Das Whitepaper des XYO Network: Das Proof-of-Origin-basierte, kryptographische Ortsdaten-Netzwerk

Arie Trouw *, Markus Levin †, Scott Scheper ‡

Januar 2018

Kurzfassung

Mit der zunehmenden Existenz von verknüpften, ortsdatenabhängigen Technologien, sind unsere Privatsphäre und Sicherheit besonders von der **Genauigkeit** und Validität von Ortsdateninformationen abhängig. Mehrere Versuche wurden unternommen, um die Notwendigkeit zentralisierter Stellen, welche den Fluss von Ortsdaten kontrollieren, zu eliminieren, aber alle diese Versuche waren von der Integrität der Geräte abhängig, die diese Daten in der realen Welt sammelten. Unser Vorschlag ist ein **vertrauensfreies**, kryptographisches Ortsdatennetzwerk, dass auf einer neuartigen Formel beruht, die von einer Kette aus Zero-Knowledge-Beweisen beruht, um ein hohes Maß an Daten-Gewissheit der Ortsdateninformationen zu erzielen. Das XYO **Network (XY Oracle Network)** ist eine Abstraktion, die eine vielschichtige Ortsdatenverifizierung über viele Geräteklassen und Protokolle hinweg, ermöglicht. In ihrem Zentrum befinden sich zwei neuartige, kryptographische Mechanismen, die als **Proof of Origin** & **Bound Witness** bekannt sind, und mithilfe derer heute die Leistungsfähigkeit der Blockchain-Technologie und die Datensammlung aus der realen Welt in einem System mit direkten Anwendungen, zusammengefasst werden können.

1 Einleitung

Mit der Ankunft Blockchain-basierter, **vertrauensfreier Smart Contracts**, nimmt die Notwendigkeit von Orakel-Diensten, die das Ergebnis eines Vertrags überwachen, bedeutend zu. Die meisten gegenwärtigen Umsetzungen von Smart Contracts verlassen sich auf einen einzelnen oder angesammelten Satz maßgebender Orakel, um das Ergebnis des Vertrags festzulegen. Wenn sich beide Parteien über die Maßgeblichkeit und Unkorrumpierbarkeit des bestimmten Orakels einigen können, ist dies ausreichend. In vielen Fällen existiert ein geeignetes Orakel jedoch nicht, oder das Orakel kann aufgrund von möglichen Fehlern oder Korruption nicht als maßgeblich angesehen werden.

Ortsdatenorakel fallen in diese Kategorie. Die Bestimmung der Ortsdaten eines Gegenstands in der körperlichen Welt hängt von Berichterstattungs-, Weiterleitungs-, Aufbewahrungs- und Verarbeitungskomponenten des entsprechenden Orakels ab, die alle Fehlerquellen sein und korrumpiert werden können. Risiken beinhalten Datenmanipulation, Datenverunreinigung, Datenverlust und Kollusion.

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

Es existiert daher folgendes Problem: **Sowohl die Gewissheit als auch die Genauigkeit von Ortsdaten werden, durch das Nichtvorhandsein eines vertrauensfreien, dezentralisierten Ortsdaten-Orakels, negativ beeinflusst.** Plattformen wie Ethereum und EOS sind bereits umfangreich hinsichtlich ihrer Fähigkeit, Interaktionen sicher online zu vermitteln, genutzt worden, wobei die am häufigsten genutzten Anwendungen treuhänderische Tätigkeit bei der Mittelbeschaffung in Form von ICO umfassten. Aufgrund verrauschter und in ihrer Integrität korrumpierbarer Informationskanäle, hat sich bisher jedoch jede Plattform ausschließlich auf die Online-Welt konzentriert und nicht auf die körperliche Welt.

Das XYO Network auf ein Konzept hingearbeitet, dass es Entwicklern, wie denen, die Smart Contracts für Blockchain-Plattformen schreiben, ermöglicht, mit der realen Welt zu interagieren, als wäre sie eine Programmierschnittstelle. Das **XYO Network** ist das weltweit erste Orakel-Protokoll, dass es zwei Parteien ermöglicht, in der realen Welt Transaktionen ohne eine zentralisierte Drittpartei durchzuführen. Unsere Abstraktionen erlauben es uns, Ortsdatenverifizierung für Entwickler vertrauensfrei zu machen, wodurch ein neuartiges Protokoll mit Anwendungsmöglichkeiten entsteht, die bisher nicht möglich waren.

Das XYO Network wird auf einer bestehenden Infrastruktur aus über 1.000.000 im Umlauf befindlichen Geräten aufgebaut, die durch das verbraucherorientierte Findables-Geschäft verbreitet wurden. Die Bluetooth- und GPS-Geräte von XY ermöglichen es gewöhnlichen Verbrauchern, physische Ortungssender an Gegenständen zu befestigen, die sie nachverfolgen wollen (wie etwa Schlüssel, Gepäck, Fahrräder und sogar Haustiere). Wenn Sie einen solchen Gegenstand verlegen oder verlieren, können sie seinen Standort genau bestimmen, indem sie den Ort über die Smartphone-Applikation bestimmen. In nur sechs Jahren hat das XYO Network eines der größten Bluetooth- und GPS- Verbrauchernetzwerke der Welt aufgebaut.

2 Historischer Hintergrund und frühere Ansätze

2.1 Proof of Location

Das Konzept der nachweisbaren Ortsdaten existiert seit den sechziger Jahren des vergangenen Jahrhunderts und kann sogar bis in die 1940er Jahre, mit bodenstationären Funknavigationssystemen wie LORAN [1], zurückverfolgt werden. Heute gibt es Ortsdatendienste, die zur Erzeugung eines Proof of Location durch Triangulation und GPS-Dienste, verschiedene Verifikationsmedien übereinanderschichten . Diese Ansätze lassen jedoch die kritischste Komponente, der wir heutzutage in der Ortsdatentechnologie begegnen, außer Acht: Die Entwicklung eines Systems, dass gefälschte Signale entdeckt und die Manipulation von Ortsdaten unrentabel macht. Aus diesem Grund sind wir der Überzeugung, dass die erfolgreichste Krypto-Ortsdatenplattform diejenige sein wird, die am stärksten auf den Proof of Origin physischer Ortsdatensignale fokussiert ist.

Überraschenderweise wurde das Konzept der Blockchain-Anwendung zur Ortsdatenverifizierung erstmals 2016 bei der Ethereum DevCon 2 vorgestellt. Eingeführt wurde es von Lefteris Karapetsas, einem Ethereum Entwickler aus Berlin. Karapetsas Projekt, *Sikorka*, erlaubte es **Smart Contracts**, unter Verwendung von „*Proof of Presence*", augenblicklich in der realen Welt eingesetzt zu werden. Seine Anwendung der Verknüpfung von Ortsdaten und Blockchain-Technologie

war zunächst hauptsächlich auf Anwendungsbereiche der erweiterten Realität ausgerichtet, und er führte neuartige Konzepte ein, wie etwa PrüfAbfragen zum Nachweis von Aufenthaltsorten [2].

Am 17. September 2016 erschien der Begriff „*Proof of Location*" formell in der Gemeinschaft von Ethereum[3]. Es wurde dann durch den Ethereum Foundation Entwickler Matt Di Ferrante vertieft dargelegt:

> *"Vertrauenswürdige Proof of Location ist tatsächlich eines der am schwierigsten umzusetzenden Dinge. Selbst wenn man über eine große Anzahl an Teilnehmern verfügt, die ihre gegenseitigen Ortsdaten bestätigen können, gibt es keine Garantie, dass eine zukünftige Sybil-Attacke ausgeschlossen werden kann, und da man immer nur auf eine Mehrheit vertraut, ist das sein riesige Schwäche. Wenn man eine Art spezialisierter Hardware zur Verfügung hätte, die über manipulationssichere Technologie verfügte, sodass der private Schlüssel zerstört würde, sobald man versuchte das Gerät zu öffnen oder seine Firmware zu ändern, dann könnte man*

möglicherweise größere Sicherheit erzielen, gleichzeitig ist es aber auch wirklich nicht unmöglich, GPS-Signale zu manipulieren. Eine echte Implementation hierfür benötigte so viel Rückgriff und so viele verschiedene Datenquellen, um Genauigkeit zu garantieren, dass es ein sehr gut finanziertes Projekt sein müsste." [3]

—Matt Di Ferrante, Entwickler, Ethereum Foundation

2.2 Proof of Location: Schwachpunkte

Zusammengefasst kann Proof of Location als Kombination der leistungsstarken Eigenschaften der Blockchain, wie Zeit-Stempelung und Dezentralisierung, mit *, hoffentlich,* nur mühsam zu täuschenden Geräten verstanden werden. Wir bezeichnen den Bereich der kryptographischen Ortsdatentechnologie als „*Krypto-Ortsdaten*." Krypto-Ortsdatensysteme sind also mit einem Problem konfrontiert, dass mit dem von **Smart-Contracts** vergleichbar ist, deren **Orakel** Wahrheit aus einer einzigen Quelle beziehen (und damit eine einzige Fehlerquelle haben). Die Verwundbarkeit gegenwärtiger Krypto-Ortsdatentechnologien umkreist die Offchain-Geräte, die über die Ortsdaten eines Objekts berichten. Bei Smart Contracts ist die Offchain-Datenquelle ein Orakel. Beim **XYO-Network** bewegt sich die Offchain-Datenquelle in der realen Welt, in Form einer spezialisierten Form von Orakel namens **Sentinel**. Die bedeutendste Innovation im Zusammenhang mit dem XYO Network, dreht sich um identitätslose, ortsdatenbasierte Beweise, die den Komponenten unseres Systems zugrunde liegen, um ein **vertrauensfreies** Krypto-Ortsdatenprotokoll zu erstellen.

---

3 DAS XY Oracle Network

"Die Notwendigkeit eines schwer zu störenden Systems zur Ergänzung von GPS, ist seit Jahren bekannt. GPS ist außergewöhnlich genau und verlässlich, Stauungen, Täuschungen, Cyber-Attacken und andere Formen der Beeinträchtigung scheinen jedoch in Häufigkeit und Schwere zuzunehmen. Dies hat potentiell schwerwiegende Folgen für unser Leben und unsere wirtschaftliche Tätigkeit." [4]

—Dana Goward, President, RNT Foundation

3.1 Einleitung

Das Ziel des **XYO Network** ist es ein **vertrauensfreies**, dezentralisiertes System von Ortsdaten-**Orakeln** zu erstellen, das Angriffen widersteht und bei Abfragen zu verfügbaren Daten, Antworten mit höchstmöglicher Gewissheit produziert. Wir erreichen dies durch eine Reihe an Abstraktionen, die das Risiko gefälschter Ortsdaten, dank einer Kette von Zero-Knowledge-Beweisen entlang der Systemkomponenten, maßgeblich reduzieren.

3.2 Netzwerkübersicht

Unser System bietet einen Einstiegspunkt zu einem Protokoll vernetzter Geräte, die durch eine Kette kryptographischer Beweise, Ortsdaten mit hoher Gewissheit bereitstellen. Nutzer werden in der Lage sein, als „*Abfragen*" bekannte Transaktionen durchzuführen, um daraufhin bestimmte Ortsdaten von einer Blockchain-Plattform zu erhalten, die über **Smart Contract-**Funktionalität verfügt.[1] Aggregatoren des XYO Network hören dann die an den Vertrag gestellten Abfragen und beschaffen die mit der höchsten Genauigkeit

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter- party, Monax und andere – line

versehenen Antworten von einem dezentralisierten Netzwerk aus Geräten, welche kryptographische Beweise an diese Aggregatorenweiterleiten. Diese Aggregatorenspeisen dann diese Antworten in den Smart Contract ein, nachdem ein Konsens hinsichtlich der Antwort mit dem besten Wert erzielt wurde. Dieses Netzwerk von Komponenten ermöglicht es mit der größtmöglich überprüfbaren, **vertrauensfreien** Gewissheit zu bestimmen, ob sich ein Objekt zu einem gegebenen Zeitpunkt an einer bestimmten XY-Koordinate befindet.

Das XYO Network besteht aus vier Hauptkomponenten: **Sentinels** (Die Datensammler), **Bridges** (Die Weiterleiter der Daten), **Archivists** (Die Datenspeicherer), und **Diviners** (The Antworten-Aggregatoren). Sentinels sammeln Ortsdateninformationen über Sensoren, Sender und andere Mittel. Bridges übernehmen diese Daten von Sentinels und stellen sie den Archivists bereit. Archivists speichern die Daten, damit sie durch Diviner analysiert werden können. Diviner analysieren, von Archivists bereitgestellte Ortsdaten-**Heuristiken**, um Antworten auf Abfragen zu generieren und ihnen Werte entsprechend ihrer Genauigkeit zuzuordnen. Diviner leiten diese Antworten dann an den Smart Contract weiter (in dieser Hinsicht dienen Diviner dann als **Orakel**). Der Wert der Genauigkeit, bezeichnet als **Origin Chain Score**, wird durch eine Anzahl an Zero-Knowledge-Beweisen bestimmt, auch bekannt als **Proof of Origin Chain**. Diese Kette bestätigt zwei oder mehr Daten aus derselben Quelle, ohne zugrunde liegende Informationen zu enthüllen. Jede Komponente entlang des Wegs der Abfrage, generiert ihren eigenen Proof of Origin, der dann mit jeder Komponente an die Daten weitergeleitet werden, verkettet wird. **Proof of Origin** ist eine neuartige Formulierung, die eine Reihe kryptographischer Garantien entlang eines Pfads von Weiterleitungen innerhalb des Netzwerks bildet, um besonders vertrauenswürdige Daten aus der realen Welt zu schaffen. Diese **Proof of Origin Chain** umfasst das Vertrauen, dass wir in Ortsdaten haben können, bis hin zum ersten Gerät, das die Daten gesammelt hat. Wir werden im folgenden Abschnitt näher auf die Funktionsweise des Proof of Origin eingehen.

Zur Etablierung eines dezentralisierten Konsensmechanismus unter Diviners, vertraut das XYO Network auf eine öffentliche, unveränderliche Blockchain, die **XYOMainChain** , in der Abfragetransaktionen zusammen mit von Diviners gesammelten Daten und deren zugeordneten Ursprungswerten, gespeichert werden. Bevor wir in die Vorgehensweise des gesamten Systems eintauchen, definieren wir zunächst eindeutig die Aufgaben jeder Netzwerkkomponente.

3.2.1 Sentinels

Sentinels sind Ortsdaten-Zeugen. Sie beobachten **Heuristiken** und garantieren deren Gewissheit und Genauigkeit, durch Erzeugen temporärer Ledger. Der wichtigste Aspekt eines Sentinel ist, dass er Ledger erstellt, die anderen Komponenten die Sicherheit geben, aus derselben Quelle zu kommen. Sie erreichen dies, indem sie einer Weiterleitungskette kryptographischer Beweise **Proof of Origin** hinzufügen. Da es sich beim **XYO Network** um ein **vertrauensfreies** System handelt, müssen dem Sentinel zur Bereitstellung ehrlicher Ortsdateninformationen, Anreize geboten werden. Dies wird durch Kombination einer Reputationskomponente mit einer Entlohnungskomponente erreicht. Ein Sentinel wird mit XYO Network-Token (XYO) belohnt, wenn seine Informationen zur Beantwortung einer Abfrage verwendet wird. Um die Wahrscheinlichkeit seiner Entlohnung zu erhöhen, muss er Ledger anlegen, die mit denen ihrer gleichrangigen Teilnehmer übereinstimmen, und um sich selbst als Quelle der Ortsdateninformationen zu identifizieren, müssen sie einen Proof of Origin liefern.

3.2.2 Bridges

Bridges sind Protokollanten von Ortsdaten. Sie leiten Ortsdaten-Ledger sicher von **Sentinels** an **Archivists** weiter. Der wichtigste Aspekt einer Bridge ist, dass ein Archivist sicher sein kann, dass der von einer Bridge empfangene, **heuristische** Ledger in keiner Weise verändert wurde. Der zweitwichtigste Aspekt einer Bridge ist, dass sie einen zusätzlichen **Proof of Origin** hinzufügt. Da es sich beim **XYO Network** um ein **vertrauensfreies** System handelt, müssen der Bridge zur Bereitstellung ehrlicher Analysen von Heuristiken, Anreize geboten werden. Dies wird durch Kombination einer Reputationskomponente mit einer Entlohnungskomponente erreicht. Eine Bridge wird mit XYO Network-Token (XYO) belohnt, wenn die von ihr weitergeleiteten Informationen zur Beantwortung einer Abfrage verwendet werden. Um die Wahrscheinlichkeit ihrer Entlohnung zu erhöhen, muss sie Ledger anlegen, die mit

denen ihrer gleichrangigen Teilnehmer übereinstimmen und, um sich selbst als weiterleitende Stelle der Heuristik zu identifizieren, müssen sie einen Proof of Origin liefern.

3.2.3 Archivists

Archivists speichern Informationen, die sie von Bridges erhalten, in dezentralisierter Form und mit dem Ziel, der Speicherung aller historischen Ledger. Selbst wenn Daten verloren gehen oder zeitweise nicht verfügbar sein sollten, funktioniert das System weiterhin, nur mit verminderter Genauigkeit. Archivists indizieren außerdem Ledger, sodass sie bei Bedarf eine Kette von Ledgerdaten liefern können. Archivists speichern ausschließlich Rohdaten und werden ausschließlich für den Abruf der Daten und ihre anschließende Nutzung mit XYO Network-Token bezahlt. Die Speicherung erfolgt immer ohne Bezahlung.

Archivists sind miteinander vernetzt, sodass eine Abfrage an einen Archivist dazu führt, dass dieser Archivist andere Archivists nach Daten abfragt, die er selbst nicht vorhält. Ein Archivist kann optional alle Ledger-Informationen speichern, die er erhält. Dies wird höchstwahrscheinlich in zwei Typen von Archivists resultieren: solche in der Daten produzierenden Ecke der „Cloud“, und solche in der Daten konsumierenden Ecke der „Cloud“. Dazwischen wird es hybride Archivists geben. Die Wahl der Datenspeicherung wird nicht erzwungen, kann aber leicht über IPFS oder eine andere, dezentralisierte Speicherlösung, erreicht werden. Jedes Mal, wenn Daten von einem Archivist an einen anderen weitergegeben werden, wird zusätzlicher Proof of Origin hinzugefügt, damit Zahlungen nachverfolgt werden können, denn alle Archivists werden bezahlt. Für einen Datenabruf kann ein Mindestwert des Proof of Origin festgelegt werden, um die Validität zu erhöhen. Die Interessen von **Sentinels**, Bridges, und Archivists müssen aufeinander abgestimmt sein, um eine Datenschwemme zu verhindern.

3.2.4 Diviners

Diviners sind der komplexeste Bestandteil des **XYO Network**. Das übergreifende Ziel eines Diviners ist es, auf eine Abfrage hin die passenden Daten mit der höchsten Genauigkeit aus dem XYO Network zu beschaffen und an den Steller der Abfrage weiterzuleiten. Diviner befragen die entsprechende Blockchain-Plattform (d. h. Ethereum, Stellar, Cardano, IOTA usw.) zu Abfragen aus dem XYO **Smart Contract**. Durch direkten Austausch mit dem **Archivist**-Netzwerk, finden sie dann die Antwort auf die Abfrage, indem sie die Antwort mit dem höchsten Wert an **Genauigkeit**/Vertrauen auswählen. Sie erreichen dies durch Bewertung des Zeugen mit der besten **Proof-of-Origin-Chain**. Der jeweilige Diviner, der die Antwort mit dem höchsten Wert in der kürzesten Zeit beschafft hat, ist dann in der Lage, einen Block auf der Haupt-XYO-Blockchain (**XYOMainChain**), durch **Proof of Work** zu erstellen. Abfragen werden entsprechend Belohnungsumfang und Komplexität priorisiert. Je mehr XYO für eine Antwort bietet, umso höhere Priorität wird die Abfrage erhalten.

Andere Diviners erzielen einen Konsens hinsichtlich der Validität des Blocks und signieren den Block digital. Der Diviner, dessen Coinbase-Adresse sich im Block befindet, wird dann eine Transaktion an den Smart Contract senden, die sowohl die Antwort als auch deren Genauigkeitswert enthält. Er sendet darüber hinaus eine Liste der anderen Diviner-Signaturen, um zu verhindern, dass ein Angreifer, unter der Vorgabe, selbst ein Diviner zu sein, falsche Informationen an die Blockchain abgibt. Der Smart Contract kann dann die Integrität der Informationen, durch Überprüfung der Signaturenliste der Nutzdaten kontrollieren.

3.3 Durchgehende Funktionalität

Jetzt, da die Verantwortlichkeiten jeder Komponente dargelegt sind, wollen wir ein durchgehendes Beispiel betrachten, wie das System arbeiten wird:

1. **Sentinels sammeln Daten**

Sentinels sammeln Ortsdaten-**Heuristiken** der realen Welt und erstellen ihren eigenen **Proof of Origin** zur Angliederung an die übergeordneten Knoten

2. Bridges sammeln Daten von Sentinels

Bridges sammeln notwendige Daten von Sentinels online und fügen deren Kette Proof of Origin hinzu. Bridges stellen sich dann **Archivists** in ihrem Netzwerk zur Verfügung.

3. Archivists indizieren/stellen Daten von Bridges zusammen

Bridges senden kontinuierlich Daten an Archivists, von denen sie dann dezentralisiert und mit einem ortsdatenheuristischen Index versehen gespeichert werden.

4. Diviner nehmen Abfragen von Nutzern entgegen

Diviner suchen nach Abfragen, die an Etherum **Smart Contracts** gestellt wurden, und entscheiden sich dann, den Formulierungsprozess einer Antwort zu beginnen

5. Diviner sammeln Daten von Archivists

Diviner entscheiden dann eine Abfrage anzunehmen, indem Sie die entsprechend notwendigen Informationen aus dem Archivist-Netzwerk beziehen.

6. Diviner formulieren Antworten

Diviner wählen dann die **Best Answer** für die Abfrage aus dem Archivist-Netzwerk mit dem besten **Origin Chain Score**.

7. Diviner schlagen einen Block vor

Diviner schlagen dann einen Block auf der **XYOMainChain** vor, welcher die Inhalte der Antwort, die Abfrage und die XYO-Token (XYO), die durch **Proof of Work** bezahlt wurden, enthält. Andere Diviner des Netzwerks signieren dann digital die Inhalte des Blocks, dann wird die Nonce des Coinbase-Dviviners aktualisiert, um seinen Proof of Work im System darzustellen, sobald Konsens bezüglich der Validität des Blocks erreicht wurde.

8. Diviner liefern Antworten an den Abfragesteller

Diviner verpacken die Antwort, ihren Origin Chain Score und ihren Satz digitaler Signaturen und senden sie an eine Adapter-Komponente, die sicher mit dem XYO Smart Contract Verbindung herstellt. Der Adapter ist verantwortlich für die Sicherstellung, dass die Integrität des Diviners nicht kompromittiert wurde, und sendet den Satz digital signierter Antworten an den Smart Contract. Dies geschieht direkt nach Erstellung des Blocks. Der Coinbase Diviner wird dann für seine Bemühungen belohn.

9. Die Komponenten des XYO Network werden für ihre Arbeit belohnt

Die Komponenten entlang der Proof of Origin Chain werden für ihren jeweiligen Beitrag zur Beschaffung der Antwort der Abfrage belohnt. Sentinels, Bridges, Archivists und Diviner werden alle für ihre Arbeit belohnt.

Sollte dieselbe Abfrage mehrfach gestellt werden, dann können mehrere Antworten gegeben werden, da jede zu einem bestimmten Moment gegebene Antwort auf den, zu diesem Moment verfügbaren Heuristiken des Systems beruht. Die Lieferung einer Antwort an die Blockchain erfordert zwei Schritte. Zunächst, eine Analyse zur Bestimmung der **Best Answer** auf eine Abfrage. Wenn vom System mehrere Antworten generiert werden, dann vergleichen Knoten die Antworten und wählen in jedem Fall die bessere Antwort. Ein Beispiel für eine einfache Abfrage wäre: "*Wo befand sich ein Netzwerkknoten zu einem bestimmten Zeitpunkt in der Vergangenheit?*"

3.4 Blockchain als einzige Quelle der Wahrheit

Grundlegend transformieren **Diviners** einfach relative Daten zu absoluten Daten. Sie sind in der Lage das gesamte **Archivist**-Netzwerk zu erforschen, um eine absolute Antwort zu einer Abfrage im **XYO Network**, zu konkretisieren. Diviner sind auch die Knoten, die der **XYOMainChain** Blöcke vorschlagen und hinzufügen und für ihre **Proof of Work** belohnt werden. Da das Archivist-Netzwerk ein Speicher unverarbeiteter Daten ist und es sich bei der Blockchain um einen Speicher absoluter, verarbeiteter Daten handelt, wird das Netzwerk schließlich die neusten Daten der XYOMainChain verwenden können, anstatt sich auf teure Berechnung durch das Archivist-Netzwerk verlassen zu müssen.

Da die Blöcke der XYOMainChain die **Proof of Origin Chain** und Komponentengraphen speichern, die zur Beantwortung von Abfragen verwendet wurden, können zukünftige Diviner diese absoluten Daten, bei geringerer Bandbreitenausnutzung, zum Erhalt genauer Antworten verwenden. So wird die XYOMainChain schrittweise zur wichtigsten Quelle der Wahrheit des Systems. Ein Archivist-Netzwerk wird jedoch auch weiterhin benötigt werden, um die aktuellsten Informationen zu Ortsdaten-**Heuristiken**, die von **Sentinels** gesammelt wurden, aufzunehmen.

3.5 XYO Network-Rahmen zur Auswahl der Best Answer

Wir definieren die ***Best Answer*** als die einzige Antwort aus einer Liste von Antwortkandidaten, die den höchsten Wert an Gültigkeit liefert und einen höheren Wert an **Genauigkeit** aufweist, als den geforderten Mindestwert. Der Gültigkeitswert basiert auf dem **Origin Chain Score**. Dem System ist der höchste, aufgezeichnete Origin Score bekannt, der als 100-%-Wert dient, bis ein höherer Wert erreicht wird, welcher dann seinerseits zum neuen 100-%-Wert wird. Das **XYO Network** gestattet zur Bestimmung der Best Answer die Auswahl eines **Best Answer Algorithmus**. So wird Raum für zukünftige Forschung zu alternativen Algorithmen geschaffen.

Wenn Daten als minderwertig oder inkorrekt von einer Antwort ausgeschlossen werden, wird dies den Archivists mitgeteilt, sodass sie diese Daten von ihren dezentralisierten Speichern entfernen können.

3.6 Initiale Integration mit öffentlichen Blockchains

Das **XYO Network** wurde als eine Abstraktion entwickelt, die mit jeder **Smart Contract**-fähigen, öffentlichen Blockchain, wie Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano und anderen, kommunizieren kann. Zur Interaktion mit dem XYO Network können Anwender auf beispielsweise Etherum Abfragen an unseren XYO Smart Contract stellen und in XYO-Token (ERC20) bezahlen. Die Knoten in unserer eigenen XYO-Blockchain, als **Diviners** bezeichnet, würden kontinuierlich Ethereum zu diesen Abfragen befragen und in der nativen Währung unserer XYO Blockchain (auch als XYO-Tokens bezeichnet) belohnt werden. Zu einem zukünftigen Zeitpunkt werden wir einen Umtausch im Verhältnis von eins-zu-eins für Besitzer unserer ERC20-Token in die native Währung unserer Blockchain durchführen, um unsere Plattformen mit Transaktionsgebühren zu versehen, die Mikrozahlungsanforderungen unterstützen, welche für skalierbare IdD-Anwendungen notwendig sind. In diesen Fällen werden wir Anwendern gestatten, Abfragen direkt an unsere Blockchain zu stellen, anstatt durch öffentliche Smart Contracts zu agieren.

---

4 Proof of Origin

Mit einem physischen Netzwerk aus vertrauensfreien Knoten ist es möglich, die Gewissheit von Daten zu

bestimmen, die von Eckknoten, basierend auf Zero-Knowledge-Beweisen, bereitgestellt wurden, dass zwei oder mehr Daten aus derselben Quelle stammen. Kennt man die absoluten Ortsdaten wenigstens eines Knoten und verwendet die genannten Datensätze in Verbindung mit anderen, ähnlichen Datensätzen, dann lasen sich die absoluten Ortsdaten des anderen Knoten ableiten.

4.1 Einführung zu Proof of Origin

Traditionelle, **vertrauensfreie** Systeme verlassen sich auf private Schlüssel zur Unterzeichnung von Transaktionen oder Verträgen innerhalb eines Systems. Das funktioniert sehr gut, unter der Voraussetzung, dass der Netzwerkknoten welcher die betreffenden Daten unterzeichnet, physisch und virtuell sicher ist. Ist der private Schlüssel jedoch kompromittiert, versagt die Fähigkeit des Ursprungsnachweises.

Wenn wir vertrauensfreie Konzepte im Internet der Dinge anwenden, muss angenommen werden, dass die Eckknoten des Netzwerks physisch oder virtuell nicht sicher sind. So entsteht die Notwendigkeit, Eckknoten, ohne Verwendung eindeutiger IDs, zu identifizieren, und stattdessen die von ihnen produzierten Daten als ehrlich und gültig zu bewerten, ohne hierfür Wissen von außerhalb des Netzwerks zu verwenden.

4.2 Der Kern des Proof of Origin: Bound Witnesses

Proof of Origin beruht auf dem Konzept eines **Bound Witness**. Da eine nicht vertrauenswürdige Datenquelle zur Verwendung bei Erfüllung eines digitalen Vertrags (ein **Orakel**) nicht hilfreich ist, wird durch die Etablierung eines bidirektionalen Proof of Location eine substantielle Zunahme der Gewissheit der Daten erreicht. Die vorrangige bidirektionale Ortsdaten-**Heuristik** ist Nähe, da beide Parteien das Stattfinden und den Umfang einer Interaktion durch gemeinsames Signieren der Interaktion validieren können. Dies ermöglicht einen Zero-Knowledge-Beweis, dass sich die beiden Knoten in Nähe zu einander befanden.

Anschließend benötigen wir die Gewissheit, dass ein Orakel-Zeugenknoten innerhalb eines **vertrauensfreien** Systems, die von ihm geteilten Daten auch gesammelt hat. Ein Knoten kann in einem vertrauensfreien System, entweder durch Defekt oder durch Korruption, falsche Daten produzieren. Ungültige Daten können leicht entdeckt und entfernt werden, wenn sie sich außerhalb des für eine Heuristik erlaubten Wertebereichs befinden. Gültige, aber inkorrekte Daten (d.h. Falschdaten) sind viel schwieriger zu entdecken.

4.3 Unidirektionale gegen Bidirektionale Ortsdatenheuristiken

Die meisten mit der physischen Welt verbundenen Daten (**Heuristiken**) sind unidirektional. Das bedeutet, dass das vermessene Element nicht zurück vermessen kann, was die Validierung unidirektionaler Heuristiken sehr schwierig macht. Bei einer bidirektionalen Heuristik kann das vermessene Element seine eigene Messung an die andere Partei zurückmelden, was eine Validierung ermöglicht. Ortsdaten sind ungewöhnliche Heuristiken, da sie bidirektional sein können, wenn zwei Eckknoten zueinander Berichten. **Ein Beispiel hierfür, aus der realen Welt, wären zwei Personen, die sich nebeneinander befänden, jeweils ein Selfie aufnähmen, die Selfies dann für beide Parteien ausdruckten und die Drucke beide signieren würden. Dieser Prozess würde beiden Parteien einen Proof of Proximity geben. Die einzig mögliche Weise, wie diesen beiden Personen in Besitz dieser „Daten" gelangt haben könnten, ist durch gemeinsamen Aufenthalt am selben Ort.**

Setzen wir uns nun mit den Aufwirkungen auf das Netzwerk auseinander: Stellen Sie sich ein System vor, in dem von jedem Eckknoten erwartet wird, konstant solche „Selfies" aufzunehmen und, während sie herumgereicht werden, in einem Ordner zu speichern. Es würde weiterhin von ihnen erwartet, die zeitliche Reihenfolge innerhalb des Ordners zu bewahren, und es wäre ihnen nicht erlaubt, jemals ein „Selfie" zu löschen. Dies etabliert eine Aufnahme von in der Nähe befindlichen Objekten für jeden Eckknoten und dient als Querverweis für die Aufnahmen anderer Eckknoten.

4.4 Nicht-Eckknoten

Alle Knoten, einschließlich Bridge-, Weiterleitungs-, Speicher- und Analyse-Knoten, werden als “Zeugen“ angesehen. Dies ermöglicht die Bündelung der Daten, die von einem Knoten an den nächsten weitergereicht werden. Das ist das Konzept des **Bound Witness**.

4.5 Querverweis

Die Analyse aller “Selfies“, die aufgenommen und von allen Eckknoten aneinander gekettet wurden, ermöglicht es dem System, die **Best Answer** aus der relativen Nähe aller im System befindlichen Knoten, zu ermitteln. Wenn jeder Knoten ehrlich und genau berichtet, wird die Abbildung aller relativen Positionen der Eckknoten die maximal mögliche **Gewissheit** und Genauigkeit erreichen: 100 Prozent. Umgekehrt können Gewissheit und **Genauigkeit** den Minimalwert von 0 Prozent erreichen, wenn jeder Knoten entweder unehrlich oder fehlerhaft ist.

Mithilfe eines berichteten Datensatzes und einer Abfrage nach der relativen Position eines der Eckknoten, kann die Position gemeinsam mit den Koeffizienten für Gewissheit und Genauigkeit generiert werden.

Mit demselben Datensatz und bei Verwendung des gleichen Algorithmus, sollte jede Berechnung zum selben Ergebnis bezüglich der angenäherten Position und der Koeffizienten von Gewissheit und Genauigkeit gelangen.

4.6 Diagramm

S’ und *S”* (Abbildung 1.) sind jeweils ein **Sentinel** (Eckknoten), der Heuristiken sammelt. Wenn sie miteinander in Kontakt treten, tauschen sie **heuristische** Daten und öffentliche Schlüssel miteinander aus. Beide erstellen eine komplette Aufzeichnung der Interaktion und signieren die resultierende Interaktion. Diese signierte Aufzeichnung wird dann zum nächsten Eintrag ihrer jeweiligen Ortsdaten-Ledger (16 für *S’* und 3 für *S”*). Dieser Vorgang verbindet die beiden Zeugen miteinander als in der Nähe zueinander befindlich.

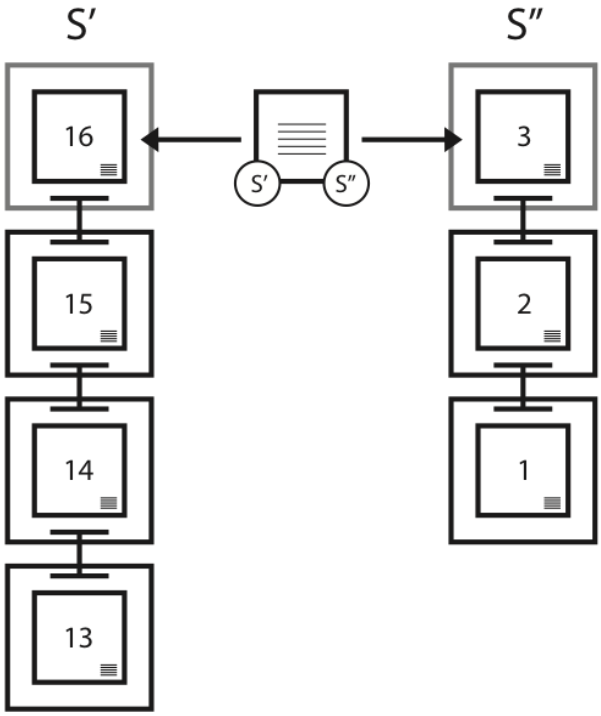

Abbildung 1. Beispiel der Verbindung von Zeugen (Witness Binding) zwischen zwei Sentinels.

4.7 Ursprungsketten

Zur Erstellung einer **Proof of Origin Chain**, erstellt jeder Ursprung (Origin) seinen eigenen Ledger und signiert diesen. Sobald Informationen mit der Proof of Origin Chain geteilt wurden, werden sie tatsächlich permanent. Das liegt daran, dass die der Mitteilung nachfolgende Gabelung die Kette beendet, und alle nachfolgenden Daten des Zeugen behandelt werden, als kämen sie von einem neuen Zeugen. Zur Erstellung eines Links in eine Proof of Origin Chain, generiert der Ursprung ein öffentliches/privates Schlüsselpaar. Er unterzeichnet dann jeweils den vorangehenden und den nachfolgenden Block mit demselben Paar, nachdem der öffentliche Schlüssel in beiden Blöcken verzeichnet wurde. Der private Schlüssel wird sofort, nachdem die Unterzeichnung erfolgt ist, gelöscht. Durch die sofortige Löschung des privaten Schlüssels, wird das Risiko des Diebstahls oder der Wiederverwendung eines Schlüssels maßgeblich verringert.

Proof of Origin Chains sind der Schlüssel zur Verifizierung, dass Ledger, die in das **XYO Network** einfließen, gültig sind. Eine eindeutige ID für Quelldaten ist unpraktisch, da sie gefälscht werden kann. Die Unterzeichnung mit privaten Schlüsseln ist ebenfalls unpraktisch, da die meisten Bestandteile des XYO Network nur mühsam oder gar nicht physisch gesichert werden können. Das Risiko, dass ein privater Schlüssel durch eine böswillige Person gestohlen werden könnte, ist daher zu hoch. Zur Behebung dieses Problems, verwendet das XYO Network **Transient Key Chains**. Der Vorteil dieser Vorgehensweise liegt in der Unmöglichkeit, die Ursprungskette der Daten zu fälschen. Wird die Kette jedoch einmal unterbrochen, so ist sie unwiderruflich unterbrochen und kann nicht fortgeführt werden. Sie wird zur Insel.

Jedes Mal, wenn ein **Heuristik**-Ledger im XYO Network abgegeben wird, fügt der Empfänger seinen eigenen **Proof of Origin** hinzu, wodurch die Proof of Origin Chain länger wird und eine Proof of Origin Intersection generiert wird. Proof of Origin Chains und Proof of Origin Intersections sind die von **Diviners**, bei der Verifizierung

der Ledgervalidität, verwendeten Hauptindikatoren. Die Gleichung für eine Ledger-Reputation ist prinzipiell, welcher Prozentsatz der XYO Network an der Erstellung des damit assoziierten Proof of Origin Ball beteiligt war. Wenn 100 Prozent der Aufzeichnungen des XYO Network durch Proof of Origin verknüpft und vollständig analysiert sind, liegt die Wahrscheinlichkeit theoretisch bei 100 Prozent. Wenn 0 Prozent der Aufzeichnungen des XYO Network zur Analyse verfügbar sind, dann sinkt die Validität auf 0 Prozent.

Als zusätzliche Sicherheit wird der öffentliche Schlüssel für einen Chain Link nicht zur Verfügung gestellt, bis der zweite Eintrag hierfür bereitgestellt wird. So kann auch das Zeitintervall zwischen Einträgen oder Daten, im vorherigen oder nachfolgenden Link gespeichert werden.

4.8 Origin Chain Score

Der Origin Chain Score wird folgendermaßen berechnet (Standardalgorithmus):

- *PcL* = Länger de Proof of Origin Chain
- *PcD* = Schwierigkeit der Proof of Origin Chain
- *Pc' Pc" O* = Überlappung der Proof of Origin Chain für *Pc'* und *Pc"*

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

4.9 Origin Tree

Ein Origin Tree wird zur Berechnung der annähernden Validität einer Antwort verwendet. Er verwendet die gesammelten Daten zur Erstellung eines Ideal Tree, also dem Tree, der am besten zu den Daten einer gegebenen, bestätigten Antwort passt. Wenn der Knoten N sich an den Ortsdaten X, Y, Z, T befindet, muss der Fehler aller Daten einen bestimmten Wert haben. Zur Ermittlung dieses Fehlers, würden wir zunächst MIN, MAX, MITTEL, MEDIAN und den DURCHSCHNITTLICHEN ABSTAND ZUM MITTELWERT berechnen.

Für einen Satz S aller Werte s, einen Schwierigkeitsgrad *PcD der* Proof of Origin Chain und einen Fehlerfaktor Fehler, wird die **Best Answer** folgendermaßen bestimmt:

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

Anders gesagt, die bestätigte Antwort mit dem höchsten **Best Answer** Score ist die Best Answer. Durch Verwendung des Proof of Origin Tree, können wir unmögliche Zweige (Ausreißer) identifizieren und entfernen.

4.10 Transient Key Chaining

Eine Reihe von Datenpaketen kann, durch Verwendung temporärer, privater Schlüssel in zwei aufeinander folgenden Paketen, aneinander gekettet werden. Wenn der mit dem öffentlichen Schlüssel gepaarte private Schlüssel in den Datenpaketen enthalten ist, kann der Empfänger verifizieren, dass beide Pakete mit demselben privaten

Schlüssel signiert wurden. Die in dem Paket enthaltenen Daten, können nicht ohne Zerstörung der Signatur verändert werden. So wird sichergestellt, dass die signierten Pakete nicht von einer Drittpartei, wie einer **Bridge** oder einem Speicherknoten, verändert wurden.

4.11 Link-Tiefe

Ein Knoten generiert mindestens ein neues öffentliches/privates Schlüsselpaar für jeden Link zur **Proof of Origin Chain**, die eine Link-Tiefe von 1 hat. Es kann N Einträge in der Linktabelle jedes gegebenen Ledger Entry geben, wobei jeder Eintrag den Zeitpunkt in der Zukunft angibt, zu dem der zweite Teil des Links hinzugefügt wird. Alle Links haben eine unterschiedliche Größenordnung auf einer binären Skala. Der Eintrag [1,3,7,12,39] wäre beispielsweise erlaubt aber [1,3,7,12,15] wäre nicht erlaubt.

Der Link mit Tiefe 1 wird erstellt, verwendet und gelöscht, sobald der vorausgehende Block veröffentlicht wird. Für Links mit einer größeren Tiefe als 1jedoch, werden die Paare generiert, während der vorausgehende Block signiert wird, und die zweite Signatur erfolgt nicht früher als N Blöcke später, woraufhin der private Schlüssel gelöscht wird. Aus diesem Grund werden Links mit einer Tiefe von mehr als 1 immer als weniger Sicher angesehen als Links mit der Tiefe 1. Sie können jedoch mit diesem Abstrich an Sicherheit, zur Verbesserung der Leistung und Verringerung von Datenverlust, verwendet werden.

4.12 Geregelte Reihenfolge

Das Schlüsselelement in der Sequenzbestimmung der Ledger, ist die Reihenfolge in der sie berichtet wurden. Da es einem Gerät nicht möglich ist, die Reihenfolge eines mit **Proof of Origin** signierten Ledgers zu verändern, kann eine absolute Reihenfolge durch Betrachtung aller Ledger festgelegt werden.

4.13 Veröffentlichung des vorletzten Eintrags

Eine Hauptmethode zur Etablierung des **Proof of Origin** basiert auf der Tatsache, dass ein **Sentinel** immer seinen vorletzten Block berichtet, ohne den letzten Block zu erwähnen. Dies erlaubt es dem letzten Block, den signierten Link zu seinem Vorgänger, als Beweis des Links zu verwenden.

4.14 Leere Verbindungen

Um eine **Proof of Origin Chain** sicherer zu gestalten, ist es notwendig, dass Updates der Kette nicht häufiger als alle zehn Sekunden und nicht seltener als alle sechzig Minuten durchgeführt werden. Sollten keine neuen Daten verfügbar sein, so wird der Kette ein leerer Block hinzugefügt.

4.15 Diagramm

Während die Zeit von links nach rechts verläuft (Abbildung 2), wird die im Aufbau befindliche **Proof of Origin Chain** länger. Der Produzent der Kette wird, zu jedem Zeitpunkt, nur die Einträge mit den abgedunkelten Rändern an den Abfragesteller weiterleiten und auf die zweite Signatur aller Einträge warten, bevor er diese verfügbar macht. Beispielsweise werden aus der 3. Spalte nur die Einträge 2 und 1 als Teil der Kette bereitgestellt.

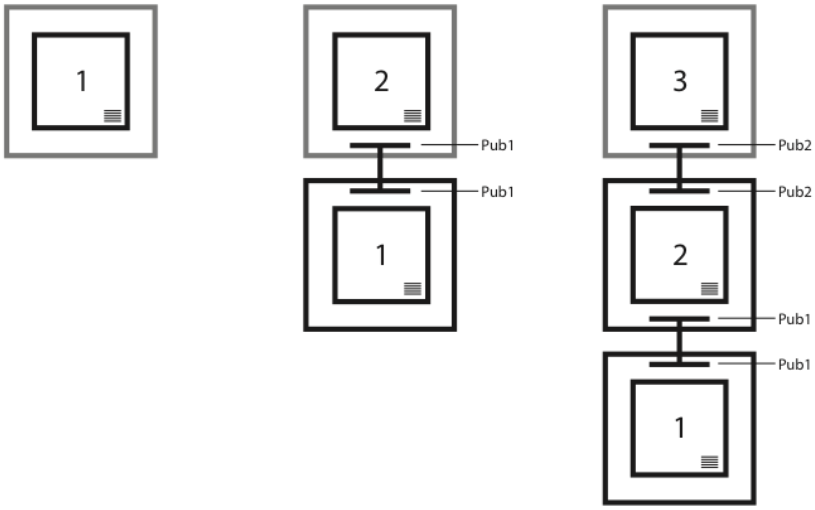

Abbildung 2. Beispiel der Linkinklusion in einer Proof of Origin Chain

4.16 Zusammenfassung

Für eine Reihe von Datenpaketen, die in sequenziellen Paaren mit temporären privaten Schlüsseln und gepaarten öffentlichen Schlüsseln signiert sind, kann mit absoluter **Gewissheit** bestimmt werden, dass diese Pakete denselben Ursprung haben.

5 Sicherheitsaspekte

5.1 Fake Diviner Angriff

Ein Satz digitaler Signaturen wird zum XYO **Smart Contract** geschickt, da der Contract die Integrität des **Diviners** verifizieren muss, der die Antwort geschickt hat. Der Vertrag kann dann, innerhalb eines hohen Vertauensintervalls, die anderen Diviner identifizieren, die diese Liste signiert haben. Ohne diesen Vorgang wäre das Orakel die einzige Fehlerquelle und ein Risiko innerhalb des Systems.

5.2 Sentinel DDos Angriff

Ein anderer zu berücksichtigender Angriff ist ein Distributed Denial of Service (DDoS) unter **Sentinel**-Knoten in einer bestimmten Region. Ein Angreifer könnte versuchen, eine große Anzahl von Verbindungen mit Sentinels herzustellen, um sie an der Weitergabe korrekter Informationen oder jeglicher Informationen überhaupt, an Bridges zu hindern. Wir können dieses Problem umgehen, indem wir von jeder Partei, die mit einem Sentinel Kontakt aufnehmen möchte verlangen, zunächst ein kleines, kryptographisches Puzzle zu lösen. Da eine Abfrage keine große

Anzahl von Verbindungen zu Sentinels beinhaltet, wird dies keine große Belastung für das XYO-Weiterleitungssystem darstellen und würde vom Angreifer eine große Menge an Ressourcen verlangen, um einen erfolgreichen DDoS gegen unser Netzwerk durchzuführen. Eine Proof of Origin Chain kann zu jedem gegebenen Zeitpunkt, durch jedwede Person überprüft werden, da sie in der **XYOMainChain** gespeichert ist. So wird garantiert, dass die Genauigkeit der Antwort auf eine Abfrage (**Origin Chain Score**) auf 0 sinkt, wenn eine einzige Einheit entlang der Kette kompromittiert war.

---

6 XYO-Tokenökonomie

Orakel stellen einen bedeutenden Teil der Macht und der Infrastrukturbedürfnisse dezentralisierter Anwendungen, wobei der Fokus hauptsächlich auf Konnektivität und Aggregation maßgeblicher Orakel liegt. Wir glauben, dass ein vollkommen dezentralisiertes und **vertrauensfreies** System von Orakeln notwendig ist, damit dezentralisierte Anwendungen ihr volles Potential erreichen können.

6.1 Kryptoökonomie des XYO Network

Wir verwenden XYO-TOKEN als Anreiz für das wünschenswerte Verhalten der Bereitstellung korrekter, zuverlässiger Ortsdaten-**Heuristiken**. XYO-Token können als „Treibstoff" betrachtet werden, der als Schnittstelle mit der realen Welt benötigt wird, um die XY-Koordinaten eines bestimmten Objekts zu verifizieren.

Der Prozess funktioniert folgendermaßen: Ein Besitzer eines Tokens stellt zunächst eine Abfrage an das **XYO Network** (z.B. *„Wo ist mein bestelltes E-Commerce-Paket mit XYO-Adresse* 0x123456789...*"*). Die Abfrage wird dann in eine Warteschlange geschickt, wo sie darauf wartet, verarbeitet und beantwortet zu werden. Ein Anwender kann beim Erstellen der Abfrage seine gewünschte Vertrauensstufe und den XYO-Treibstoffpreis festlegen. Die Kosten einer Abfrage (in XYO-Token) wird durch die Menge erforderlicher Daten bestimmt, die notwendig sind, um die Abfrage zu beantworten, sowie aus der Dynamik des Marktes. Je mehr Daten benötigt werden, umso teurer wird die Abfrage und umso höher wird der XYO-Treibstoffpreis. Abfragen an das XYO Network haben das Potential sehr groß und teuer zu werden. Ein Speditions- und Logistikunternehmen könnte beispielsweise die Abfrage an das XYO Network stellen: „*Was sind die jeweiligen Ortsdaten jedes einzelnen Fahrzeugs in unserem Fuhrpark?*"

Sobald der Besitzer des XYO-TOKEN beim XYO Network die Abfrage stellt und den benötigten Treibstoff bezahlt, wenden sich alle an der Aufgabe arbeitenden **Diviners** an alle relevanten **Archivists**, um alle entsprechenden Daten abzurufen, die notwendig sind um die Abfrage zu beantworten. Die gelieferten Daten werden von **Bridges** bereitgestellt, die sie ursprünglich von den **Sentinels** gesammelt hatten. Sentinels sind im Grunde genommen die Geräte oder Signale, welche die Ortsdaten eines Objekts verifizieren. Dies umfasst solche Geräte wie Bluetooth-Tracker, GPS-Tracker, in IdD-Geräte integriertes Geo-Tracking, Satelliten-Tracking-Technologie, QR-Code-Scanner, RFID-Scans und viele andere. XY Findables hat seine Verbraucher-Bluetooth- und GPS-Unternehmen vorbereitet und am Markt eingeführt, mithilfe derer es möglich war, Heuristiken zu Ortsdaten aus der realen Welt zu testen und zu verarbeiten. Alle Bemühungen in der Entwicklung des kundenorientierten Geschäfts von XY Findables, haben dem Zweck gedient, bei der Entwicklung des XYO Network Blockchain Protocol maßgeblich zu helfen.

Wenn die von einem Sentinel-Gerät (etwa einem Bluetooth-Sender) bereitgestellten Daten verwendet werden, um eine Abfrage zu beantworten, dann erhalten alle vier an der Transaktion beteiligten Komponenten einen Anteil des vom Besitzer des Tokens bezahlten XYO-Treibstoffs: der Diviner (der nach der Antwort gesucht hat), der Archiver (der die Daten gespeichert hat), die Bridge (welche die Daten übermittelt hat) und der Sentinel (der die Ortsdaten aufgezeichnet hat). Die Treibstoffverteilung zwischen 3 der 4 Komponenten des XYO Network erfolgt

immer im gleichen Verhältnis. Die Ausnahme stellen die Diviner dar, deren Beteiligung am Prozess der Bereitstellung einer Antwort umfangreicher ist. Innerhalb jeder Komponente wird der Treibstoff gleichmäßig verteilt.

6.2 Belohnungen für Unabhängigkeit

Ortsdaten sammelnde Geräte sind die atomaren Bestandteile des Netzwerks und ein einzelnes Gerät kann die Funktion einer oder mehrerer der vier Systemkomponenten übernehmen. Es wäre jedoch ungewöhnlich, besonders in einem großen **XYO Network**, dass ein Gerät mehr als zwei dieser Komponenten darstellt. Darüber hinaus hat ein Blockchain Ledger mit unabhängigerem **Proof of Origin** ein höheres Ansehen, sodass es eine **kryptoökonomische** Strafe für Geräte gibt, die als multiple Komponenten fungieren.

6.3 Belohnungen für stationäre Integrität

Sentinels im **XYO Network** wird ein stationärer Koeffizient für das Ausmaß ihrer Bewegungen während ihres Lebenszyklus zugeteilt. Je weniger sich ein Sentinel während eines Zeitraums bewegt, umso vertrauenswürdiger sind seine Daten. **Archivists** zeichnen diese stationären Koeffizienten auf und analysieren sie, wenn sie entscheiden, an welche Sentinels sie Abfragen weiterleiten.

6.4 Schaffung von Anreizen zur Verwendung von Token

Ein System, in dem Besitzer von Token ermutigt werden, ihre Token nicht zu verwenden, kreiert ein langfristiges Problem für die zugrunde liegende Ökonomie. Es kreiert ein Ökosystem mit sehr niedrigen Wertanlagen und löst einen natürlichen Impuls aus, Token nicht zu verwenden, anstatt Gebrauch und Liquidität zu fördern.

Das Problem der meisten **kryptoökonomischen** Anreize liegt darin, dass sie zu stark auf die Token-Miners (z.B. **Sentinels**, **Bridges**, **Archivists**, **Diviners**) und gar nicht auf die Token-Anwender fokussiert sind. Der XYO-Token berücksichtigt beides.

Das XYO-Token-Modell bietet Minern nicht nur Anreize, genaue Daten zu liefern, sondern auch zu wissen, wann sie überhaupt keine Daten bereitstellen sollen. Endnutzer werden ermutigt bei niedriger Netzwerkliquidität mehr Transaktionen durchzuführen als bei hoher Netzwerkliquidität. Das Ökosystem der XYO-Token ist daher geeignet, ausgeglichen, flüssig und robust zu bleiben.

6.5 XYO Token-Vorgaben

Der öffentliche Tokenverkauf hat eine gestaffelte Preisstruktur mit einem Ausgangspreis von 1 ETH: 100.000 XYO und einem Höchstpreis von 1 ETH: 33.333 XYO. Details hinsichtlich unseres Volumens und eine zeitbasierte Preisstruktur werden in Kürze veröffentlicht.

- Plattform für Smart Contracts: Ethereum
- Contract Typ: ERC20
- Token: XYO
- Token-Name: **XYO Network** Utility Token
- Token-Adresse: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Emissionsvolumen: Begrenzt und gedeckelt mit dem erreichten Betrag des Token-Hauptverkaufs
- Geplante Obergrenze der XYO Token: USD 48 Millionen
- Unverkaufte und nicht zugeteilte Token: Verbrannt nach Abschluss der Token-Verkaufsveranstaltung. Keine weiteren XYO Token werden nach Abschluss des XYO-Token-Hauptverkaufs generiert.

7 Anwendungsmöglichkeiten des XYO Network

Das **XYO Network** hat weite Anwendungsmöglichkeiten, die eine Vielzahl von Branchen umfassen. Ein Unternehmen im Bereich E-Commerce könnte so, beispielsweise, seinen Premiumkunden einen Zahlung-bei-Lieferung-Service anbieten. Um diesen Dienst anbieten zu können, würde das E-Commerce-Unternehmen das XYO Network (das XYO-Tokens verwendet) nutzen, um einen **Smart Contract** (etwa auf der Ethereum-Plattform) zu schreiben. Das XYO Network könnte dann die jeweiligen Ortsdaten des an den Kunden gesandten Pakets während jedes einzelnen Schritts des Erfüllungsprozesses nachverfolgen, vom Regal im Warenlager über den Zusteller bis hin zum Haus des Kunden und jeden dazwischenliegenden Ort. So könnten E-Commerce-Händler und Webseiten auf **vertrauensfreie** Weise verifizieren, dass ein Paket nicht nur sicher an der Türschwelle eines Kunden angelangt ist, sondern auch sicher in deren Räumlichkeiten. Sobald das Paket in den Räumlichkeiten des Kunden angekommen ist (definiert und bestätigt durch eine spezifische XY-Koordinate), wird die Zustellung als erfüllt angesehen und die Zahlung an den Verkäufer ausgelöst. Die E-Commerce-Integration des XYO Network bietet so dem Händler Schutz vor Betrug und stellt sicher, dass Kunden nur für Produkte zahlen, die auch in ihren Räumlichkeiten angekommen sind.

Stellen Sie sich einen vollständig anderen Einsatzbereich des XYO Network vor, etwa mit einer Hotelbewertungswebseite, die aktuell mit dem Problem zu kämpfen hat, dass ihren Bewertungen oft nicht vertraut wird. Natürlich ist es für Hoteliers reizvoll, ihre Bewertungen mit allen Mitteln zu verbessern. Was wäre, wenn man mit extrem hoher Gewissheit sagen könnte, dass jemand in San Diego war, nach Bali flog und dort zwei Wochen in einem Hotel verbrachte, nach San Diego zurückkehrte und anschließend eine Bewertung des Hotels in Bali schrieb? Diese Bewertung hätte ein hohes Ansehen, speziell wenn Sie von einer Person verfasst wurde, die bereits viel Bewertung mit verifizierten Aufenthaltsdaten abgeben hat.

---

8 Ausbau des XYO Network

Wir sind in der glücklichen Position, über ein kundenorientiertes Geschäft zu verfügen, dass in der realen Welt erfolgreich ein Netzwerk mit über einer Million (1.000.000) Bluetooth- und GPS-Geräten weltweit aufgebaut hat. Die meisten Netzwerke der Standortbestimmung scheitern, bevor sie diese Phase und die notwendige, kritische Masse erreichen, um ein weitreichendes Netzwerk auszubauen. Das von uns aufgebaute **Sentinel**-Netzwerk ist nur der Anfang. Das **XYO Network** ist ein offenes System, in das sich jeder Betreiber von Ortungsgeräten einloggen und mit dem Verdienst von XYO-Tokens beginnen kann.

Allgemein gilt, je höher die Kardinalität eines Sentinel im XYO Network, umso zuverlässiger ist es. Um das Netzwerk weiter auszubauen, ist das XYO Network in Verhandlung mit anderen Unternehmen, um sein Netzwerk an Sentinels über das eigne Netzwerk an XY-Findables-Sendern hinaus, auszudehnen.

9 Danksagung

Dieses Weißbuch ist das Ergebnis einer inspirierenden Team-Anstrengung, die durch das Vertrauen folgender Personen in unsere Vision möglich wurde. Raul Jordan (Harvard College, Thiel Fellow und **XYO Network**-Berater), für seinen Beitrag bei der verständlicheren Gestaltung unseres Weißbuchs und für seine Hilfe bei

der eleganten Kommunikation der technischen Details. Wir danken Christine Sako für ihre außergewöhnliche Arbeitsmoral und Detailgenauigkeit in ihrer Korrektur. Die Konsistenz in Struktur und bester Verfahrensweisen in diesem Weißbuch, ist das Ergebnis von Christines Arbeit. Wir danken Johnny Kolasinski für seine Untersuchung und Zusammenstellung der Anwendungsmöglichkeiten. Zuletzt möchten wir uns bei John Arana für seine umsichtige Durchsicht und seinen kreativen Beitrag bedanken.

Literaturverzeichnis

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

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

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

[4] Goward, Dana. RNT Foundation Testifies Before Congress. Anhörung des US-Repräsentantenhauses: “Finding Your Way: The Future of Federal Aids to Navigation,” Washington, DC, 4. Februar 2014.

Glossar

Genauigkeit Ein Maß der Zuversicht, dass sich ein Datenpunkt oder eine Heuristik innerhalb einer bestimmten Fehlermarge befindet. -

Archivist Ein Archivist speichert Heuristiken als Teil des dezentralisierten Datensatzes, mit dem Ziel der Speicherung aller historischen Ledger aber ohne der Notwendigkeit dies zu erreichen. Selbst wenn einige Daten verloren gehen oder zeitweise nicht verfügbar sein sollten, funktioniert das System weiterhin, nur mit verminderter Genauigkeit. Archivists indizieren außerdem Ledgers, sodass sie bei Bedarf eine Kette von Ledger-Daten liefern können. Archivists speichern ausschließlich Rohdaten und werden ausschließlich für den Abruf der Daten bezahlt. Die Speicherung erfolgt immer ohne Bezahlung.

Best Answer Wir definieren die Best Answer als die einzige Antwort aus einer Liste von Antwortkandidaten, die den höchsten Wert an Validität liefert und einen höheren Wert an Genauigkeit aufweist, als den geforderten Mindestwert.

Best Answer Algorithmus Ein Algorithmus, der zur Generierung von Best Answer-Werten verwendet wird, wenn ein Diviner eine Antwort auswählt. Das XYO Network erlaubt das Hinzufügen spezialisierter Algorithmen und gestattet dem Kunden festzulegen, welcher Algorithmus verwendet werden soll. Es ist notwendig, dass

dieser Algorithmus auf jedem Diviner beim gleichen verfügbaren Datensatz zum selben Ergebnis führt.

Bound Witness Bound Witness ist ein Konzept, dass durch die Existenz einer bidirektionalen Heuristik erzeugt wird. Da eine nicht vertrauenswürdige Datenquelle zur Verwendung bei Erfüllung eines digitalen Vertrags (ein Orakel) nicht hilfreich ist, wird durch die Etablierung einer solchen Heuristik eine substantielle Zunahme der Gewissheit der Daten erreicht. Die vorrangige bidirektionale Heuristik ist Nähe, da beide Parteien das Stattfinden und den Umfang einer Interaktion durch gemeinsames Signieren der Interaktion validieren können. Dies ermöglicht einen Zero-Knowledge-Beweis, dass sich die beiden Knoten in Nähe zueinander befanden.

Bridge Eine Bridge ist ein heuristischer Protokollant. Sie leitet heuristische Ledgers sicher von Sentinels an Diviners weiter. Der wichtigste Aspekt einer Bridge ist, dass ein Diviner sicher sein kann, dass der von einer Bridge empfangene, heuristische Ledger in keiner Weise verändert wurde. Der zweitwichtigste Aspekt einer Bridge ist, dass sie zusätzliche Proof-of-Origin-Metadaten hinzufügt. **Gewissheit** Ein Maß der Wahrscheinlichkeit, dass ein Datenpunkt oder eine Heuristik nicht korrumpiert sind oder manipuliert wurden.

Krypto-Ortsdaten Der Bereich der kryptographischen Ortsdatentechnologie.

Kryptoökonomie Eine formelle Disziplin, die Protokolle untersucht, mithilfe derer die Produktion, Verteilung und der Verbrauch von Gütern in einer dezentralisierten, digitalen Ökonomie gesteuert werden. Kryptoökonomie ist eine angewandte Wissenschaft, die sich auf Entwicklung und Beschreibung dieser Protokolle konzentriert.

Diviner Ein Diviner beantwortet gestellte Abfragen durch Analyse historischer Daten, die im XYO Network gespeichert wurden. Heuristiken, die im XYO Network gespeichert werden, benötigen ein hohes Maß an Proof of Origin zur Bestimmung der Validität und Genauigkeit der Heuristik. Ein Diviner erhält und liefert eine Antwort durch Beurteilung des Zeugen anhand seines Proof of Origin. Da es sich beim XYO Network um ein vertrauensfreies System handelt, müssen dem Diviner zur Bereitstellung ehrlicher Analysen von Heuristiken, Anreize geboten werden. Anders als Sentinels und Bridges, verwenden Diviner Proof of Work, um der Blockchain Antworten hinzuzufügen.

Heuristik Ein Datenpunkt bezüglich der realen Welt und realtiv zur Position eines Sentinel (Nähe, Temperatur, Licht, Bewegung usw...).

Orakel Teil eines DApp-Systems (dezentralisierte Applikationen), das für die Erfüllung eines digitalen Vertrags durch Bereitstellung einer Antwort mit Genauigkeit und Gewissheit, verantwortlich ist. Der Begriff „Orakel“ hat seinen Ursprung in der Kryptographie, wo er eine wahrhaft zufällige Quelle beschreibt (z. B. eine Zufallszahl). Dies liefert die notwendige Verbindung von einer Krypto-Gleichung zur Außenwelt. Orakel speisen Smart Contracts mit Daten von außerhalb der Kette (der realen Welt oder „Offchain“). Orakel sind Schnittstellen zwischen digitaler Welt und realer Welt. Betrachten wir als morbides Beispiel einen Vertrag über einen letzten Willen und Testament. Die Bestimmungen des letzten Willens werden umgesetzt, sobald das Ableben des Hinterlassenden bestätigt ist. Ein Orakeldienst könnte erstellt werden, um den letzten Willen durch Ansammeln und Zusammenfassen relevanter Daten offizieller Quellen, auszulösen. Das Orakel könnte dann als Datenquelle oder Endpunkt für einen Smart Contract verwendet werden, um zu überprüfen ob die Person verstorben ist.

Origin Chain Score Der einer Origin Chain, zur Bestimmung ihrer Glaubwürdigkeit, zugeordnete Wert. Diese Einschätzung berücksichtigt Länge, Verwirrung, Überlappung und Redundanz.

Origin Tree Ein Datensatz von Ledger-Einträgen aus unterschiedlichen Origin Chains zur Feststellung des Ursprungs eines heuristischen Ledger-Eintrags, mit einem bestimmten Grad der Gewissheit.

Proof of Origin Proof of Origin ist der Schlüssel zur Verifizierung, dass Ledger, die in das XYO Network einfließen, gültig sind. Eine eindeutige ID für Datenquellen ist unpraktisch, da sie gefälscht werden kann. Die Unterzeichnung mit privaten Schlüsseln ist ebenfalls unpraktisch, da die meisten Bestandteile des XYO Network nur mühsam oder gar nicht physisch gesichert werden können. Das Risiko, dass ein privater Schlüssel durch eine böswillige Person gestohlen werden könnte, ist daher zu hoch. Zur Behebung dieses Problems, verwendet das XYO Network Transient Key Chaining. Der Vorteil dieser Vorgehensweise liegt in der Unmöglichkeit, die Daten der Ursprungskette zu fälschen. Wird die Kette jedoch einmal unterbrochen, so ist sie unwiderruflich unterbrochen und kann nicht fortgeführt werden. Sie wird zur Insel.

Proof of Origin Chain Eine Transient Key Chain die eine Reihe von heuristischen Bound Witness Ledger-Einträgen miteinander verbindet.

Proof of Work Proof of Work ist ein Datum, dass bestimmte Voraussetzungen erfüllt, schwer zu erstellen (d.h. teuer, zeitaufwändig), aber leicht für andere zu verifizieren ist. Die Erstellung eines Proof of Work kann ein zufälliger Prozess mit geringer Generierungswahrscheinlichkeit sein, sodass für gewöhnlich gründliches Ausprobieren notwendig ist, bevor ein gültiger Proof of Work erstellt ist.

Sentinel Ein Sentinel ist ein heuristischer Zeuge. Er beobachtet Heuristiken und garantiert deren Gewissheit und Genauigkeit durch Erzeugen temporärer Ledger. Der wichtigste Aspekt eines Sentinels ist, dass er durch Hinzufügen von Proof of Origin Ledger erstellt, die Diviners die Gewissheit geben, aus derselben Quelle zu kommen.

Smart Contract Ein Protokoll, geprägt von Nick Szabo vor Bitcoin, mutmaßlich 1994 (weshalb manche meinen, er sei Satoshi Nakamoto, der geheimnisvolle und unbekannte Erfinder von Bitcoin). Die grundlegende Idee hinter Smart Contracts ist es, eine rechtliche Übereinkunft in ein Programm zu kodifizieren und seine Bedingungen durch dezentralisiere Computer umsetzen zu lassen, anstatt Verträge durch Menschen interpretieren und sie dann den Verträgen entsprechend handeln zu lassen. Smart Contracts kippen Geld (z.B: Ether) und Verträge in dasselbe Konzept. Da Smart Contracts deterministisch sind (wie Computerprogramme) sowie vollkommen transparent und lesbar, dienen sie als leistungsstarkes Mittel, um Mittelsmänner und Broker zu ersetzen.

Transient Key Chain Eine Transient Key Chain verbindet eine Reihe von Datenpaketen durch Transient Key Cryptography.

vertrauensfrei Eine Eigenschaft, bei der alle Parteien in einem System Konsens dahingehend erreichen können, was die kanonische Wahrheit ist. Macht und Vertrauen wird unter den Stakeholdern des Netzwerks (z.B. Entwicklern, Minern und Verbrauchern) verteilt (oder geteilt), anstatt bei einer einzelnen Person oder Organisation (z.B. Bank, Regierung und Finanzinstitutionen) konzentriert zu werden. Dies ist ein allgemeiner Begriff, der leicht missverstanden werden kann. Blockchains eliminieren nicht wirklich Vertrauen. Sie minimieren das notwendige Vertrauen, das in einen einzelnen Teilnehmer des Systems investiert werden muss. Dies wird durch Verteilung von Vertrauen unter verschiedenen Akteuren des Systems mithilfe eines ökonomischen Spiels erreicht, das Akteuren Anreize bietet mit den durch das Protokoll definierten Regeln zu kooperieren.

XY Oracle Network XYO Network.

XYO Network XYO Network steht für „XY Orakel Netzwerk." Es umfasst das gesamte System XYO-fähiger Komponenten/Knoten, einschließlich Sentinels, Bridges, Archivists und Diviners. Die Hauptfunktion des XYO Network ist die eines Portals, mithilfe dessen Smart Contracts durch bestätigte Geodaten der realen Welt, erfüllt werden können.

XYOMainChain Eine unveränderliche Blockchain im XYO Network, die Abfrage-Transaktionen, gemeinsam mit den von Divinern gesammelten Daten und deren zugeordnetem Origin Wert, speichert.