenere tale raccoglitore secondo l'ordine cronologico e che non sia mai permesso loro di cancellarne uno. Questo genera per ogni nodo edge un registratore di prossimità che può essere incrociato con i registratori degli altri nodi edge.

4.4 Nodi non-edge

Tutti i nodi sono considerati dei "*witness*", testimoni, inclusi i nodi bridge, di trasmissione, di archiviazione e di analisi. In questo modo tutti i dati trasmessi da un nodo all'altro possono essere legati. È questo il concetto di **Bound Witness** (letteralmente, testimone legato).

4.5 Riferimento incrociato

L'analisi di ogni set di "selfie" prodotto e concatenato da ciascun nodo edge permette al sistema di generare la Best Answer dalla prossimità relativa di tutti i nodi presenti nella rete. Se ogni nodo riferisce in maniera onesta ed accurata, la mappatura di tutte le posizioni relative dei nodi edge raggiungerà la massima certezza ed accuratezza possibili: il 100%. Nel caso opposto, se ogni nodo è disonesto o viziato, sia la certezza che l'accuratezza possono raggiungere il valore minimo di 0%.

Dato un insieme di dati comunicati e una query per una posizione relativa di uno dei nodi edge, è possibile generare un'approssimazione della posizione con i relativi coefficienti di certezza ed accuratezza.

Considerando il medesimo set di dati e lo stesso algoritmo di analisi, ogni calcolo dovrebbe portare alla stessa approssimazione di posizione nonché agli stessi coefficienti di certezza ed accuratezza.

4.6 Diagramma

S' e S" (Figura 1) sono entrambi Sentinel (nodi edge) che raccolgono euristiche. Quando si contattano l'un l'altro, si scambiano dati euristici e chiavi pubbliche. Entrambi generano una registrazione completa dell'interazione e firmano l'interazione risultante. Quella registrazione firmata diventa poi la voce successiva in entrambi i loro ledger locali (`16` per *S'* e `3` per *S"*). Questa azione lega questi due testimoni come in prossimità l'uno all'altro.

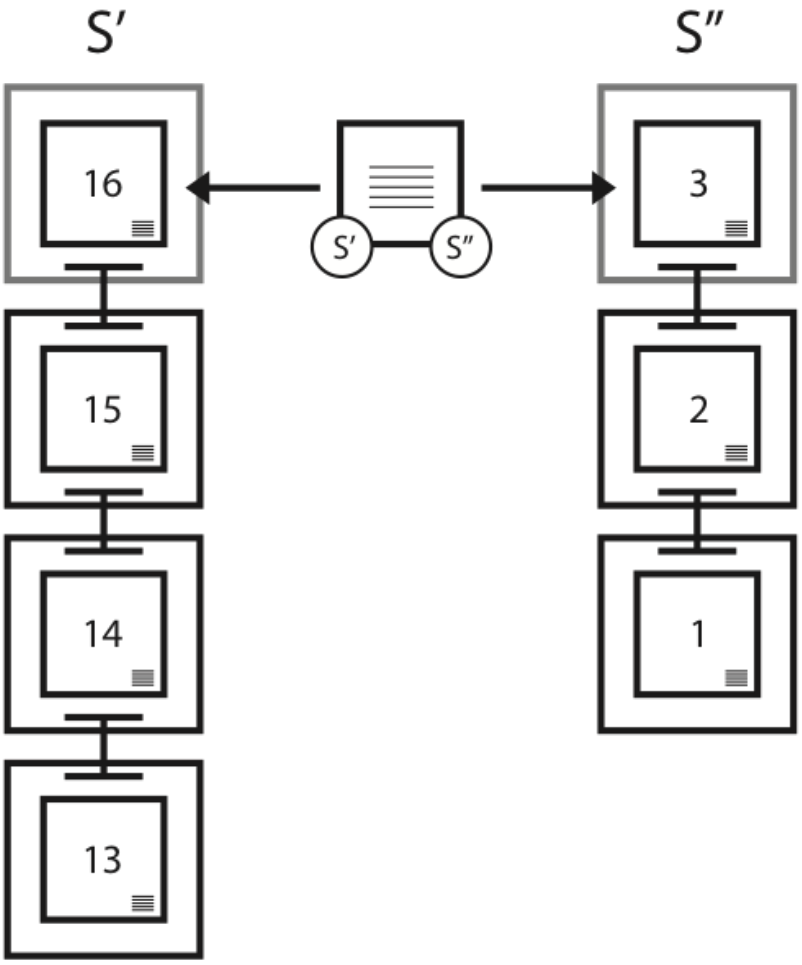

Figura 1 - Esempio di Bound Witness in azione fra due Sentinel

4.7 Le Origin Chain

Ogni origine mantiene il proprio ledger e lo firma per creare una Proof of Origin Chain. Una volta che l'informazione presente sulla Proof of Origin Chain è stata condivisa, è a tutti gli effetti permanente. Questo perché la fork che avviene dopo la condivisione pone fine alla catena e fa sì che tutti i dati futuri provenienti dal testimone siano trattati come se il testimone fosse nuovo. Per generare un collegamento in una Proof of Origin Chain, l'origine genera una coppia di chiavi pubblica/privata con cui poi firma sia il blocco precedente che il successivo, dopo aver incluso la chiave pubblica in entrambi. Subito dopo la realizzazione della firma, la chiave privata viene cancellata, così minimizzando significativamente il rischio di furto o riutilizzo della stessa.

Le Proof of Origin Chain costituiscono la chiave per verificare la validità dei ledger che circolano all'interno di XYO Network. Un ID univoco per la fonte dei dati non risulta un'opzione praticabile, poiché passibile di contraffazione. Una firma con chiave privata non è praticabile perché gran parte di XYO Network è difficile, se non impossibile, da porre fisicamente in sicurezza, rendendo quindi oltremodo possibile il furto di una chiave privata ad opera di un cattivo agente. Per risolvere questo punto, XYO Network utilizza delle Transient Key Chain (catene a chiave transitoria), che offrono il beneficio di rendere impossibile la falsificazione della catena di origine per i dati. Tuttavia, una volta che la catena si rompe, è rotta per sempre e non può proseguire, costituendo un'isola.

Ogni volta che un ledger euristico viene passato ad altri in XYO Network, il ricevente allega la propria Proof of Origin, allungando la Proof of Origin Chain e generando una Proof of Origin Intersection. Le Proof of Origin Chain e le Proof of Origin Intersection costituiscono i principali indicatori che i Diviner utilizzano per verificare la validità dei ledger. L'equazione per una Ledger Reputation è effettivamente quale percentuale di XYO Network è stata coinvolta nella realizzazione della relativa Proof of Origin Ball. In teoria, se il 100% delle registrazioni di XYO Network sono collegate con Proof of Origin e poi analizzate completamente, la probabilità che risultino valide è del 100%. Se per l'analisi risulta disponibile lo 0% delle registrazioni di XYO Network, allora la validità decade allo 0%.

Per una sicurezza aggiuntiva, la chiave pubblica per un Chain Link non è fornita finché non si rende disponibile la seconda registrazione. Questo consente anche di memorizzare l'intervallo di tempo tra registrazioni o altri dati nel collegamento precedente o successivo.

4.8 Origin Chain Score

L'Origin Chain Score è calcolato come segue (algoritmo di default):

- PcL = Lunghezza della Proof of Origin Chain
- PcD = Difficoltà della Proof of Origin Chain
- Pc' Pc'' O = Sovrapposizione della Proof of Origin Chain per Pc' e Pc''

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

4.9 Origin Tree

Un Origin Tree è impiegato per calcolare la validità approssimata di una risposta. Utilizza i dati raccolti per generare un Ideal Tree, ovvero l'albero ideale, quello che meglio si adatta a quei dati per una data risposta asserita. Se il nodo N è localizzato alla posizione X,Y,Z,T, l'errore fra tutti i dati dell'insieme deve avere un certo valore. Per calcolare tale errore, dovremmo calcolare MIN, MAX, MEDIA, MEDIANA e SCARTO MEDIO.

Dato un insieme S di tutti i punteggi s, una Proof of Origin Chain Difficulty PcD e un fattore di errore, *error*, la Best Answer è determinata come segue:

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

In altre parole, la Best Answer è la risposta asserita che ottiene il Best Answer Score più elevato. Usando il Proof of Origin Tree, possiamo identificare e potare i rami impossibili (gli outlier).

4.10 Concatenamento di Transient Key

Una serie di pacchetti di dati possono essere concatenati attraverso l'utilizzo di chiavi private temporanee che firmino due pacchetti successivi. Quando la chiave pubblica accoppiata alla chiave privata è inclusa nei pacchetti di dati, il ricevente può verificare che entrambi i pacchetti siano stati firmati dalla medesima chiave privata. Non è possibile alterare i dati inclusi nel pacchetto senza rompere la firma, così garantendo che i pacchetti siglati non siano stati alterati da una terza parte, come ad esempio un Bridge o un nodo di archiviazione.

4.11 Link Depth

Come minimo, un nodo genera una nuova coppia di chiavi pubblica/privata per ogni collegamento nella Proof of Origin Chain, che ha una Link Depth pari a 1. Per una determinata *Ledger Entry* (registrazione/voce del ledger), nella tavola dei collegamenti possono esistere N registrazioni, ciascuna indicante il tempo futuro in cui sarà aggiunta la seconda parte del link. Nessun collegamento potrà avere lo stesso ordine di grandezza su una scala a base due. Per esempio, la registrazione `[1,3,7,12,39]` sarebbe ammessa, mentre `[1,3,7,12,15]` no.

Il Link Depth 1 viene creato, usato ed eliminato alla pubblicazione del blocco precedente. Tuttavia, per i link con una profondità superiore a 1, la coppia di chiavi è generata al momento della firma del blocco precedente e la seconda firma non avverrà che dopo N blocchi successivi; dopodiché la chiave privata viene eliminata. Per questa ragione, i collegamenti con una profondità superiore a 1 sono sempre considerati meno sicuri di quelli con Link Depth pari a 1. Tenendo in conto la minore sicurezza, possono comunque essere usati per incrementare la performance e ridurre la perdita di dati.

4.12 Ordine fisso

L'elemento chiave nella determinazione della sequenza dei ledger è l'ordine con cui sono stati comunicati. Dato che un dispositivo non è in grado di modificare l'ordine di un ledger di Proof of Origin firmato, è possibile stabilire un ordine assoluto considerando tutti i ledger collettivamente.

4.13 La penultima pubblicazione

Un metodo primario per stabilire la Proof of Origin è basato sul fatto che una Sentinel comunica sempre il suo penultimo blocco senza riferire l'ultimo. Questo permette all'ultimo blocco di avere il link firmato al suo predecessore come prova del link.

4.14 Link vuoti

Per rendere più sicura una Proof of Origin Chain, si richiede che la catena non sia aggiornata con frequenza maggiore a una volta ogni dieci secondi né inferiore a sei minuti. Nel caso in cui non risultino disponibili nuovi dati, sarà aggiunto alla catena un blocco vuoto.

4.15 Diagramma

Considerando che il tempo scorre da sinistra a destra (Figura 2), la Proof of Origin Chain in costruzione si fa più lunga. In un qualsiasi momento dato, il generatore della catena fornirà all'interrogante soltanto le registrazioni con bordi in neretto, attendendo la seconda firma della registrazione prima di renderla disponibile. Per esempio, nella terza colonna, si restituirà l'informazione secondo cui solo le registrazioni 2 e 1 fanno attualmente parte della catena.

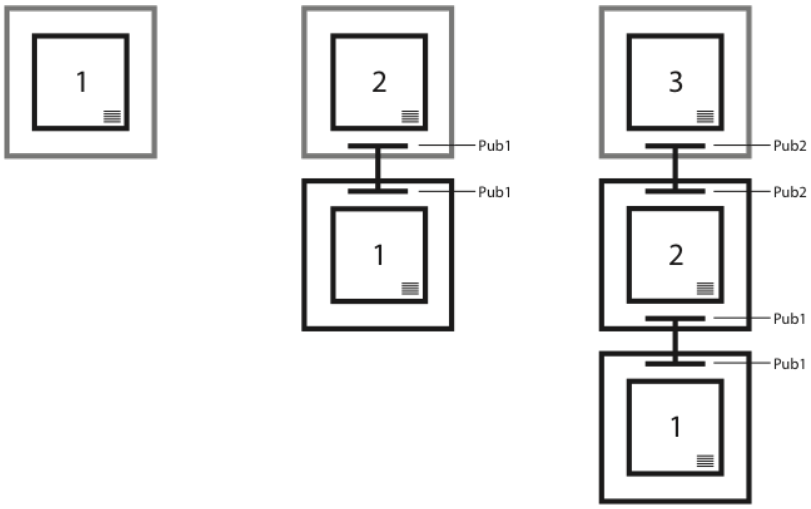

Figura 2 - Esempio di inclusione link in una Proof of Origin Chain

4.16 Riepilogo

Data una serie di pacchetti di dati che sono stati firmati in coppie sequenziali con chiavi private temporanee e che includono le corrispondenti chiavi pubbliche, è possibile determinare con assoluta certezza che tali pacchetti derivano dalla medesima origine.

---

5 Considerazioni sulla sicurezza

5.1 Attacco di falsi Diviner

Una serie di firme digitali viene inviata allo smart contract XYO perché il contratto ha la necessità di verificare l'integrità del Diviner che ha inviato la risposta. Il contratto può poi verificare gli altri Diviner che hanno firmato tale lista all'interno di un intervallo di confidenza elevato. Senza questo aspetto, l'oracle trasmittente rappresenterebbe la singola fonte di fallimento e di rischio all'interno del sistema.

5.2 Attacchi DDoS alle Sentinel

Un'altra minaccia da considerare sono i Distributed Denial of Service (DDoS) fra i nodi Sentinel di una particolare area. Un attaccante potrebbe tentare di stabilire un ampio

numero di connessioni verso le Sentinel al fine di impedire loro di comunicare le informazioni corrette oppure di interrompere del tutto la trasmissione dei dati ai Bridge. Possiamo aggirare questo problema richiedendo la risoluzione di un piccolo puzzle crittografico a chiunque tenti di connettersi a una Sentinel. Siccome una query non coinvolgerà un numero molto grande di connessioni alle Sentinel, questa procedura non graverà pesantemente sul sistema di trasmissione XYO, mentre invece richiederà all'attaccante di ricorrere a un vasto ammontare di risorse per compiere con successo un attacco DDoS alla nostra rete. Una Proof of Origin Chain può essere verificata da chiunque e in qualsiasi momento, se archiviata sulla XYOMainChain. Questo garantisce che se lungo la catena una singola entità è stata compromessa, l'accuratezza della risposta alla query (Origin Chain Score) calerà a 0.

---

6 L'economia del Token XYO

Gli oracle costituiscono una porzione significativa delle necessità infrastrutturali e di energia delle applicazioni decentralizzate, con una maggiore concentrazione intorno alla connettività e all'aggregazione degli oracle autorevoli. Affinché le applicazioni decentralizzate raggiungano il loro massimo potenziale, riteniamo sia necessario un sistema di oracle pienamente decentralizzato e trustless.

6.1 La criptoeconomia di XYO Network

Utilizziamo i Token XYO per incentivare la fornitura di euristiche di localizzazione affidabili ed accurate. I Token XYO possono essere considerati come il "gas" necessario per interfacciarsi con il mondo reale al fine di verificare le coordinate XY di uno specifico oggetto.

Il processo funziona in questo modo: prima di tutto, un detentore di token sottopone una query a XYO Network (es. "*Dove si trova il mio pacco dell'ordine e-commerce con Indirizzo XYO 0x123456789...*"). Dopodiché, la query viene inserita in una coda, dove attende il suo processamento e risposta. Alla creazione della query, un utente può impostare il livello di confidenza desiderato e il prezzo del gas XYO. Il costo di una query (in Token XYO) è determinato dall'ammontare di dati richiesti per fornirle risposta, come anche dalle dinamiche del mercato. All'aumentare dei dati necessari, la query risulterà più costosa e il prezzo del gas XYO più alto. Le query rivolte a XYO Network hanno il potenziale di farsi davvero grandi e costose. Per esempio, un'impresa di trasporto e logistica potrebbe interrogare XYO Network per chiedere: "*Qual è la posizione di ogni singolo automezzo della nostra flotta?*"

Una volta che il detentore di Token XYO interroga XYO Network e paga il gas richiesto, tutti i Diviner chiamati all'opera si rivolgono agli Archivist pertinenti per consultare i dati rilevanti che servono a dare risposta alla query. I dati restituiti sono derivati dai Bridge, che originariamente li avevano raccolti dalle Sentinel. Le Sentinel sono essenzialmente quei dispositivi o segnali che verificano la posizione di oggetti, quindi tracker Bluetooth, tracker GPS, geolocalizzatori inseriti nei dispositivi IoT, tecnologie di controllo satellitare, scanner di QRcode o RFID e molto altro ancora. XY Findables è stata pioniera nel lancio di prodotti consumer basati su Bluetooth e GPS, attività che ha permesso di testare e processare l'euristica di localizzazione del mondo reale. Tutti gli sforzi compiuti nello sviluppo del business di XY Findables rivolto ai consumatori hanno sostenuto in maniera significativa la progettazione del Protocollo Blockchain XYO Network.

Qualora i dati forniti da un dispositivo Sentinel (come ad esempio un Beacon Bluetooth) siano impiegati per rispondere a una query, allora tutti e quattro i componenti coinvolti nella transazione riceveranno una porzione del gas XYO pagato dal detentore del token: il Diviner (che ha cercato la risposta), l'Archivist (che ha memorizzato i dati), il Bridge (che ha trasmesso i dati) e la Sentinel (che ha registrato i dati di posizione). La distribuzione del gas fra 3 dei 4 componenti di XYO Network avviene sempre nella stessa proporzione. L'eccezione è costituita dai Diviner, che giocano un ruolo più ampio nel processo di fornitura di una risposta. All'interno di una stessa categoria di componenti, il gas viene distribuito in parti uguali.

6.2 Ricompense per l'indipendenza

I dispositivi che rilevano i dati di posizione costituiscono gli atomic block della rete e un singolo dispositivo potrebbe agire in uno o più ruoli fra i quattro che compongono il sistema. Tuttavia, in particolare in una rete ampia come XYO Network, sarebbe cosa inconsueta che un dispositivo assumesse più di due ruoli. Oltretutto, un ledger blockchain che registra Proof of Origin maggiormente indipendenti riceverà una maggiore considerazione; esiste pertanto una penalizzazione criptoeconomica per un dispositivo che agisce in molteplici ruoli.

6.3 Ricompense per l'integrità della stazionarietà

Alle Sentinel di XYO Network è assegnato un coefficiente di stazionarietà in base al loro grado di movimento lungo tutto il loro ciclo di vita. Meno una Sentinel si muove durante un certo periodo di tempo, maggiore fiducia potrà essere accordata ai dati che rileva. Quando devono considerare a quali Sentinel inoltrare le query, gli Archivist tracciano e analizzano tali coefficienti di stazionarietà.

6.4 Incentivazione all'uso del Token

Un sistema in cui i detentori dei token hanno incentivo a *non* farne uso genera necessariamente un problema di lungo periodo per l'economia sottostante. Si crea un ecosistema dalle riserve di valore veramente scarse e si scatena un naturale impulso a partorire ragioni per *non* utilizzare il token, invece di favorirne utilità e liquidità.

Il problema mostrato dalla gran parte degli incentivi criptoeconomici riguarda il focus troppo stringente sui miner (es. Sentinel, Bridge, Archivist e Diviner), i generatori dei token, piuttosto che su coloro che li utilizzano. Il Token XYO prende in considerazione entrambe le parti.

Il modello del Token XYO dà incentivo al miner non soltanto a fornire dati accurati, ma anche a sapere quando evitare di fornirne. L'utente finale è ricompensato per effettuare più transazioni quando la liquidità della rete è bassa, rispetto a quando è più elevata. In tal modo l'ecosistema del Token XYO ha la capacità di restare ben bilanciato, fluido e solido.

6.5 Specifiche del Token XYO

La vendita pubblica di token avrà una struttura di prezzo a livelli, a partire da 1 ETH: 100.000 XYO fino a 1 ETH: 33.333 XYO. I dettagli riguardo alla nostra struttura di prezzi in base al volume e al tempo saranno annunciati presto.

- Piattaforma di smart contract: Ethereum
- Tipo di contratto: ERC20
- Token: XYO

- Nome del token: XYO Network Utility Token
- Indirizzo del token: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Emissione totale: Finita e limitata all'ammontare raggiunto dopo la Main Sale
- Tetto di Token XYO Previsto: $48 Milioni
- Token invenduti e non allocati: Saranno bruciati al termine del periodo di vendita. Non saranno generati ulteriori Token XYO una volta conclusasi la Main Sale.

---

7 Casi d'uso di XYO Network

XYO Network ha individuato numerose applicazioni che abbracciano una moltitudine di settori. Prendiamo ad esempio un'impresa di e-commerce che voglia offrire ai suoi clienti un servizio di pagamento alla consegna. Per riuscirci, sfrutterebbe XYO Network (che utilizza Token XYO) per redigere uno smart contract (per es. sulla piattaforma Ethereum). XYO Network potrebbe poi tracciare la localizzazione del pacco invitato al cliente lungo ogni singola fase della spedizione: dallo scaffale del magazzino del fornitore al corriere, fino alla casa del cliente ed ogni altra posizione intermedia. Questo potrebbe permettere ai retailer e ai siti di e-commerce di verificare non soltanto che il pacco è arrivato sull'uscio di casa del cliente, ma anche che vi ha fatto il suo ingresso, il tutto in maniera trustless, ovvero senza l'intervento di terze parti fiduciarie. Una volta che il pacco è arrivato in casa del cliente (evento definito e verificato da specifiche coordinate XY), la spedizione può considerarsi completata e a quel punto viene rilasciato il pagamento verso il venditore. L'integrazione di XYO Network nell'e-commerce permette così di proteggere il commerciante dalle truffe e di garantire ai consumatori di pagare solo per quei beni che gli arrivano effettivamente a casa.

Consideriamo ora un'integrazione di XYO Network completamente differente, un sito di recensioni di hotel il cui problema è l'affidabilità dei feedback inseriti. È naturale che i titolari degli hotel abbiano incentivo a migliorare le proprie recensioni a tutti i costi. Ipotizziamo che si possa affermare con certezza estremamente alta che qualcuno si trovasse a San Diego, sia volato fino a Bali, abbia soggiornato in hotel per due settimane e poi, di ritorno a San Diego, ne abbia scritto una recensione. Tale feedback avrebbe un'affidabilità davvero elevata, in particolar modo se a scrivere fosse una persona che ha pubblicato molte altre recensioni con dati di localizzazione verificati.

---

8 Espansione di XYO Network

Abbiamo la fortuna di avere un'impresa consumer che ha costruito con successo una rete di oltre un milione (1.000.000) di dispositivi Bluetooth e GPS nel mondo fisico. La maggior parte dei network di localizzazione non riesce a raggiungere questo stadio e ad arrivare a quella massa critica necessaria per costruire una rete di vasta portata. La rete di Sentinel che abbiamo creato è solo il punto di inizio. XYO Network è un sistema aperto in cui qualsiasi operatore di dispositivi di localizzazione può inserirsi e iniziare ad aggiudicarsi Token XYO.

In linea generale, all'aumentare della cardinalità delle Sentinel operanti in XYO Network, maggiore sarà l'affidabilità della rete. Per il suo ulteriore sviluppo, XYO Network sta intrattenendo contatti con altre imprese al fine di espandere la propria rete di Sentinel oltre il proprio network di beacon di XY Findables.

9 Ringraziamenti

Questo white paper è il prodotto degli sforzi di un team pieno di entusiasmo e della fiducia verso la nostra visione da parte delle seguenti persone: Raul Jordan (Harvard College, beneficiario della Thiel Fellowship e Advisor di XYO Network), per il suo contributo nel rendere il nostro white paper più conciso, aiutandoci a comunicare al mondo in forma elegante i dettagli tecnici del progetto. Ringraziamo Christine Sako per la sua eccezionale etica del lavoro e l'attenzione al dettaglio nella revisione dei nostri contenuti. La coerenza in termini di struttura e di best practice che risalta dal nostro white paper è il prodotto del suo impegno. Un grazie anche a Johnny Kolasinski, per la sua attività di ricerca ed esposizione dei casi d'uso applicabili. Infine, ringraziamo John Arana per la sua attenta revisione e lo spunto creativo.

Fonti

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

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

[3] Di Ferrante, Matt. *Proof of Location*. `https://www.reddit.com/r/ethereum/comments/539o9c/proof_of_location/`. 17 settembre 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, 4 febbraio 2014.

Glossary

accuratezza Una misura di confidenza secondo cui un dato o euristica ricada all'interno di uno specifico margine di errore. 1, 2, 4, 5, 7, 9

Archivist Un Archivist memorizza le euristiche come parte del dataset decentralizzato con l'obiettivo di mantenere archiviati tutti i ledger storici, ma senza tale requisito. 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, qualora necessario, possano restituire una stringa di dati del registro. Archiviano soltanto dati grezzi e ricevono un pagamento esclusivamente per la loro consultazione. L'archiviazione è sempre gratuita. 4, 5, 7, 14, 15

Best Answer Definiamo come Best Answer all'interno di una lista di Answer Candidates quella singola risposta che restituisce il punteggio di validità maggiore e possiede un punteggio di accuratezza superiore al valore minimo necessario. 6, 7, 9, 11

Best Answer Algorithm Un algoritmo utilizzato per generare i Best Answer Score quando un Diviner seleziona una risposta. XYO Network permette l'aggiunta di algoritmi specializzati e consente al cliente di specificare quale usare. Si richiede che tale algoritmo restituisca il medesimo punteggio quando applicato a un determinato dataset processato da qualsiasi Diviner. 7

Bound Witness Il concetto di Bound Witness è derivato dall'esistenza di un'euristica bidirezionale. Dato che una fonte di dati untrusted non è utile alla risoluzione di un contratto digitale (un oracle), si registra un incremento sostanziale della certezza dei dati forniti attraverso la dimostrazione di una determinata euristica. La principale euristica bidirezionale è la prossimità, dato che entrambe le parti possono validare l'occorrenza e l'intervallo di un'interazione firmandola congiuntamente. Questo permette di compiere una dimostrazione a conoscenza zero del fatto che i due nodi fossero in prossimità l'uno all'altro. 1, 8, 9

Bridge Un Bridge è un trascrittore di euristica.Trasmette in modo sicuro i ledger di euristica dalle Sentinel ai Diviner. L'aspetto più importante di un Bridge è che un Diviner 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 metadato di Proof of Origin addizionale. 4, 5, 12, 14, 15

certezza Una misura della probabilità che un dato o euristica sia esente da corruzione o manomissione. 1–4, 8, 9, 13, 16

cripto-localizzazione L'ambito della tecnologia di localizzazione crittografica. 3

criptoeconomia Disciplina formale che studia i protocolli che governano la produzione, la distribuzione e il consumo di beni e servizi in un'economia digitale decentralizzata. La criptoeconomia costituisce una scienza pratica focalizzata sulla progettazione e caratterizzazione di tali protocolli. 15

Diviner Un Diviner dà risposta a una determinata query analizzando i dati storici memorizzati da XYO Network. Le euristiche archiviate all'interno di XYO Network devono avere un elevato livello di Proof of Origin per determinare la validità ed accuratezza dell'euristica. Un Diviner ottiene e fornisce una risposta attraverso una valutazione del testimone sulla base della sua Proof of Origin. Dato che XYO

Network è un sistema trustless, i Diviner devono essere incentivati a fornire delle analisi delle euristiche veritiere. Diversamente dalle Sentinel e dai Bridge, i Diviner impiegano la Proof of Work per aggiungere risposte alla blockchain. 4, 5, 7, 8, 11, 13–15

euristica Dato riguardante il mondo reale relativo alla posizione di una Sentinel (prossimità, temperatura, luce, movimento ecc.). 4, 5, 7–9, 11, 14

oracle Parte di un sistema DApp (applicazione decentralizzata) responsabile della risoluzione di un contratto digitale attraverso la fornitura di una risposta con accuratezza e certezza. Il termine "oracle", oracolo, trae origine dalla crittografia, dove indica una fonte genuinamente casuale (per es. un numero casuale). Ciò fornisce la porta necessaria da una cripto-equazione al mondo che ne sta oltre. Gli oracle forniscono agli smart contract informazioni dall'esterno della catena (off-chain, il mondo reale). Sono quindi delle interfacce fra il mondo digitale e quello fisico. Come macabro esempio, si consideri un contratto di Ultime Volontà, il Testamento. I termini di tale contratto sono eseguiti alla conferma del decesso del testatore. Si potrebbe generare un servizio oracle che dia esecuzione al Testamento attraverso la compilazione e l'aggregazione di dati rilevanti derivati da fonti ufficiali. L'oracle potrebbe allora essere utilizzato come feed o end-point per uno smart contract a cui ricorrere per verificare se la persona sia deceduta o meno. 1, 3, 4, 8, 14

Origin Chain Score Il punteggio assegnato a una Origin Chain per determinarne la credibilità. È una valutazione che tiene conto delle variabili di lunghezza, tangling, overlapping e ridondanza. 4, 6, 7, 11, 14

Origin Tree Un dataset di registrazioni del ledger tratto da varie Origin Chain per stabilire con uno specifico grado di certezza l'origine di una voce del ledger euristico. 11

Proof of Origin La Proof of Origin è la chiave per verificare la validità dei ledger che circolano all'interno di XYO Network. Un ID univoco per la fonte dei dati non risulta un'opzione praticabile, poiché passibile di contraffazione. Una firma con chiave privata non è praticabile perché gran parte di XYO Network è difficile, se non impossibile, da porre fisicamente in sicurezza, rendendo quindi oltremodo possibile il furto di una chiave privata ad opera di un cattivo agente. Per risolvere questo punto, XYO Network utilizza delle Transient Key Chain, che offrono il beneficio di rendere impossibile la falsificazione della catena di origine per i dati. Tuttavia, una volta che la catena si rompe, è rotta per sempre e non può proseguire, costituendo un'isola. 1, 4, 5, 8, 11, 12, 15

Proof of Origin Chain Una Transient Key Chain che collega una serie di voci Bound Witness del ledger euristico. 4, 7, 10–12, 14

Proof of Work La Proof of Work è costituita da dati che soddisfano certi requisiti; è difficile da produrre (è costosa e richiede tempo), ma rende semplice la verifica da parte di terzi. La generazione di una Proof of Work può rappresentare un processo casuale dalle ridotte probabilità di successo, quindi è generalmente richiesto un rigoroso processo per tentativi ed errori prima di produrre una Proof of Work valida. 5–7

Sentinel Una Sentinel è testimone di un'euristica. Osserva le euristiche dei dati e ne garantisce la certezza e l'accuratezza generando dei ledger temporali. L'aspetto più importante di una Sentinel è il fatto che, grazie all'aggiunta della Proof of Origin, produce dei ledger di cui i Diviner possono avere la certezza che provengano dalla medesima fonte. 3–5, 7, 9, 12–16

smart contract Un protocollo coniato da Nick Szabo prima dell'avvento del Bitcoin, presumibilmente nel 1994 (per questo motivo qualcuno crede che sia lui Satoshi Nakamoto, il misterioso e sconosciuto inventore del Bitcoin). L'idea alla base degli smart contract consiste nel codificare un accordo legale all'interno di un programma e predisporre dei computer decentralizzati che ne eseguano i termini, invece dell'intervento umano volto a interpretare e dare esecuzione ai contratti. Gli smart contract riuniscono denaro (es. Ether) e contratti all'interno dello stesso concetto. Siccome gli smart contract sono deterministici (come i programmi per computer) nonché pienamente trasparenti e comprensibili, rappresentano una formidabile maniera per rimpiazzare intermediari e broker. 1–5, 7, 13, 16

Transient Key Chain Una Transient Key Chain collega una serie di pacchetti di dati impiegando la Crittografia a Transient Key. 11

trustless Caratteristica in cui tutte le parti operanti in un sistema sono in grado di raggiungere un consensus in merito a una verità canonica. Potere e fiducia risultano distribuiti (o condivisi) fra gli stakeholder della rete (es. sviluppatori, miner e consumatori), invece di essere concentrati nelle mani di un singolo individuo o entità (es. banche, governi e istituzioni finanziarie). Rappresenta un termine comune che può facilmente fuorviare. Le blockchain non eliminano effettivamente la fiducia, ma si occupano piuttosto di minimizzarne l'ammontare richiesto da un qualunque singolo agente nel sistema. Compiono questo distribuendo la fiducia fra i diversi attori all'interno del sistema, attraverso un gioco economico che dà incentivo a tali attori affinché cooperino secondo le regole definite dal protocollo. 1, 3–5, 8, 14, 16

XY Oracle Network XYO Network. 1

XYO Network XYO Network indica "XY Oracle Network." È una rete costituita dall'intero sistema di componenti/nodi abilitati alla tecnologia XYO, fra cui Sentinel, Bridge, Archivist e Diviner. La principale funzione di XYO Network è agire come un portale tramite cui gli smart contract digitali possono essere eseguiti attraverso delle conferme di geolocalizzazione del mondo reale. 2–5, 7, 11, 14–17

XYOMainChain Una blockchain immutabile all'interno di XYO Network che archivia le operazioni di query insieme ai dati raccolti dai Diviner e al loro relativo punteggio di origine. 14