White Paper da XYO Network: a rede de localização criptográfica baseada em Proof-of-Origin

de Arie Trouw[1], Markus Levin[2], Scott Scheper[3]

Resumo

Com a presença crescente de tecnologias conectadas baseadas em localização, nossa privacidade e segurança confiam fortemente na **precisão** e validade de informações de localização. Foram feitas várias tentativas de eliminar a necessidade de que entidades centralizadas controlem o fluxo de dados de localização, mas cada tentativa se baseou na integridade dos dispositivos que coletavam esses dados no mundo físico. Propomos uma rede de localização criptográfica **sem verificação de confiabilidade** usando uma nova formulação baseada em uma cadeia de provas de conhecimento zero para estabelecer um alto grau de **certeza** de dados em informações de localização. A **XYO Network** (**XY Oracle Network**) é uma abstração que habilita verificação de localização escalonada em muitos protocolos e classes de dispositivos. No seu âmago há um conjunto de novos mecanismos criptográficos conhecidos como **Proof of Origin** e **Bound Witness**, que vinculam o poder da tecnologia blockchain e coleta de dados no mundo real em um sistema com aplicações diretas hoje.

1 Introdução

Com o advento dos **contratos inteligentes sem verificação de confiabilidade** baseados em blockchain, a necessidade de serviços **oracle** que arbitrem o desfecho de um contrato cresceu de forma significativa. A maioria das implantações atuais de contratos inteligentes se baseia em um único oracle ou em um conjunto agregado de oracles confiáveis para definir o desfecho de um contrato. Em casos nos quais ambas as partes conseguem chegar a um acordo sobre a autoridade e incorruptibilidade do oracle específico, isso é suficiente. No entanto, em muitos casos não existe um oracle suficiente ou o oracle não pode ser considerado confiável devido à possibilidade de erro ou corrupção.

[1] XYO Network, arie.trouw@xyo.network
[2] XYO Network, markus.levin@xyo.network
[3] XYO Network, scott.scheper@xyo.network

Os oracles de localização caem nessa categoria. A adivinhação da localização de um item no mundo físico se baseia nos componentes de reporte, retransmissão, armazenagem e processamento do oracle específico, todos os quais introduzem erros e podem ser corrompidos. Os riscos incluem manipulação de dados, poluição de dados, perda de dados e conluio.

Assim, existe o seguinte problema: **tanto a certeza quanto a precisão de localização são impactados negativamente pela falta de um oracle de localização descentralizado sem verificação de confiabilidade.** Plataformas como Ethereum e EOS têm sido amplamente usadas para mediar interações on-line com segurança, com os principais casos de uso envolvendo cauções para cauções de angariação de fundos na forma de ICOs. No entanto, até esse ponto, cada plataforma focou inteiramente no mundo on-line e não no mundo físico devido a distorções e corruptibilidade da integridade de dados dos canais atuais de informação.

A XY está trabalhando rumo ao conceito de proporcionar aos desenvolvedores (como os que redigem contatos inteligentes Ethereum) o poder de interagir com o mundo real como se fosse uma API. A **XYO Network** é o primeiro protocolo oracle do mundo que possibilita que duas entidades transacionem no mundo real sem um terceiro centralizado. Nossas abstrações permitem que façamos verificação de localização sem verificação de confiabilidade para desenvolvedores, criando um protocolo com novos casos de uso que não eram possíveis até hoje.

A XYO Network será construída com base em uma infraestrutura existente de um milhão de dispositivos distribuídos ao redor do mundo por meio da nossa empresa de relacionamento com os consumidores da Findables. Os dispositivos Bluetooth e GPS da XY permitem que consumidores frequentes coloquem marcadores de rastreamento físico em coisas que desejam rastrear (como chaves, bagagem, bicicletas e até mesmo animais de estimação). Se perderem ou extraviarem esses itens, poderão ver exatamente onde eles estão ao visualizar a localização em um aplicativo para smartphone. Em apenas seis anos, a XY Network criou uma das maiores redes de Bluetooth e GPS de consumidores do mundo.

---

2 Antecedentes e tentativas anteriores

2.1 Proof of Location

O conceito de localização provável existe desde os anos sessenta e pode remontar até mesmo aos anos quarenta com os sistemas de rádio-navegação baseados em terra, como o LORAN [1]. Hoje em dia há serviços de localização que empilham múltiplos meios de verificação para criar uma Proof of Location por meio de serviços de triangulação e GPS. No entanto, essas abordagens ainda precisam enfrentar o componente mais crítico que enfrentamos hoje

nas tecnologias de localização: conceber um sistema que detecte sinais fraudulentos e desestimule o uso de dados de localização falsos. Por essa razão, acreditamos que a plataforma de criptolocalização mais significativa hoje será aquela que se concentre principalmente em provar a origem de sinais de localização físicos.

Incrivelmente, o conceito de aplicação da verificação de localização a tecnologias blockchain surgiu pela primeira vez em setembro de 2016, na DevCon 2 da Ethereum. Foi apresentado por Lefteris Karapetsas, um desenvolvedor da Ethereum de Berlim. O projeto de Karapetsas, o *Sikorka*, possibilitou que **contratos inteligentes** fossem implantados imediatamente no mundo real, usando o que ele denominou como "*Proof of Presence*". O aplicativo dele, que visavaunir a localização e o mundo da blockchain, focava principalmente casos de uso de realidade aumentada, e ele apresentou novos conceitos como perguntas de segurança para provar a localização de alguém [2].

Em 17 de setembro de 2016 o termo "*Proof of Location*" veio formalmente à tona na comunidade da Ethereum [3]. Então, ele foi objeto de esclarecimentos adicionais pelo desenvolvedor da Ethereum Foundation, Matt Di Ferrante:

> "*Honestamente, uma Proof of Location em que se possa confiar é uma das coisas mais difíceis de implantar. Mesmo que haja muitos participantes que possam atestar a localização uns dos outros, não há garantia de que eles não perderiam a confiabilidade em algum momento futuro, e como somente se pode confiar em reporte majoritário, isso é um ponto fraco muito importante. Se fosse possível exigir algum tipo de dispositivo de hardware especializado que tivesse alguma tecnologia antiadulteração de modo que a chave privada fosse destruída quando alguém tentasse abri-lo ou alterar o firmware dele, seria possível ter mais segurança, mas ao mesmo tempo, não é como se fosse impossível falsificar sinais de GPS. A implantação apropriada disso requer tantos passos atrás e tantas fontes de dados diferentes para ter alguma garantia de precisão que precisaríamos de um projeto muito bem financiado.*" [3]
>
> *— Matt Di Ferrante, desenvolvedor, Ethereum Foundation*

2.2 Proof of Location: deficiências

Em síntese, a Proof of Location pode ser compreendida como um elemento que potencializa as propriedades robustas da blockchain, como marcação de horário e descentralização, e as combina com dispositivos difíceis de enganar. Referimo-nos ao reino da tecnologia de localização criptográfica como "criptolocalização". Da mesma forma que o ponto fraco dos **contratos inteligentes** gira em torno de **oracles** que usam uma única fonte de verdade (e, assim, uma única fonte de falhas), os sistemas de criptolocalização enfrentam o mesmo problema. A vulnerabilidade das tecnologias de criptolocalização atuais gira em torno dos

dispositivos que informam a localização de um objeto. Em contratos inteligentes, essa fonte de dados é um oracle. Na X**YO Network,** a fonte de dados off-chain circula no mundo real como um tipo especializado de oracle que chamamos de **Sentinel**. A verdadeira inovação no âmago da **XYO Network** se concentra em torno de uma prova baseada em localização subjacente aos componentes do nosso sistema para criar um protocolo de criptolocalização seguro.

---

3 A XY Oracle Network

> "*A necessidade de um sistema difícil de sabotar para complementar o GPS é bem conhecida há anos. O GPS é excepcionalmente preciso e confiável; ainda assim, interferências propositais, falsificações, ciber-ataques e outras formas de interferência parecem estar crescendo em frequência e gravidade. Isso pode gerar efeitos arrasadores em nossas vidas e atividades econômicas.*" [4]
> — *Dana Goward, presidente, RNT Foundation*

3.1 Introdução

A meta da **XYO Network** é criar um sistema de localização **oracle** descentralizado **sem verificação de confiabilidade** que seja resistente a ataques e produza a mais alta **certeza** possível quando questionado quanto a dados disponíveis. Atingimos isso por meio de um conjunto de abstrações que reduzem significativamente o risco de falsificação de localização através de uma cadeia de provas de conhecimento zero ao longo dos componentes do sistema.

3.2 Panorama geral da rede

O nosso sistema proporciona um ponto de entrada em um protocolo de dispositivos conectados apresentando alta **certeza** em dados de localização por meio de uma cadeia de provas criptográficas. Os usuários conseguem emitir transações, denominadas "*consultas*", para recuperar um dado de localização em qualquer plataforma blockchain que processe a funcionalidade **contrato inteligente**.[4] Agregadores da XYO Network então ouvem essas consultas emitidas para o contrato e pegam as respostas que tenham a maior precisão a partir de um conjunto descentralizado de dispositivos que retransmitem provas criptográficas de volta para esses agregadores. Esses agregadores alimentam essas respostas de volta para o contrato inteligente após atingir um consenso sobre a reposta com a melhor pontuação. Essa rede de dispositivos torna possível determinar se um objeto está em

[4] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter-party, Monax e outras

coordenadas XY específicas em um dado momento, com a certeza mais provável possível **sem verificação de confiabilidade**.

A XYO Network tem quatro componentes principais: **Sentinels** (os coletores de dados), **Bridges** (os retransmissores de dados), **Archivists** (os armazenadores de dados) e **Diviners** (os agregadores de respostas). Sentinels coletam informações de localização através de sensores, rádios e outros meios. Bridges pegam esses dados de Sentinels e os fornecem a Archivists. Archivists armazenam essas informações para que Diviners as analisem. Diviners analisam heurísticas de localização de Archivists para gerar respostas a consultas e atribuir pontuações de precisão a elas. Então, Diviners retransmitem essas respostas de volta para um contrato inteligente (assim, Diviners servem como **oracles**). A pontuação de precisão, denominada **Origin Chain Score**, é determina por meio de um conjunto de provas de conhecimento zero conhecido como **Proof of Origin Chain**. Essa cadeia garante que dois ou mais dados se originaram da mesma fonte, sem revelar informações subjacentes. Cada componente ao longo do caminho da consulta gera o seu próprio, que é então encadeado a cada componente para o qual retransmite dados. **Proof of Origin** é uma formulação nova que constrói uma cadeia de garantias criptográficas ao longo de um caminho de retransmissores na rede para oferecer alta confiança em dados do mundo real. A **Proof of Origin Chain** encapsula a confiança que podemos ter em um dado de localização, remontando ao primeiríssimo dispositivo que coletou os dados. Na seção seguinte, exploraremos em profundidade como a Proof of Origin funciona.

Para estabelecer um mecanismo de consenso descentralizado entre Diviners, a XYO Network se baseará em uma blockchain pública imutável conhecida como **XYOMainChain**, que armazena transações de consultas juntamente com dados coletados de Diviners e as pontuações de origem associadas. Antes de mergulharmos nos detalhes da funcionalidade de todo o sistema, definiremos claramente as responsabilidades de cada componente da nossa rede.

3.2.1 Sentinels

Sentinels são testemunhos de localização. Eles observam a **heurística** dos dados e atestam a **certeza** e a **precisão** desses dados produzindo registros cronológicos. O aspecto mais importante de um Sentinel é que os Diviners podem comprovar que os registros por ele produzidos vieram da mesma fonte, adicionando a eles uma Proof of Origin. Isso é feito adicionando uma **Proof of Origin** a uma cadeia de retransmissão de provas criptográficas. Dado que a **XYO Network** é um sistema **sem verificação de confiabilidade**, os Sentinels devem ser incentivados a fornecer informações honestas de localização. Isso é feito combinando um componente de reputação com um componente de pagamento. Um Sentinel é recompensado com Tokens XYO Network (XYO) quando suas informações são usadas para

responder a uma consulta. Para aumentar as chances de serem recompensados, eles precisam criar registros que sejam coerentes com os dos seus pares e proporcionarm Proof of Origin para se identificarem como a fonte das informações de localização.

3.2.2 Bridges

Bridges são transcritores de dados de localização. Eles retransmitem com segurança os registros heurísticos dos **Sentinels** para **Archivists**. O aspecto mais importante de um Bridge é que um Archivist pode ter certeza de que os registros **heurísticos** recebidos de um Bridge não sofreram nenhuma alteração. O segundo aspecto mais importante de um Bridge é que ele acrescenta uma **Proof of Origin** adicional. Dado que a **XYO Network** é um sistema **sem verificação de confiabilidade**, os Bridges devem ser incentivados a fornecer retransmissões de heurística honestas. Isso é feito combinando um componente de reputação com um componente de pagamento. Um Bridge é recompensado com Tokens XYO Network (XYO) quando as informações que ele retransmitiu são usadas para responder a uma consulta. Para aumentar as chances de serem recompensados, eles precisam criar registros que sejam coerentes com os dos seus pares e proporcionar Proof of Origin para se identificarem como a retransmissão da heurística.

3.2.3 Archivists

Archivists armazenam informações de localização de **Bridges** de forma descentralizada com a meta de armazenar todos os registros históricos. Mesmo que alguns dados sejam perdidos ou fiquem temporariamente indisponíveis, o sistema continua a funcionar, embora com precisão reduzida. Archivists também indexam registros de modo que possam retornar uma sequência de dados de registros, se necessário. Archivists armazenam somente dados brutos e são pagos com Tokens XYO Network somente pela recuperação e uso subsequente dos dados. A armazenagem sempre é grátis.

Archivists formam uma rede, então fazer uma consulta a um Archivist fará com que esse Archivist peça a outros Archivists dados que ele não contém. Opcionalmente, um Archivist pode armazenar quaisquer informações de registro que sejam devolvidas a ele. Isso muito provavelmente resultará em dois tipos de Archivists: os que estão na extremidade de produção de dados da “nuvem” e os que estão na extremidade de consumo de dados da “nuvem”. Os Archivists no meio serão híbridos. A opção de armazenar dados não é imposta, mas pode facilmente ser feita por meio da IPFS ou outra solução de armazenagem descentralizada. Sempre que dados forem transmitidos de um Archivist para outro, uma Proof of Origin adicional é anexada de modo a rastrear o pagamento, para que todos os Archivists sejam pagos. Para recuperações, pode ser ajustado um nível mínimo de Proof of Origin para aumentar a validade. Os interesses de **Sentinels**, Bridges e Archivists devem estar alinhados para impedir excesso de dados.

3.2.4 Diviners

Diviners são a parte mais complexa da **XYO Network**. A meta geral de um Diviner é buscar os dados mais precisos para uma consulta da XYO Network e retransmitir esses dados de volta para o emissor da consulta. Diviners pesquisam a plataforma blockchain aplicável (isto é, Ethereum, Stellar, Cardano, IOTA etc.) para consultas emitidas para o **contrato inteligente** XYO. Então, eles encontram a resposta à consulta interagindo diretamente com a rede de **Archivists** para buscar a resposta com a pontuação mais alta de **precisão**/confiança. Fazem isso julgando o testemunho com a melhor **Proof of Origin Chain**. Os Diviners que pegam a resposta com a melhor pontuação no intervalo de tempo mais curto terão a capacidade de criar um bloco na blockchain principal XYO (**XYOMainChain**) por meio de **Proof-of-Work**. As consultas são priorizadas por tamanho da recompensa e complexidade, então quanto mais XYO for oferecido por uma resposta, mais alta seria a prioridade da consulta.

Outros Diviners chegam a um consenso sobre a validade de um bloco e assinam esse bloco digitalmente. O Diviner que foi o endereço da coinbase daquele bloco enviará ao contrato inteligente uma transação contendo a resposta, juntamente com a pontuação de precisão. Ele também enviará uma lista de assinaturas de outros Diviners para impedir que um invasor emita informações falsas para a blockchain fingindo ser um Diviner. Então, o contrato inteligente pode verificar a integridade dessa informação checando a lista de assinaturas da carga útil.

3.3 Funcionalidade integral

Agora que as responsabilidades de cada componente foram detalhadas, aqui está um exemplo completo de como o sistema funcionará:

1. **Os Sentinels coletam dados**
    - Os **Sentinels** coletam **heurísticas** de localização do mundo real e preparam sua própria **Proof of Origin** a ser encadeada a nós acima delas.
2. **Os Bridges coletam dados dos Sentinels**
    - Os **Bridges** coletam dados necessários de Sentinels on-line e anexam Proof of Origin à cadeia deles. Os Bridges então ficam disponíveis para os **Archivists** na Rede.
3. **Os Archivists indexam/montam dados dos Bridges**
    - Os Bridges enviam constantemente informações aos Archivists, que são então mantidos em estoques descentralizados juntamente com um índice heurístico de localização.
4. **O Diviner pega a consulta de um usuário**

• Diviners pesquisam as consultas enviadas ao **contrato inteligente** da Ethereum e decidem começar o processo de formulação da resposta.

5. **O Diviner coleta dados de Archivists**

• Os Diviners então decidem aceitar uma consulta buscando as informações apropriadas necessárias na rede de Archivists.

6. **O Diviner formula a resposta**

• Os Diviners escolhem a **Best Answer** para a consulta na rede de Archivists que contém a melhor **Origin Chain Score**.

7. **O Diviner propõe um bloco**

• Os Diviners então propõem blocos na **XYOMainChain** contendo o conteúdo da resposta, a consulta e os Tokens XYO (XYO) pagos por meio de **Proof of Work**. Outros Diviners na rede assinam digitalmente o conteúdo do bloco e então a conta aleatória do Diviner da coinbase é atualizada para exibir sua Proof of Work no sistema assim que um consenso sobre um bloco válido for atingido.

8. **O Diviner retorna o resultado para o iniciador da consulta**

• Os Diviners unem a resposta, sua Origin Chain Score e o seu conjunto de assinaturas digitais e envia para um componente adaptador que se conecta com segurança ao contrato inteligente XYO. O adaptador é responsável por garantir que a integridade do Diviner não tenha sido comprometida e envia o conjunto de respostas assinado digitalmente para o contrato inteligente. Isso acontece logo após o processo de criação do bloco. O Diviner da coinbase é então pago pelos seus esforços.

9. **Os componentes da XYO Network são recompensados pelo trabalho deles**

• Os componentes ao longo da Proof of Origin Chain são pagos pelo envolvimento na busca da resposta para a consulta. Os Sentinels, Bridges, Archivists e Diviners são remunerados pelo trabalho deles.

Caso a mesma consulta seja feita mais de uma vez, mais de uma resposta poderá ser produzida, já que a resposta produzida em um dado momento se baseia nas heurísticas disponíveis que o sistema pode oferecer naquele momento. A apresentação de uma resposta à blockchain segue duas etapas. Primeiro, deve-se fazer uma análise para determinar a Best Answer à uma consulta. Se o sistema gerar respostas múltiplas, os nós compararão as respostas e sempre escolherão a melhor. Um exemplo de consulta simples seria: "*Onde estava um nó na rede em um momento específico no passado?*"

3.4 A Blockchain como fonte única de verdade

No seu âmago, os **Diviners** simplesmente transformam dados relativos em dados absolutos. Eles conseguem explorar toda a rede de **Archivists** para concretizar uma resposta absoluta a uma consulta na **XYO Network**. Os Diviners também são os nós que propõem e adicionam blocos à **XYOMainChain** e são recompensados pela sua **Proof-of-Work**. Sendo a rede de Archivists um estoque de dados não processados e a blockchain um estoque de dados absolutos processados, a rede pode, no devido tempo, usar as últimas informações da XYOMainChain para responder consultas futuras em vez de confiar em computação onerosa por meio da Rede de Archivists.

Uma vez que os blocos na XYOMainChain armazenem a **Proof of Origin Chain** e o gráfico de componentes que foram usados para responder consultas, Diviners futuros podem explorar esses dados absolutos para atingir resultados precisos com menor uso de largura de banda. Como tal, a XYOMainChain se tornará gradativamente a fonte de verdade mais importante do sistema. No entanto, uma rede de Archivists ainda será necessária para manter as informações mais atualizadas sobre **heurísticas** de localização coletadas por **Sentinels**.

3.5 Estrutura da XYO Network para selecionar a Best Answer Candidate

Definimos **Best Answer** como a única resposta, dentre uma lista de Answer Candidates, que retorna a pontuação de validade mais alta e tem uma pontuação de **precisão** mais alta do que a precisão mínima requerida. A pontuação de validade se baseia na **Origin Chain Score**. O sistema sabe qual é a Origin Score mais alta registrada, que seria 100% até que uma pontuação mais alta fosse atingida e então se tornasse a nova 100%. A **XYO Network** possibilita a seleção do **Best Answer Algorithm** para determinar a Best Answer. Isso cria expansão para futuras pesquisas em algoritmos alternativos.

Quando forem excluídos dados de uma resposta por serem considerados ruins ou incorretos, ela será enviada aos archivists para que expurguem esses dados dos seus estoques descentralizados.

3.6 Integração inicial com Blockchains públicas

A **XYO Network** foi concebida para ser uma abstração capaz de interagir com qualquer blockchain pública habilitada para **contratos inteligentes** como Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano e outras. Para interagir com a XYO Network, os usuários do Ethereum, por exemplo, podem emitir consultas para o nosso contrato inteligente XYO e pagar em Tokens XYO (ERC20). Os nós da nossa XYO Blockchain, denominados **Diviners**, pesquisariam constantemente a Ethereum quanto a essas consultas e seriam recompensados na moeda corrente nativa da nossa própria XYOMainChain (também denominada Tokens XYO). No futuro, faremos uma conversão individual a partir de portadores do nosso token ERC20 para a moeda corrente nativa da nossa própria blockchain a fim de prover nossas

plataformas com taxas de transações compatíveis com os requisitos de micropagamentos necessários para casos de uso escaláveis de IoT. Nesses casos, permitiremos que os usuários emitam consultas diretamente para a nossa blockchain, em vez de interagir por meio de um contrato inteligente público.

---

4 Proof of Origin

Com uma rede física composta por nós sem verificação de confiabilidade é possível determinar a certeza de dados que tenham sido fornecidos por nós periféricos com base em uma prova de conhecimento zero originada de dois ou mais dados da mesma fonte. Usando esses conjuntos de dados combinados com um número de conjuntos de dados similares e o conhecimento da localização absoluta de pelo menos um nó, a localização absoluta do outro nó pode ser determinada.

4.1 Introdução à Proof of Origin

Sistemas **sem verificação de confiabilidade** tradicionais recorrem a uma chave privada para assinar transações ou contratos em um sistema. Isso funciona muito bem com a premissa de que o nó na rede que assina os dados em questão está física e virtualmente seguro. No entanto, se a chave privada for comprometida, a capacidade de comprovar a origem falha.

Ao aplicar conceitos sem verificação de confiabilidade na Internet das Coisas, deve-se presumir que nós periféricos não são física ou virtualmente seguros. Isso gera a necessidade de identificar nós periféricos sem o uso de IDs exclusivos e, em vez disso, julgar os dados produzidos por eles como sendo honestos e válidos sem conhecimento de fora da rede.

4.2 O fundamento da Proof of Origin: Bound Witnesses

A **Proof of Origin** se baseia no conceito de **Bound Witness**. Dado que uma fonte de dados não confiável usada para resolver um contrato digital (um **oracle**) não é útil, podemos aumentar significativamente a **certeza** dos dados fornecidos primeiramente estabelecendo a existência de uma prova de localização bidirecional. A **heurística** de localização bidirecional principal é a proximidade, já que ambas as partes podem validar a ocorrência e o alcance de uma alteração co-assinando a interação. Isso permite uma prova de conhecimento zero de que os nós estavam próximos um do outro.

Então, precisamos determinar a certeza de que um nó de testemunho de oracle em um sistema **sem verificação de confiabilidade** reuniu os dados que está compartilhando. Em um sistema sem verificação de confiabilidade, um nó de testemunho pode produzir dados falsos devido a defeito ou corrupção. Dados inválidos podem ser

detectados e removidos facilmente se saírem da faixa permitida para essa heurística. Dados válidos, mas incorretos (isto é, dados falsos) são muito mais difíceis de detectar.

4.3 Heurísticas de localização unidirecional x bidirecional

A maioria dos dados relacionados ao mundo físico (uma **heurística**) é unidirecional. Isso significa que o elemento sendo medido não pode ser medido de volta, tornando os dados heurísticos unidirecionais muito difíceis de validar. Uma heurística bidirecional é aquela em que o elemento medido pode reportar sua própria medida de volta para a outra parte, o que torna a validação possível. Localização é uma heurística rara por poder ser bidirecional, com dois nós periféricos reportando um sobre o outro. **Um exemplo disso no mundo real seria o seguinte: duas pessoas próximas uma à outra tirando uma selfie, imprimindo uma cópia para cada uma e assinando a selfie. Esse processo daria uma Proof of Proximity a ambas as partes. A única maneira dessas duas pessoas terem conseguido esses "dados" seria terem estado juntas na mesma localização.**

A seguir, vamos discutir efeitos de rede: imagine um sistema no qual se espera que cada nó periférico produza essas "selfies" constantemente ao longo do percurso e as armazenem em uma pasta. Também se espera que elas mantenham essa pasta em ordem sequencial de tempo e nunca possam ser apagadas. Isso estabelece um registro de proximidade para cada nó periférico que possa ser objeto de referência com os registros de outros nós periféricos.

4.4 Nós não periféricos

Todos os nós são considerados "testemunhos", inclusive nós de Bridge, retransmissão, armazenagem e análise. Isso permite que todos os dados retransmitidos de um nó ao seguinte sejam vinculados. Esse é o conceito de **Bound Witness**.

4.5 Referência

Analisar cada conjunto de "selfies" produzidas e encadeadas juntas pelos nós periféricos permite que o sistema produza a **Best Answer** a partir da proximidade relativa de todos os nós que estejam na rede. Se cada nó reportar honesta e precisamente, o mapeamento de todas as posições relativas dos nós periféricos atingirá **certeza** e precisão máximas possíveis: 100%. Inversamente, se cada nó for desonesto ou defeituoso, a **certeza** e a precisão podem aproximar-se do mínimo de 0%.

Com um conjunto de dados reportados e uma consulta quanto a uma posição relativa de um dos nós periféricos, pode-se gerar uma aproximação da posição juntamente com coeficientes de certeza e precisão.

Com o mesmo conjunto de dados e o mesmo algoritmo de análise, todos os cálculos devem chegar à mesma aproximação de posição e aos mesmos coeficientes de certeza e precisão.

4.6 Diagrama

S' e S" (Figura 1.) são **Sentinels** (nós periféricos) que coletam heurísticas. Quando em contato, partilham dados **heurísticos** e chaves públicas. Ambos constroem um registro completo da interação e assinam a interação resultante. Esse registro assinado torna-se o próximo lançamento em ambos os seus registros locais (16 para S' e 3 para S"). Essa ação vincula esses dois testemunhos como estando próximos entre si.

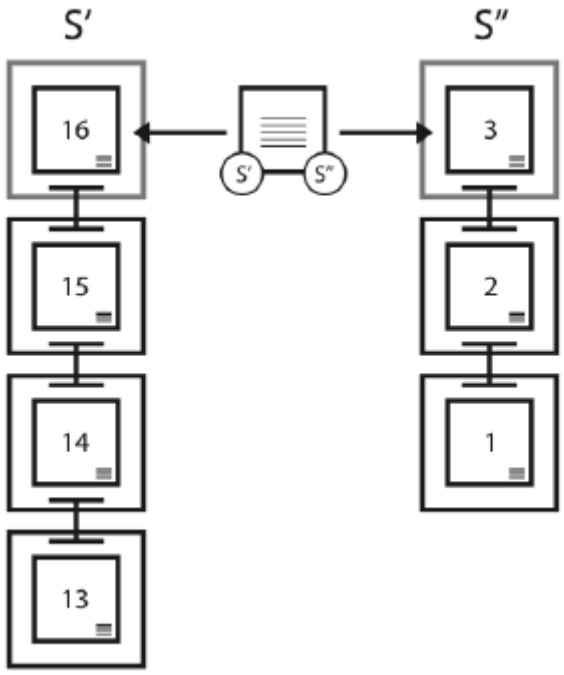

Figura 1. Exemplo de vinculação de testemunhos entre dois Sentinels

4.7 Origin Chains

Cada origem mantém seu próprio registro e o assina para formar uma **Proof of Origin Chain**. Uma vez que as informações da Proof of Origin Chain são compartilhadas, elas se tornam permanentes. Isso ocorre porque a bifurcação que acontece após o compartilhamento termina a cadeia e faz com que todos os dados futuros do testemunho sejam tratados como se fossem de um novo testemunho. Para gerar um link em uma Proof of Origin Chain, a origem gera um par de chaves pública/privada. Ela então assina o bloco anterior e o próximo com o mesmo par após incluir a chave pública em ambos os blocos. Imediatamente após a assinatura, a chave privada é deletada. Com a deleção imediata da chave privada, o risco de que uma chave seja roubada ou reutilizada é minimizado de forma significativa.

Proof of Origin Chains são a chave para verificar se os registros fluindo para a **XYO Network** são válidos. Uma ID exclusiva por fonte de dados não é praticável porque pode ser forjada. A assinatura com chave privada não é praticável porque a maioria das partes da XYO Network são difíceis ou impossíveis de proteger fisicamente, assim, o potencial de que um indivíduo mal-intencionado roube uma chave física é muito grande. Para resolver isso, a XYO Network usa **Transient Key Chaining**. O benefício disso é o seguinte: é impossível falsificar a cadeia de origem dos dados. No entanto, uma vez que a cadeia seja quebrada, ela é quebrada para sempre e não pode ser continuada, tornando-a uma ilha.

Cada vez que um registro **heurístico** é tratado na XYO Network, o recebedor anexa a sua própria **Proof of Origin**, o que torna mais longa a **Proof of Origin Chain** e gera uma **Proof of Origin Intersection**. Proof of Origin Chains e Proof of Origin Intersections são os principais indicadores usados por **Diviners** para verificar a validade de registros. A equação para uma Reputação de Registro é, efetivamente, qual porcentagem da XYO Network estava envolvida na associação da Proof of Origin Ball a ela. Em teoria, se 100% dos registros da XYO Network forem ligados a Proof of Origin e então totalmente analisados, a chance de serem válidos é de 100%. Se 0% dos registros da XYO Network estiverem disponíveis para análise, a validade cai para 0%.

Para maior segurança, a chave pública para um Chain Link só é fornecida quando o segundo lançamento para ele é disponibilizado. Isso também permite que o intervalo de tempo entre lançamentos ou outros dados seja armazenado no link anterior ou no próximo.

4.8 Origin Chain Score

A **Origin Chain Score** é calculada conforme segue (algoritmo padrão):

- PcL = Comprimento da **Proof of Origin Chain**
- PcD = Dificuldade da Proof of Origin Chain
- Pc' Pc" O = Coincidência da Proof of Origin Chain para Pc' e Pc"

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

4.9 Origin Tree

Uma **Origin Tree** é usada para calcular a validade aproximada de uma resposta. Usa os dados coletados para gerar uma Ideal Tree, que é a árvore que melhor se enquadra nesses dados para uma dada resposta reafirmada. Se o nó N estiver situado na localização X,Y,Z,T, o erro em todos os dados do conjunto terá que conter um certo valor. Para computar esse erro, calcularíamos a DISTÂNCIA MÍN, MÁX, MEDIANA, e DISTÂNCIA MÉDIA DA MEDIANA.

Dado um conjunto S de todas as pontuações s, uma Dificuldade de **Proof of Origin Chain** PcD e um fator de erro, a **Best Answer** é determinada conforme segue:

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

Em outras palavras, a resposta reafirmada que tiver a Pontuação de **Best Answer** mais alta é a Best Answer. Usando a Proof of Origin Tree podemos identificar e podar árvores impossíveis (valores extremos).

4.10 Transient Key Chaining

Uma série de pacotes de dados podem ser encadeados juntos usando chaves privadas temporárias para assinar dois pacotes sucessivos. Quando a chave pública pareada com a chave privada é incluída nos pacotes de dados, o recebedor pode verificar se ambos os pacotes foram assinados pela mesma chave privada. Os dados do pacote não podem ser alterados sem violar a assinatura, presumindo-se que os pacotes assinados não foram alterados por terceiros, como um Bridge ou nó de armazenagem.

4.11 Profundidade do link

No mínimo, um nó gera um novo par de chaves pública/privada para cada link na **Proof of Origin Chain**, que tem uma Profundidade de Link igual a 1. Pode haver N lançamentos na tabela de links de um dado Lançamento de Registro, sendo que cada lançamento especifica a distância no futuro quando a parte dois do link será adicionada. Não há dois links com a mesma ordem de magnitude em uma escala de base 2. Por exemplo, o lançamento [1,3,7,12,39] seria permitido, mas [1,3,7,12,15] não.

O link de profundidade 1 é criado, usado e deletado quando o bloco anterior é publicado. No entanto, links com profundidade acima de 1 têm seu par gerado à medida que o bloco anterior estiver sendo assinado, e a segunda assinatura ocorre somente N blocos mais tarde, depois que a chave privada é deletada. Por essa razão, links com profundidade acima de 1 sempre são considerados menos seguros do que links com profundidade 1, mas podem ser usados para melhorar o desempenho e reduzir perdas de dados à custa da segurança.

4.12 Ordem fixa

O principal elemento na determinação da sequência de registros é a ordem em que foram reportados. Dado que não é possível que um dispositivo altere a ordem de qualquer registro assinado com **Proof of Origin**, uma ordem absoluta pode ser estabelecida observando todos os registros coletivamente.

4.13 Penúltima publicação

Um método fundamental para estabelecer a **Proof of Origin** baseia-se no fato de que um **Sentinel** sempre reporta seu penúltimo bloco sem reportar o último bloco. Isso

permite que o último bloco tenha o link assinado para o seu predecessor como comprovação do link.

4.14 Links vazios

Para tornar uma **Proof of Origin Chain** mais segura, é necessário que a cadeia seja atualizada não mais de uma vez a cada dez segundos e não menos de uma vez a cada sessenta minutos. Caso não haja dados novos disponíveis, um bloco vazio será adicionado à cadeia.

4.15 Diagrama

Como o tempo viaja da esquerda para a direita (Figura 2.), a **Proof of Origin Chain** que está sendo construída fica mais longa. Em determinado momento, o produtor da cadeia só fornecerá ao chamador os lançamentos com limites obscurecidos, esperando pela segunda assinatura do lançamento antes de disponibilizá-lo. Por exemplo, na terceira coluna somente os lançamentos 2 e 1 serão retornados como sendo parte da cadeia.

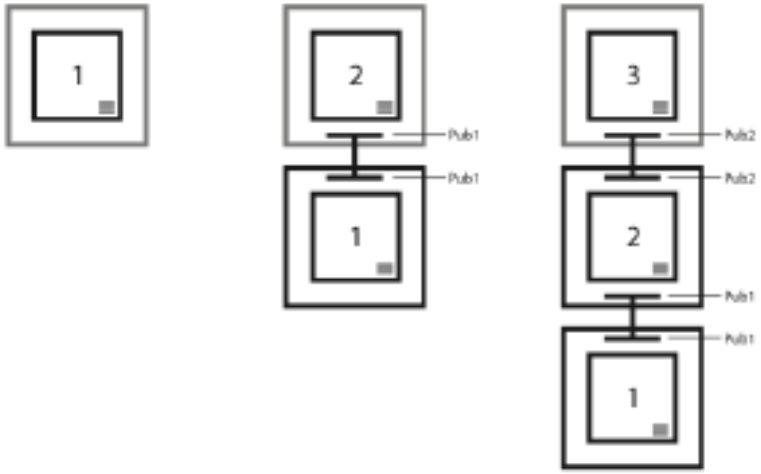

Figura 2: Exemplo de inclusão de link em uma Proof of Origin Chain

4.16 Resumo

Dada uma série de pacotes de dados que sejam assinados em pares sequenciais com chaves privadas temporárias e incluam as chaves públicas pareadas, pode-se determinar com **certeza** absoluta que os pacotes vêm da mesma origem.

---

5 Considerações de segurança

5.1 Ataque de falsos Diviners

Um conjunto de assinaturas digitais é enviado ao **contrato inteligente** XYO porque o contrato precisa verificar a integridade do **Diviner** que enviou a resposta. O contrato pode então verificar os outros Diviners que assinaram essa lista com um alto intervalo de confiança. Sem isso, o oracle retransmissor seria a única fonte de falhas e riscos no sistema.

5.2 Ataques de DDoS nos Sentinels

Outro ataque a considerar é uma Negação Distribuída de Serviço (DDoS) entre nós Sentinel em uma região específica. Um invasor poderia tentar estabelecer um grande número de conexões a Sentinels para impedi-los de retransmitir as informações corretas ou quaisquer informações ao **Bridge**. Podemos contornar esse problema exigindo que um pequeno enigma criptográfico seja resolvido por quem quer que tente se conectar a um Sentinel. Como uma consulta não envolverá um número muito grande de conexões a Sentinels, isso não imporá uma carga pesada ao sistema de retransmissão XYO e exigirá que o invasor gaste uma grande quantidade de recursos para executar uma DDoS bem-sucedida contra a nossa rede. A qualquer momento, uma **Proof of Origin Chain** pode ser verificada por qualquer pessoa por ser armazenada na **XYOMainChain**. Isso assegura que se uma entidade única ao longo da cadeia for comprometida, a precisão da resposta à consulta (**Origin Chain Score**) será reduzida a zero.

---

6 Especificações dos Tokens XYO

Os **oracles** representam uma porção significativa das necessidades de potência e infraestrutura para aplicações descentralizadas, com o foco principal na conectividade e na agregação de oracles confiáveis. Acreditamos na necessidade de um sistema de oracles **sem verificação de confiabilidade** totalmente descentralizado para que as aplicações descentralizadas atinjam o potencial máximo.

6.1 Criptoeconomia da XYO Network

Usamos Tokens XYO para incentivar o comportamento desejado de proporcionar **heurística** precisa e confiável. Os Tokens XYO podem ser pensados como o "combustível" necessário para interagir com o mundo real a fim de verificar as coordenadas XY de um objeto especificado.

O processo funciona assim: O portador de um token primeiro faz uma consulta à **XYO Network** (por exemplo: "*Onde está o pacote do meu pedido de eCommerce com endereço XYO 0x123456789...?*"). A consulta é enviada a uma fila, na qual espera para ser processada e respondida. Um usuário pode estipular o nível de confiança desejado e o preço do combustível XYO na criação da consulta. O custo de uma consulta (em Tokens XYO) é

determinado pelo volume de dados necessários para proporcionar uma resposta à consulta e pela dinâmica de mercado. Quanto mais dados forem necessários, mais cara será a consulta e mais alto será o preço do combustível XYO. Consultas à XYO Network podem ser muito longas e caras. Por exemplo, uma empresa de transporte rodoviário e logística pode perguntar à XYO Network "*Qual é a localização cada veículo específico da nossa frota?*"

Assim que o portador do Token XYO consultar a XYO Network e pagar o combustível necessário, todos os **Diviners** trabalhando na tarefa recorrerão aos **Archivists** relevantes para recuperar os dados pertinentes necessários para responder à consulta. Os dados apresentados são derivados dos **Bridges**, que originalmente coletaram tais dados dos **Sentinels**. Sentinels são, essencialmente, os dispositivos ou sinais que verificam a localização de objetos. Abrangem entes como rastreadores Bluetooth, rastreadores GPS, rastreamento de geolocalização integrado a dispositivos IoT, tecnologia de rastreamento por satélite, leitores de códigos QR, leitores RFID e muitos outros. A XY Findables criou e lançou o seu negócio de Bluetooth e GPS de consumo, o que a permitiu testar e processar a heurística de localização do mundo real. Todos os esforços no desenvolvimento do negócio de consumo da XY Findables serviram para ajudar significativamente na concepção do Protocolo Blockchain da XYO Network.

Se os dados fornecidos por um dispositivo Sentinel (como um Marcador Bluetooth) forem usados para responder uma consulta, todos os quatro componentes envolvidos na transação recebem uma parte do combustível XYO pago pelo portador do token: o Diviner (que pesquisou a resposta), o Archiver (que armazenou os dados), o Bridge (que transmitiu os dados) e o Sentinel (que registrou os dados de localização). A distribuição do combustível entre três dos quatro componentes da XYO Network é feita sempre na mesma proporção. A exceção se refere aos Diviners, cujo envolvimento no processo de proporcionar uma resposta é mais amplo. O combustível é distribuído uniformemente em cada componente.

6.2 Recompensas por independência

Os dispositivos de coleta de localização são os blocos fundamentais da rede, e um dispositivo único pode atuar como um ou mais dos quatro componentes do sistema. No entanto, seria raro, especialmente em uma **XYO Network** grande, que os dispositivos atuassem como mais de dois desses componentes. Além do mais, um registro blockchain que tenha **Proof of Origin** mais independente será mais considerado, então há uma penalidade **criptoeconômica** para um dispositivo que atue como múltiplos componentes.

6.3 Recompensas por integridade estacionária

Os **Sentinels** na **XYO Network** recebem um coeficiente de estacionariedade pela quantidade de movimento ao longo de todo o ciclo de vida. Quanto menos um Sentinel se move em um período de tempo, mais confiáveis são os seus dados. Os **Archivists**

acompanham esses coeficientes de estacionariedade ao considerar a quais Sentinels encaminhar consultas.

6.4 Incentivando o uso de tokens

Um sistema no qual portadores de tokens são encorajados a não usar seus tokens cria um problema de longo prazo para a economia subjacente. Cria um ecossistema com lojas de valor muito escassas e desencadeia um impulso natural de inventar razões para não usá-los, em vez de estimular a utilidade e a liquidez.

O problema da maioria dos incentivos criptoeconômicos é que o foco fica excessivamente direcionado aos mineradores de tokens (como **Sentinels**, **Bridges**, **Archivists**, **Diviners**) e nunca aos usuários de tokens. O Token XYO leva ambos em consideração.

O modelo dos Tokens XYO incentiva o minerador a não apenas fornecer dados precisos, mas também a saber quando não fornecer nenhum dado. O usuário final é recompensado para transacionar mais quando a liquidez da rede é baixa do que quando a liquidez da rede é alta. Assim, o ecossistema dos Tokens XYO tem capacidade para permanecer bem equilibrado, fluido e robusto.

6.5 Especificações dos Tokens XYO

A venda pública de tokens tem uma estrutura de preços escalonada que começa em 1 ETH: 100.000 XYO e atinge um máximo de 1 ETH: 33.333 XYO. Os dados relativos à nossa estrutura de preços baseada em volume e tempo serão anunciados em breve.

Plataforma de contratos inteligentes: Ethereum

- Tipo de contrato: ERC20
- Token: XYO
- Nome do token: Token utilitário da **XYO Network**
- Endereço do token: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Emissão total: Finita e culminando no valor atingido após a Venda Principal de Tokens
- Valor emitido durante a venda principal: ilimitado
- Tokens não vendidos e não alocados: queimados após o evento de venda de tokens. Não serão gerados mais Tokens XYO após o final da Venda Principal.

---

7 Casos de uso da XYO Network

De objetivas a complexas, o uso da XYO Network tem inúmeras aplicações que abrangem uma profusão de setores. Por exemplo, considere uma empresa de eCommerce que poderia

oferecer serviços de pagamento contra entrega aos seus clientes especiais. Para conseguir oferecer esse serviço, a empresa de eCommerce potencializaria a XYO Network e a Plataforma XY (que usa Tokens XYO) para redigir um **contrato inteligente** (isto é, na plataforma da Ethereum). Então, a XYO Network poderia rastrear a localização do pacote sendo enviado ao consumidor ao longo de cada etapa individual do processo; da prateleira do depósito ao despachante de envio e até a casa do consumidor, assim como cada local entre essas etapas. Isso poderia possibilitar que varejistas e sites de eCommerce constatassem, **sem verificação de confiabilidade**, que o pacote não apenas chegou à casa do cliente, mas também foi recebido em segurança dentro da casa. Quando for confirmado que o pacote está na casa do cliente (definido e verificado por coordenadas XY específicas), o envio é considerado concluído e o pagamento ao vendedor é liberado. Assim, a integração de eCommerce da XYO Network habilita a capacidade de proteger o comerciante contra fraudes e assegura que os consumidores só paguem por mercadorias que cheguem às suas casas.

Considere uma integração inteiramente diferente da XYO Network com um site de avaliação de hotéis cujo problema atual é: muitas vezes, as avaliações não são confiáveis. Naturalmente, os proprietários de hotéis são incentivados a melhorar tais avaliações a qualquer custo. E se fosse possível dizer com toda **certeza** que alguém estava em San Diego, voou para um hotel em Bali, ficou lá por duas semanas, voltou a San Diego e então escreveu uma avaliação sobre a estadia no hotel em Bali? A avaliação teria uma reputação muito alta, especialmente se fosse escrita por um avaliador frequente que tenha escrito muitas avaliações com dados de localização verificados.

---

8 Expansão da XYO Network

Felizmente, temos uma empresa de consumo que conseguiu construir essa rede no mundo real, com mais de um milhão (1.000.000) de dispositivos Bluetooth e GPS ao redor do mundo. A maioria das redes de localização não consegue alcançar essa fase e atingir a massa crítica necessária para construir uma rede abrangente. No entanto, a rede **Sentinel** que estabelecemos é apenas o ponto de partida. A **XYO Network** é um sistema aberto ao qual qualquer operador de dispositivos de localização pode se conectar e começar a ganhar Tokens XYO.

De modo geral, quanto maior a cardinalidade dos Sentinels na XYO Network, mais confiável será a rede. Para expandir ainda mais a rede, a XYO Network está fazendo parcerias com outras empresas para expandir sua rede de Sentinels além da sua própria rede de marcadores XY.

9 Agradecimentos

Este White Paper é o produto de um inspirador esforço coletivo possibilitado pelas pessoas a seguir, que acreditaram na nossa visão: Raul Jordan (Harvard College, pesquisador Thiel e consultor da **XYO Network**), por suas contribuições para tornar o nosso White Paper mais conciso e por ajudar-nos a comunicar os detalhes técnicos ao mundo com elegância. Agradecemos a Christine Sako pela ética de trabalho e atenção extraordinária aos detalhes na revisão. A uniformidade estrutural e as melhores práticas observadas no nosso White Paper são frutos dos esforços de Christine. Agradecemos a Johnny Kolasinski pela pesquisa e compilação dos casos de uso aplicáveis. Finalmente, agradecemos a John Arana pela revisão cuidadosa e pela análise criativa dos nossos esforços.

Referências

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

[2] Karapetsas, Lefteris. Sikorka.io. http://sikorka.io/files/devcon2.pdf. Xangai, 29 de setembro de 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof.of.location/. 17 de setembro de 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 de fevereiro de 2014.

Glossário

precisão Uma medida de confiança de que um ponto ou heurística de dados está dentro de uma determinada margem de erro.

Archivist Um Archivist armazena heurística como parte do conjunto de dados descentralizados estabelecido com a meta de armazenar todos os registros históricos, mas sem essa exigência. Mesmo que alguns dados sejam perdidos ou fiquem temporariamente indisponíveis, o sistema continua a funcionar, embora com precisão reduzida. Archivists também indexam registros de modo que possam retornar uma sequência de dados de registros, se necessário. Archivists armazenam somente dados brutos e são pagos somente pela recuperação dos dados. A armazenagem sempre é grátis.

Best Answer Definimos Best Answer como a única resposta, dentre uma lista de Answer Candidates, que retorna a pontuação de validade mais alta e tem uma pontuação de precisão mais alta do que a precisão mínima requerida.

Best Answer Algorithm Um algoritmo usado para gerar Best Answer Scores quando um Diviner escolhe uma resposta. A XYO Network permite a adição de algoritmos especializados e possibilita que o cliente especifique qual algoritmo usar. É necessário que esse algoritmo resulte na mesma pontuação quando executado em qualquer Diviner, considerando o mesmo conjunto de dados.

Bound Witness Bound Witness é um conceito atingido pela existência de uma heurística bidirecional. Dado que uma fonte de dados sem verificação de confiabilidade não é útil para o uso de resolução de contratos digitais (um oracle), há um aumento substancial na certeza dos dados fornecidos devido ao estabelecimento de uma heurística. A heurística de localização bidirecional principal é a proximidade, já que ambas as partes podem validar a ocorrência e o alcance de uma interação co-assinando a interação. Isso permite uma prova de conhecimento zero de que os nós estavam próximos um ao outro.

Bridge Um Bridge é um transcritor heurístico. Ele retransmite com segurança os registros heurísticos dos Sentinels para Diviners. O aspecto mais importante de um Bridge é que um Diviner pode ter certeza de que os registros heurísticos recebidos de um Bridge não sofreram nenhuma alteração. O segundo aspecto mais importante de um Bridge é que ele acrescenta um metadado de Proof of Origin adicional.

certeza Uma medida de probabilidade de que um ponto ou heurística de dados está isento de corrupção ou adulteração.

criptolocalização O reino da tecnologia de localização criptográfica.

criptoeconomia Uma disciplina formal que estuda protocolos que regulam a produção, a distribuição e o consumo de bens e serviços em uma economia digital descentralizada. A criptoeconomia é uma ciência prática que se concentra na elaboração e caracterização desses protocolos.

Diviner Um Diviner responde a uma dada consulta analisando dados históricos que tenham sido armazenados pela XYO Network. A heurística armazenada na XYO Network deve ter um nível alto de Proof of Origin para mensurar a validade e precisão da heurística. Um Diviner obtém e apresenta uma resposta julgando o testemunho baseado na Proof of Origin. Dado que a XYO Network é um sistema sem verificação de confiabilidade, os Diviners devem ser incentivados a fornecer análises de heurística honestas. Ao contrário dos Sentinels e Bridges, Diviners usam Proof of Work para acrescentar respostas à blockchain.

heurístico Um ponto de dados do mundo real relacionado à posição de um Sentinel (proximidade, temperatura, luz, movimento, etc.).

oracle Parte de um sistema DApp (aplicação descentralizada) responsável por resolver um contrato digital fornecendo uma resposta com precisão e certeza. O termo “oracle” tem origem na criptografia, significando uma fonte verdadeiramente aleatória (por exemplo: de um número aleatório). Proporciona o portão necessário entre uma criptoequação e o mundo além dela. Oracles alimentam contratos inteligentes com informações de fora da cadeia (o mundo real ou off-chain). Oracles são interfaces do mundo digital com o mundo real. Como exemplo mórbido, considere um contrato para um testamento. Os termos de um testamento são executados por ocasião da confirmação de que o testador faleceu. Um serviço oracle poderia ser elaborado para desencadear um testamento compilando e agregando dados relevantes de fontes oficiais. Então, o oracle poderia ser usado como alimentação ou ponto final para que um contrato inteligente buscasse verificar se a pessoa faleceu ou não.

Origin Chain Score A pontuação atribuída a uma Origin Chain para determinar a sua credibilidade. Essa atribuição leva em consideração o comprimento, entrelaçamento, coincidência e redundância.

Origin Tree Um conjunto de dados de lançamentos de registros tomados de diversas Origin Chains para estabelecer a origem do lançamento de um registro heurístico com um nível de certeza especificado.

Proof of Origin Proof of Origin é a chave para verificar se os registros fluindo para a XYO Network são válidos. Uma ID exclusiva por fonte de dados não é praticável porque pode ser forjada. A assinatura com chave privada não é praticável porque a maioria das partes da XYO Network são difíceis ou impossíveis de proteger fisicamente, assim, o potencial de que um indivíduo mal-intencionado roube uma chave física é muito

grande. Para resolver isso, a XYO Network usa Transient Key Chaining. O benefício disso é que é impossível falsificar a cadeia de origem dos dados. No entanto, uma vez que a cadeia seja quebrada, ela é quebrada para sempre e não pode ser continuada, tornando-a uma ilha.

Proof of Origin Chain Uma Transient Key Chain que une uma série de lançamentos de registros heurísticos de Bound Witnesses.

Proof of Work Proof of Work é um dado que satisfaz certos requisitos, é difícil de produzir (isto é, oneroso, demorado), mas fácil de ser verificado por terceiros. A produção de Proof of Work pode ser um processo aleatório com baixa probabilidade de geração, de modo que, em geral, um processo rigoroso de tentativa e erro é necessário antes que uma Proof of Work válida seja criada.

Sentinel Um Sentinel é um testemunho heurístico. Ele observa os dados heurísticos e atesta a certeza e a precisão desses dados produzindo registros cronológicos. O aspecto mais importante de um Sentinel é que os Diviners podem comprovar que os registros por ele produzidos vieram da mesma fonte, adicionando a eles um Proof of Origin.

contrato inteligente Um protocolo criado por Nick Szabo antes do Bitcoin, supostamente em 1994 (razão pela qual algumas pessoas acreditam que ele é Satoshi Nakamoto, o inventor místico e desconhecido da Bitcoin). A ideia por trás dos contratos inteligentes é codificar um acordo legal em um programa para que computadores descentralizados executem seus termos, sem interpretação ou interferência humana nesses contratos. Os contratos inteligentes combinam dinheiro (por exemplo, Ether) e contratos no mesmo conceito. Considerando que os contratos inteligentes são deterministas (como os programas de computador) e totalmente transparentes e legíveis, são uma forma poderosa de substituir intermediários e corretores.

Transient Key Chain Uma Transient Key Chain liga uma série de pacotes de dados usando Transient Key Cryptography.

trustless sem verificação de confiabilidade Uma característica em que todas as partes de um sistema podem chegar a um consenso sobre qual é a verdade canônica. O poder e a confiança são distribuídos (ou compartilhados) entre as partes interessadas da rede (por exemplo, desenvolvedores, mineradores e consumidores), em vez de concentrados em um único indivíduo ou entidade (por exemplo, bancos, governos e instituições financeiras). Esse é um termo comum que pode ser facilmente mal interpretado. As Blockchains, na verdade, não eliminam a confiança. Elas minimizam a quantidade de confiança exigida de cada agente no sistema. Isso se dá pela distribuição da confiança entre os diferentes agentes por meio de um jogo econômico que os incentiva a cooperar com as regras definidas pelo protocolo.

XY Oracle Network XYO Network

XYO Network XYO Network significa “XY Oracle Network”. É composta por todo o sistema de componentes/nós habilitados para a XYO, incluindo Sentinels, Bridges, Archivists e Diviners. A função primária da XYO Network é atuar como um portal por meio do qual contratos inteligentes podem ser executados mediante confirmações de geolocalização no mundo real.

XYOMainChain Uma blockchain imutável na XYO Network que armazena transações de consultas juntamente com os dados coletados de Diviners e sua pontuação de origem associada.