Проектний документ XY Oracle Network: Криптографічна мережа визначення місцезнаходження на основі доказу походження

Arie Trouw (Арі Троув)*, Markus Levin (Маркус Левін)†, Scott Scheper (Скотт Шепер)‡

січень 2018 р

Витяг

Зі зростаючою присутністю пов’язаних, залежних від місцезнаходження технологій, наша конфіденційність та безпека залежать від точності та достовірності інформації про місцезнаходження. Були здійснені різноманітні спроби усунути потребу в централізованих організаціях, контролюючих потік даних про місцезнаходження, однак кожна спроба покладалась на чесність пристроїв, що збирають ці дані у фізичному світі. Ми пропонуємо мережу криптографічного місцезнаходження, яка **не потребує довіри**, використовуючи нову формулу, засновану на ланцюжку доказів з нульовим розголошенням для встановлення високого ступеню достовірності даних про місцезнаходження. **Мережа XYO (мережа оракулів XY)** - це абстракція, яка дозволяє проводити багаторівневу перевірку місцеположення у багатьох класах пристроїв та протоколів. В її основі знаходиться набір нових криптографічних механізмів, відомих як **«Proof of Origin (Доказ походження) та Bound Witness (Пов’язаний свідок)»**, які поєднують потужність технології блокчейну та збору реальних даних в систему з прямими прикладами застосуваннями вже сьогодні.

---

1 Вступ

З появою **смарт-контрактів на базі блокчейн, що не потребують довіри**, значно зросла потреба в службах оракулу, які визначають результат контракту. Більшість нинішніх прикладів застосувань смарт-контрактів залежать від єдиного або агрегованого набору авторитетних оракулів для визначення результатів контракту. У тих випадках, коли обидві сторони можуть домовитись про авторитетність і стійкість до втручання зазначеного оракула, цього достатньо. Проте, у багатьох випадках, або не існує відповідного оракула, або оракул не може вважатися авторитетним через можливість помилки або втручання.

Оракули місцезнаходження підпадають під цю категорію. Передбачення місцезнаходження об'єкта фізичного світу залежить від звітності, передачі, зберігання та обробки компонентів даного оракула, і кожен з цих елементів вносить помилку і може бути зміненим. Ризики включають маніпуляцію даними, забруднення даних, втрату даних та змову.

Таким чином, існує наступна проблема: **і на достовірність, і на точність місцезнаходження негативно впливає відсутність децентралізованого геолокаційного оракула, що не потребує довіри.** Такі платформи як Ethereum та EOS, завдяки своїм можливостям, широко використовувались для безпечного врегулювання взаємодій онлайн, а перші випадки використання включали депонування для залучення коштів у формі ICO. Однак, до цього моменту, кожна платформа зосереджена повністю на світі онлайн, а не на фізичному світі – а все через шумну, схильну до втручання цілісність даних поточних інформаційних каналів.

Мережа XYO працює над тим, щоб дозволити розробникам, які наприклад, пишуть смарт-контракти для блокчейн платформ, взаємодіяти з фізичним світом так, ніби це API. **Мережа XYO** - це перший у світі протокол оракула, який дозволяє двом суб'єктам здійснювати транзакції в реальному світі без централізованої третьої сторони. Наші абстракції дозволяють нам робити перевірку місцезнаходження для розробників без необхідності довіри, створюючи протокол з новими прикладами застосування, які не були можливі до сьогодні.

Мережа XYO буде побудована на існуючій інфраструктурі з більш ніж 1 000 000 пристроїв, які були поширені у світі завдяки орієнтованому на взаємодію зі споживачами рішенню «findables». Bluetooth і GPS пристрої компанії XY дозволяють повсякденним споживачам розміщувати фізичні маячки для відстежування речей, які вони хочуть відстежувати (наприклад, ключі, багаж, велосипеди та навіть домашні тварини). Якщо вони гублять, або втрачають такий предмет, вони можуть точно побачити де він, відстежуючи його місцезнаходження на смартфоні. Усього за шість років мережа XYO створила в світі одну з найбільших споживацьких мереж Bluetooth і GPS пристроїв.

---

2 сторичний контекст та попередні підходи

2.1 Доказ місцезнаходження

Концепція місцезнаходження, яке можна підтвердити, існує приблизно з 1960-х років, і навіть може бути датована ще 1940-ми роками, коли з’явились наземні радіонавігаційні системи, такі як LORAN [1]. Сьогодні існують служби визначення місцезнаходження, які складають декілька засобів перевірки один на одного, щоб створити Доказ місцезнаходження через триангуляризацію та GPS. Проте ці підходи ще не можуть вирішити найважливішої проблеми, з якою ми сьогодні стикаємося в технологіях геолокації: розробка системи, яка виявляє шахрайські сигнали та зупиняє підробку даних про місцезнаходження. З цієї причини ми вважаємо, що найважливішою крипто-локаційною платформою сьогодні буде та, яка найбільше сфокусується на підтвердженні походження сигналів фізичного місцезнаходження.

Як це не дивно, але концепція застосування підтвердження місцезнаходження на базі технології блокчейн вперше з'явилася в вересні 2016 року на конференції розробників Ethereum DevCon 2. Вона була представлена розробником Ethereum з Берліна Лефтерісом Карапетсасом. Проект Карапетсаса *Sikorka* зробив можливим використання **смарт-контрактів** в реальному світі вже сьогодні, використовуючи дещо, що він називає, «*Доказ присутності»*. Його поєднання місцезнаходження та світу блокчейну зосереджувалося головним чином на застосуванні

в доповненій реальності; і він представив нові поняття, такі як питання-виклики, що підтверджують місцезнаходження особи [2].

17 вересня 2016 року термін «Доказ місцезнаходження» формально з'явився у спільноті Ethereum [3]. Потім його розтлумачив розробник Ethereum Foundation Matt Di Ferrante (Метт Ді Ферранте):

> «Доказ місцезнаходження, якому ви можете довіряти – це, безумовно, одна з найскладніших речей для реалізації. Навіть якщо у вас є багато учасників, які можуть підтвердити місцезнаходження один одного, немає гарантії того, що хтось не організує атаку Сібілли у майбутньому, а оскільки ви завжди спираєтесь на звітність більшості, це величезна слабкість. Якщо вам знадобиться певний тип спеціалізованого апаратного пристрою, захищеного від зламів, такий, як закритий ключ, що знищується, коли хтось намагається відкрити його або змінити прошивку на ньому, то ви, можливо, матимете більший рівень безпеки, але в той же час не слід виключати spoof-атаку на GPS пристрій. Належна реалізація цього вимагає нейтралізації такої великої кількості програмних помилок, і такої кількості різних джерел даних, щоб отримати певний рівень достовірності та точності, що це повинен бути дуже добре профінансований проект».
>
> — Метт Ді Ферранте, розробник, Ethereum Foundation

2.2 Доказ місцезнаходження: недоліки

Якщо коротко, то Доказ місцезнаходження можна сприймати як використання потужних властивостей блокчейну, таких як присвоєння часових міток та децентралізація, і поєднання їх з пристроєм(ями), що не пов'язаний з мережею, і визначає місцезнаходження, який, як ми сподіваємося, не піддається spoof-атакам. Ми називаємо область застосування технології криптографічного місцезнаходження «*криптолокацією*». Крім того, подібно до того, як слабкість **смарт-контрактів** заключається в **оракулі,** який використовує єдине джерело істини (і, таким чином, має одне джерело невдачі), системи криптолокації стикаються з такою ж проблемою. Вразливість в поточних технологіях криптолокації заключається в пристроях поза мережею, які повідомляють про місцезнаходження об'єкта. У смарт-контрактах джерело даних поза мережею є оракулом. У **мережі XYO** джерело даних поза мережею переміщується в реальному світі як особливий тип оракула, який ми називаємо **Sentinel (Страж)**. Ядро інновації, яке охоплює мережу XYO, базується на доказі місцезнаходження, яке не потребує ідентичності, і лежить в основі компонентів нашої системи для створення протоколу криптолокації, який **не потребує довіри**.

---

3 Мережа оракулів XY

«Необхідність у системі, яку важко порушити, і яка б доповнила GPS, назрівала протягом багатьох років. GPS є винятково точною та надійною технологією, але здається, що атаки з використанням перешкод, спуф- та кібератаки та інші форми перешкод, зростають як за частотою, так і серйозністю. Це з часом може призвести до руйнівних наслідків для нашого життя та економічної діяльності».

— Дана Говард, президент RNT Foundation

3.1 Вступ

Метою **мережі XYO** є створення децентралізованої системи оракулів місцезнаходження, що **не потребує довіри,** стійкої до атак, та яка забезпечує найвищу **достовірність** при запиті доступних даних. Ми досягаємо цього за допомогою набору абстракцій, який значно зменшує ризик підробки місцезнаходження завдяки ланцюжку доказів з нульовим розголошенням поряд з компонентами системи.

3.2 Огляд мережі

Наша система забезпечує точку входу в протокол підключених пристроїв, що забезпечує високу **достовірність** даних про місцезнаходження за допомогою ланцюжка криптографічних доказів. Користувачі можуть відправляти транзакції, які називаються «*запитами*», щоб отримати частину даних про місцезнаходження на будь-якій блокчейн-платформі, яка підтримує технологію **смарт-контрактів**.[1] Потім агрегатори з мережі XYO зчитують ці запити, відправлені на контракт, і отримують відповіді, які мають найвищу точність з децентралізованого набору пристроїв, які передають криптографічні докази назад до цих агрегаторів. Ці агрегатори потім надсилають ці відповіді на смарт-контракт після досягнення консенсусу щодо відповіді з найкращим балом. Ця мережа компонентів дає змогу визначити, чи є об'єкт певною XY-координатою протягом певного часу, з найбільш доказовою достовірністю, що **не потребує довіри**.

Мережа XYO має чотири основні компоненти: **Sentinels** (Стражі) (збирачі даних), **Bridges** (Мости) (ретранслятори даних), **Archivists** (Архіваріуси) (зберігачі даних) та **Diviners** (Провидці) (агрегатори відповідей). Стражі збирають інформацію про місцезнаходження через датчики, радіостанції та інші засоби. Мости використовують ці дані від Стражів і передають їх Архіваріусам. Архіваріуси зберігають цю інформацію для аналітики. Провидці аналізують геолокаційну **евристику** від Архіваріусів, щоб отримати відповіді на запити і призначити їм оцінку точності. Потім Провидці передають ці відповіді назад на смарт-контракт (таким чином, Провидці є **оракулами**). Оцінка точності, яка називається **оцінкою ланцюжка походження**, визначається за допомогою набору доказів з нульовим розповсюдженням, відомим як **ланцюжок доказу походження**. Цей ланцюжок гарантує, що два або більше фрагментів даних походять з одного джерела, без розкриття будь-якої прихованої інформації. Кожен компонент на шляху запиту генерує власний Доказ походження, який потім прикріплюється до кожного компонента, на який він передає дані. **доказ походження** – це нове формулювання, яке створює ланцюжок криптографічних гарантій на шляху ретрансляторів в мережі, щоб забезпечити високу впевненість у реальних даних. Цей **ланцюжок доказу походження** являє собою впевненість, яку ми можемо

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counterparty, Monax та інші.

мати в частині даних про місцезнаходження, до самих перших пристрів, що зібрали дані. Ми глибше ознайомимося з тим, як працює Доказ походження в наступному розділі.

Для створення децентралізованого механізму консенсусу між провидцями, мережа XYO буде покладатися на загальнодоступний, незмінний блокчейн, відомий як **XYOMainChain,** який зберігає транзакції запитів разом з даними, отриманими від провидців, та пов'язаною з ними оцінкою походження. Перш ніж ми зануримось в деталі функціональності всієї системи, ми чітко визначимо обов'язки кожного компонента у нашій мережі.

3.2.1 Стражі

Стражі –це свідки місцезнаходження. Вони слідкують за **евристикою** даних та гарантують **достовірність** та **точність** евристики шляхом створення тимчасових реєстрів. Найважливіший аспект стражів полягає в тому, що вони створюють реєстри, і інші компоненти можуть бути певними, що вони походять з одного й того ж джерела. Це досягається шляхом додавання **доказів походження** до ланцюжка передачі криптографічних доказів. Враховуючи, що **мережа XYO** - це система, що не потребує довіри, стражі повинні бути зацікавлені в наданні чесної інформації про місцезнаходження. Це досягається шляхом об'єднання репутаційного та платіжного компонентів. Страж винагороджується токенами мережі XYO (XYO), коли його інформація використовується для відповіді на запит. Щоб збільшити шанси на винагороду, вони повинні створювати реєстри, сумісні з їхніми вузлами, і забезпечити доказ походження, щоб вони могли ідентифікувати себе як джерело інформації про місцезнаходження.

3.2.2 Мости

Мости –це транскриптори даних про місцезнаходження. Вони надійно передають реєстри місцезнаходження від **стражів** до **архіваріусів**. Найважливішим аспектом мосту є те, що архіваріус може бути впевненим в тому, що **евристичні** реєстри, отримані від мосту, ніяким чином не були змінені. Другий найважливіший аспект мосту – це те, що вони додають додатковий **доказ походження**. Враховуючи, що **мережа XYO** – це система, що не потребує довіри, мости повинні бути зацікавлені в забезпеченні чесної передачі евристики. Це робиться шляхом об'єднання репутаційного та платіжного компонентів. Міст винагороджується токенами мережі XYO (XYO), коли його інформація використовується для відповіді на запит. Щоб збільшити шанси на винагороду, вони повинні створювати реєстри, сумісні з їхніми вузлами, і забезпечити доказ походження, щоб вони могли ідентифікувати себе, як ретранслятори евристики.

3.2.3 Архіваріуси

Архіваріуси зберігають інформацію про місцезнаходження, отриману від **мостів** у децентралізованій формі з метою зберігання всіх історичних реєстрів. Навіть якщо деякі дані втрачаються, або стають тимчасово недоступними, система продовжує функціонувати, лише зі зниженою точністю. Архіваріуси також індексують реєстри, щоб вони могли легко повернути рядок даних реєстру за необхідності. Архіваріуси зберігають лише вихідні дані та отримують токени

мережі XYO виключно за отримання даних та подальшого їх використання. Зберігання завжди безкоштовне.

Архіваріуси об'єднуються в мережу, тому запит до одного архіваріуса призведе до того, що архіваріус запитає інших архіваріусів про дані, яких він не має. Архіваріус також може зберігати будь-яку інформацію з реєстру, що повертається до нього. Це, швидше за все, призведе до виникнення двох типів архіваріусів: тих, що знаходяться з краю генерування даних «хмари» та тих, що знаходяться з краю використання даних «хмари». Архіваріуси посередині будуть гібридами. Вибір зберігати дані чи ні, не обов'язковий, але його можна легко виконати за допомогою IPFS або іншого децентралізованого рішення для зберігання. Кожного разу, коли дані передаються від одного архіваріуса до іншого, додається додатковий доказ походження, щоб відстежити платіж, оскільки всі архіваріуси отримують плату. Для вилучення даних може бути встановлений мінімальний рівень доказу походження, щоб збільшити достовірність. Інтереси **стражів**, мостів та архіваріусів повинні бути узгоджені з метою запобігання роздування даних.

3.2.4 Провидці

Провидці – це найбільш складна частина **мережі XYO**. Кінцевою метою провидця є отримання найбільш точних даних для запиту з мережі XYO і передачі цих даних назад до ініціатора цього запиту. Провидці опитують відповідну блокчейн платформу (наприклад, Ethereum, Stellar, Cardano, IOTA та ін.) на запити, надіслані на **смарт-контракт** XYO. Потім вони шукають відповідь на запит, безпосередньо взаємодіючи з мережею **архіваріуса,** щоб отримати відповідь з найвищою оцінкою **точності**/впевненості. Це виконується шляхом оцінки свідка з найкращим **ланцюжком доказу походження**. Провидці, які отримали відповідь з найкращою оцінкою у найкоротші терміни, зможуть створити блок на основному блокчейні XYO (**XYOMainChain**) за допомогою **доказів виконаної роботи**. Запити розміщуються за пріоритетністю по розміру винагороди та складності, тому чим більше XYO пропонується для відповіді, тим вищий пріоритет отримає запит.

Інші Провидці досягають консенсусу щодо достовірності блоку та цифрового підпису блоку. Провидець, який був адресою coinbase в цьому блоці, потім направить транзакцію на смарт-контракт, що містить відповідь, і оцінку його точності. Він також надсилає список інших підписів провидців, щоб не дати зловмиснику надіслати підроблену інформацію в блокчейн, прикинувшись провидцем. Смарт-контракт може потім перевірити цілісність цієї інформації, перевіривши список підписів корисної інформації.

3.3 End-to-End функціонал

Тепер, коли обов'язки кожного компонента детально описані, наводимо end-to-end приклад того, як система буде працювати:

1. **Стражі збирають дані**
    - **Стражі** збирають **евристику** геолокації у реальному світі та готують власний **доказ походження** до прив'язки до вузлів над ними.
2. **Мости отримують дані від стражів**

- **Мости** отримують необхідні дані від онлайн стражів і додають доказ походження до їх ланцюжка. Потім мости стають доступними для **архіваріусів** у мережі.

3. **Архіваріуси індексують/збирають дані, отримані від мостів**
    - Мости постійно надсилають інформацію архіваріусам, які потім зберігаються в децентралізованих сховищах разом із індексом евристичної геолокації.
4. **Провидець отримує запит від користувача**
    - **Провидці** перевіряють запити, надіслані на **смарт-контракт** і вирішують, чи починати процес формулювання відповіді
5. **Провидці отримують дані від архіваріусів**
    - Потім провидці вирішують, чи обробляти запит, отримуючи необхідну інформацію з мережі архіваріуса.
6. **Провидець формулює відповідь**
    - **Провидці** обирають **найкращу відповідь** на запит з мережі архіваріуса, яка має найкращу **оцінку ланцюжка походження.**
7. **Провидець пропонує блок**
    - Потім провидці пропонують блоки у XYOMainChain, що містять відповідь, запит та токени XYO (XYO), оплачені після отримання доказу виконаної роботи. Інші провидці у мережі підписують вміст блоку, а потім випадковий код рахунку провидця coinbase оновлюється, щоб показати доказ виконаної роботи в системі після досягнення консенсусу по дійсному блоку.
8. **Провидець повертає результат до ініціатора запиту**
    - Провидці упаковують відповідь, його оцінку ланцюжка походження і його набір цифрових підписів і відправляють їх на компонент адаптера, який надійно підключається до смарт-контракту XYO. Адаптер відповідає за впевненість в тому, що цілісність провидця не була скомпрометована, і надсилає набір цифрових підписів на смарт-контракт. Це відбувається одразу після процесу створення блоку. Потім провидець coinbase отримує плату за свої зусилля.
9. **Компоненти мережі XYO отримують винагороду за свою роботу**
    - Компоненти ланцюжка доказу походження отримують оплату за свою участь у отриманні відповіді на запит. Стражі, мости, архіваріуси та провидці отримують винагороду за свою роботу.

У тому випадку, якщо один і той же запит запитується більше одного разу, може бути створено кілька відповідей, оскільки відповідь, що видається в даний момент часу, базується на доступній евристиці, яку система може запропонувати в той час. Відправка відповіді на блокчейн має два етапи. По-перше, необхідно провести аналіз, щоб визначити **найкращу відповідь** на запит. Якщо система створює декілька відповідей, то вузли порівнюють відповіді і завжди обирають найкращу відповідь. Прикладом простого запиту може бути: «*Де був вузол в мережі в певний час у минулому?*»

3.4 Блокчейн як єдине джерело істини

По суті, **провидці** просто перетворюють відносні дані в абсолютні. Вони можуть вивчати всю мережу **архіваріуса,** щоб конкретизувати абсолютну відповідь на запит у **мережі XYO**. Провидці також є вузлами, які пропонують і додають блоки до **XYOMainChain**, і отримують винагороду за свій **доказ виконаної роботи**. Оскільки мережа архіваріуса є сховищем

необроблених даних, а блокчейн – це сховище абсолютних, оброблених даних, то в кінцевому підсумку мережа може використовувати найновішу інформацію про XYOMainChain, щоб надавати відповіді на майбутні запити, замість того, щоб спиратися на дорогі розрахунки через мережу архіваріуса.

Оскільки блоки XYOMainChain зберігають **ланцюжок доказу походження** та графік компонентів, які використовувались для надання відповіді на запити, майбутні провидці зможуть вивчати ці абсолютні дані для досягнення точних результатів з використанням нижчої пропускної здатності. Таким чином, XYOMainChain поступово стане найважливішим джерелом істини системи. Проте, мережа архіваріуса все одно буде потрібна для зберігання найновішої інформації про **евристику** геолокації, зібрану **стражами**.

3.5 Принципи вибору кандидата на найкращу відповідь мережі XYO

Ми визначаємо **найкращу відповідь** як єдину відповідь серед списку кандидатів на відповідь, яка повертає найвищу оцінку достовірності і має більш високу **точність,** ніж мінімально необхідна точність. Оцінка достовірності базується на **оцінці ланцюжка походження.** Система знає, що є найвищим значенням оцінки походження, яке буде мати показник 100 відсотків до досягнення більшої оцінки, яка потім стане новим показником 100 відсотків. **Мережа XYO** дозволяє обирати **алгоритм найкращої відповіді** для визначення найкращої відповіді. Це створює розширення для майбутніх досліджень альтернативних алгоритмів.

Коли дані виключаються з відповіді через те, що вони вважаються поганими чи неправильними, вони будуть поширені архіваріусами, щоб вони змогли видалити ці дані зі своїх децентралізованих сховищ.

3.6 Початкова інтеграція з загальнодоступними блокчейнами

Мережа XYO розроблена так, щоб бути абстракцією, яка може взаємодіяти з будь-якими загальнодоступними блокчейнами, такими як Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano та інші, які підтримують **смарт-контракти**. Для взаємодії з мережею XYO, користувачі Ethereum, наприклад, можуть ініціювати запити на наш смарт-контракт XYO та платити токенами XYO (ERC20). Вузли в нашому блокчейні XYO, що називаються **провидцями**, будуть постійно опитувати Ethereum на ці запити та отримувати винагороду у валюті нашого блокчейну XYO (які також називаються токенами XYO). У майбутньому ми зробимо конверсію «один на один» для власників наших токенів ERC20 у валюту нашого блокчейну, щоб забезпечити наші платформи комісійними за проведення транзакцій, які відповідають вимогам мікроплатежів, необхідним для масштабованих прикладів застосування в IoT. У таких випадках ми дозволимо користувачам видавати запити безпосередньо на наш блокчейн, а не взаємодіяти через загальнодоступний смарт-контракт.

4 Доказ походження

Так як фізична мережа складається з ненадійних вузлів, є можливість визначити достовірність даних, які були надані граничними вузлами на основі доказів з нульовим поширенням, що дві або більше частин даних походять з одного джерела. Використовуючи ці набори даних у поєднанні з низкою подібних наборів даних та знанням абсолютного розташування принаймні одного вузла, можна визначити абсолютне розташування іншого вузла.

4.1 Доказ походження: Вступ

Традиційні системи, що **не потребують довіри**, покладаються на секретний ключ для підписів транзакцій або контрактів у системі. Це добре працює за припущення, що вузол в мережі, який підписує ці дані, фізично і віртуально безпечний. Проте, якщо секретний ключ скомпрометований, тоді здатність довести походження починає втрачатися.

Застосовуючи ідеї непотрібності довіри до Інтернету речей, слід припустити, що граничні вузли мережі фізично чи віртуально не захищені. Це викликає необхідність ідентифікації граничних вузлів без використання унікальних ідентифікаторів, і замість цього оцінювати створені ними дані як чесні та достовірні без будь-яких знань з-за меж мережі.

4.2 Суть доказу походження: Пов’язані свідки

Доказ походження покладається на поняття **пов'язаного свідка**. Враховуючи, що ненадійне джерело даних, що використовуються для виконання цифрового контракту (**оракул**), є непридатним, ми можемо суттєво збільшити **достовірність** даних, що надаються, встановивши спочатку існування двонаправленого доказу місцезнаходження. Первинною **евристикою** двонаправленого місцезнаходження є близькість, оскільки обидві сторони можуть підтвердити виникнення та діапазон взаємодії шляхом сумісного підпису взаємодії. Це дозволяє отримати доказ з нульовим розповсюдженням про те, що два вузли знаходяться в безпосередній близькості один від одного.

Потім нам потрібно визначити впевненість в тому, що вузол оракула свідка в системі, що **не потребує довіри**, зібрав дані, і вони поширюються. У системі, що **не потребує довіри**, вузол-свідок може або через дефект, або через втручання створювати неправдиві дані. Недійсні дані можна виявляти та видаляти просто на основі того, що вони виходять за межі дозволеного діапазону для тієї евристики. Достовірні, але неправильні дані (тобто хибні дані) набагато складніше виявити.

4.3 Однонаправлена та двонаправлена евристика геолокації

Більшість даних, що відносяться до фізичного світу (**евристика**), є однонаправленими. Це означає, що вимірюваний елемент не може вимірюватися назад, що робить перевірку однонаправлених евристичних даних дуже складною. Двонаправлена евристика – це та, де вимірюваний елемент може повідомити про свої власні виміри назад іншій стороні, що робить перевірку можливою. Місцезнаходження є рідкісною евристикою, оскільки воно може бути двонаправленим, з двома граничними вузлами, що звітують один одному. **Реальним прикладом цього можуть служити дві людини, які знаходяться поруч один з одним і роблять селфі, друкуючи копії для кожної сторони, а потім підписуючи селфі. Цей процес дасть обидвом сторонам доказ близькості. Єдиним способом отримання цих «даних» двома особами було б те, що вони були разом у тому самому місці.**

Далі, давайте поговоримо про мережеві ефекти: уявіть собі систему, в якій очікується, що кожен граничний вузол буде постійно виробляти ці «селфі», на шляху своєї подорожі, і зберігати їх у папці. Очікується, що вони також зберігатимуть цю папку у часово-послідовному порядку, і ніколи не зможуть їх видалити. Це встановлює реєстратор близькості для кожного граничного вузла, який можна перехресно зв'язати з реєстраторами інших граничних вузлів.

4.4 Негранічні вузли

Всі вузли вважаються «свідками», включаючи міст, ретранслятор, сховище та вузли аналізу. Це дозволяє пов'язати будь-які дані, які передаються з одного вузла до іншого. Це і є поняття «**пов'язаного свідка»**.

4.5 Перехресне посилання

Аналіз кожного набору «селфі», який створюється і приєднується до кожного вузла, дозволяє системі створювати **найкращу відповідь** з відносної близькості всіх вузлів, що знаходяться в мережі. Якщо кожен вузол звітує чесно та точно, відображення всіх відносних положень граничних вузлів досягне максимально можливої **достовірності** та точності: 100 відсотків. І навпаки, якщо кожен вузол є або нечесним, або пошкодженим, то достовірність і **точність** можуть досягти мінімуму 0 відсотків.

Маючи набір повідомлених даних та запит на відносну позицію одного з граничних вузлів, можна визначити приблизну позицію, а також коефіцієнти достовірності та точності.

Маючи один і той же набір даних та один і той же алгоритм аналізу, кожен розрахунок має прийти до визначення тієї ж приблизної позиції та тих же коефіцієнтів достовірності та точності.

4.6 Діаграма

S’ і S” (рис. 1) - це **страж** (граничний вузол), який збирає евристику. Коли вони контактують один з одним, вони обмінюються **евристичними** даними та відкритими ключами. Вони обидва складають повний запис взаємодії та підписують кінцеву взаємодію. Потім цей підписаний запис стає наступним записом в обох їх локальних реєстрах (16 для S’ і 3 для S”). Ця дія зобов'язує цих двох свідків бути в близькості один від одного.

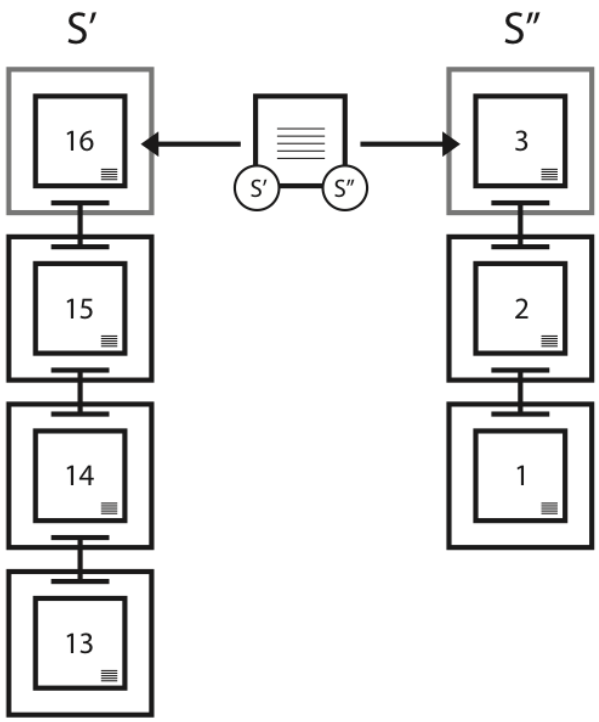

Рисунок 1. Приклад пов'язування свідків між двома стражами

4.7 Ланцюжки походження

Кожне походження зберігає власний реєстр та підписує його для ланцюжка **доказу походження**. Як тільки інформація про ланцюжок доказу походження поширюється, вона одразу стає постійною. Це пов'язано з тим, що форк, який відбувається після поширення, закінчує ланцюжок і робить так, що всі майбутні дані від свідка розглядаються так, ніби вони отримані від

нового свідка. Для того, щоб створити посилання в ланцюжку доказу походження, походження створює пару відкритого/секретного ключів. Потім воно підписує попередні та наступні блоки тією ж парою після включення відкритого ключа в обидва блоки. Одразу після того, як було створено підпис, секретний ключ видаляється. Завдяки негайному видаленню секретного ключа ризик викрадення або повторного використання ключа значно знижується.

Ланцюжки доказу походження є ключовим фактором перевірки того, що реєстри, що входять в **мережу XYO**, є дійсними. Унікальний ідентифікатор для джерела даних не є практичним, оскільки його можна підробити. Підпис секретного ключа не є практичним, оскільки більшість частин мережі XYO важко або неможливо фізично захистити, тому можливість того, що нечесний учасник викраде секретний ключ, є надто реалістичною. Для вирішення цієї проблеми мережа XYO використовує **ланцюжки змінного ключа**. Перевагою їх використання є те, що неможливо сфальсифікувати ланцюжок походження даних. Проте, як тільки ланцюжок розірваний, він рветься назавжди, без можливості продовження, і в результаті перетворюється на острів.

Кожного разу, коли у мережу XYO надходить **евристичний** реєстр, приймач додає власний **доказ походження**, що подовжує ланцюжок доказ походження і створює перехрестя доказів походження. Ланцюжки доказу походження та перехрестя доказів походження є основними показниками, що використовуються **провидцями** для перевірки достовірності реєстру. Рівняння для репутації реєстру – це, фактично, той відсоток мережі XYO, який залучається до створення оцінки доказу походження, пов'язаної з ним. У теорії, якщо 100 відсотків записів мережі XYO пов'язані з доказом походження, а потім повністю проаналізовані, то шанси бути достовірними для них – 100 відсотків. Якщо для аналізу доступні 0% відсотків записів мережі XYO, то достовірність падає до 0 відсотків.

Для додаткової безпеки відкритий ключ для ланки ланцюжка не надається, поки для нього не стане доступний другий запис. Це також дозволяє встановити проміжок часу між записами або іншими даними, що зберігаються в попередній або наступній ланці.

4.8 Оцінка ланцюжка походження

Оцінка ланцюжка походження вираховується наступним чином (алгоритм за замовчуванням):

- PcL = Довжина ланцюжка доказу походження
- PcD = Складність ланцюжка доказу походження
- Pc’ Pc” O = Перекриття ланцюжка доказу походження для Pc’ та Pc”

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

4.9 Дерево походження

Дерево походження використовується для приблизного розрахунку достовірності відповіді. Воно використовує дані, зібрані для створення ідеального дерева, тобто дерева, яке найкраще підходить тим даним для певної отриманої відповіді. Якщо вузол N розташований у місцях X, Y, Z, T, помилка у всіх даних у наборі повинна мати певне значення. Для того, щоб обчислити цю помилку, ми обчислимо МІНІМАЛЬНУ, МАКСИМАЛЬНУ, СЕРЕДНЮ, МЕДІАННУ та УСЕРЕДНЕНУ ВІДСТАНЬ ВІД СЕРЕДНЬОГО ЗНАЧЕННЯ.

Маючи набір S усіх оцінок s, складність **ланцюжка доказу походження** PcD і похибку, **найкраща відповідь** визначається наступним чином:

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

Іншими словами, отримана відповідь, яка має найвищу оцінку **найкращого результату**, є найкращою відповіддю. Використовуючи дерево доказів походження, ми можемо ідентифікувати та зрізати неможливі гілки (показники, що виходять за рамки).

4.10 Утворення ланцюжків змінного ключа

Серію пакетів даних можна об’єднати в один ланцюжок, використовуючи секретні ключі для підпису двох послідовних пакетів. Коли відкритий ключ, об'єднаний із секретним ключем, включається в пакети даних, одержувач може перевірити, чи були обидва пакети підписані тим самим секретним ключем. Дані в пакеті не можуть бути змінені без порушення підпису, що гарантує, що підписані пакети не були змінені іншими сторонами, такими як **міст** або вузол накопичувача.

4.11 Глибина ланки

Як мінімум, вузол генерує нову пару відкритих/секретних ключів для кожної ланки у **ланцюжку доказів походження**, який має глибину ланки 1. У таблиці ланки для певного запису в реєстрі може бути N кількість записів, при чому кожен запис вказуватиме відстань в майбутньому, коли буде додано частину другої ланки. Дві ланки не можуть мати один і той же порядок величин в базі шкали 2. Наприклад, запис [1,3,7,12,39] буде дозволений, а [1,3,7,12,15] ні.

Ланка глибини 1 створюється, використовується та видаляється, коли публікується попередній блок. Проте, ланки глибиною більше 1 мають свою пару, згенеровану під час підпису попереднього блоку, а другий підпис не відбувається, доки не створиться N кількість блоків, після чого секретний ключ видаляється. З цієї причини ланки глибини понад 1 завжди вважаються менш безпечними, ніж ланки глибини 1, але вони можуть бути використані для підвищення продуктивності та зниження втрат даних за рахунок цієї безпеки.

4.12 Фіксований порядок

Ключовим елементом при визначенні послідовності реєстрів є порядок, в якому вони були заповнені. З огляду на те, що пристрій не може змінити порядок будь-якого підписаного реєстру **доказу походження**, абсолютний порядок може бути встановлений шляхом перегляду всіх реєстрів разом.

4.13 Передостання публікація

Основним методом встановлення **доказу походження** ґрунтується на тому, що **страж** завжди записує свій передостанній блок, не записуючи останній блок. Це дозволяє останньому блоку мати підписану ланку до свого попередника як доказ ланки.

4.14 Порожні ланки

Для того, щоб зробити **ланцюжок доказу походження** більш безпечним, необхідно оновлювати ланцюжок не частіше, ніж раз на десять секунд, і не рідше одного разу на кожні шістдесят хвилин. У тому випадку, якщо немає нових даних, в ланцюжок буде додано порожній блок.

4.15 Діаграма

Оскільки час йде зліва направо (рис. 2), **ланцюжок доказу походження,** який будується, стає довшим. У будь-який час будівельник ланцюжка лише надасть викликаючому клієнту записи із затемненими краями, очікуючи на другий підпис запису, перш ніж зробити його доступним. Наприклад, у третьому стовпчику лише записи 2 і 1 будуть повернуті, як частина ланцюжка.

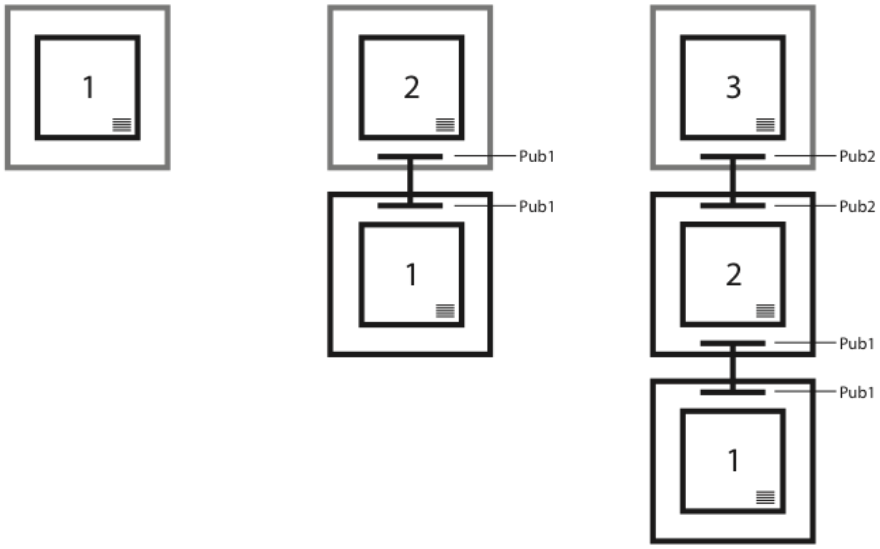

Рисунок 2. Приклад включення ланки в ланцюжок доказу походження

4.16 Резюме

Маючи серії пакетів даних, які підписані в послідовних парах тимчасовими секретними ключами і включають в себе парні відкриті ключі, абсолютно **достовірно** можна визначити, що пакети надходять з одного джерела.

5 Заходи безпеки

5.1 Атака підробного провидця

Через те, що контракт повинен підтвердити цілісність **провидця,** який відправив відповідь, на **смарт-контракт** XYO надсилається набір цифрових підписів. Контракт може потім перевірити інших провидців, які підписали цей список з інтервалом високої достовірності. Без цього оракул-ретранслятор стане єдиним джерелом невдач і ризику всередині системи.

5.2 DDoS-атаки стража

Інша атака, яку подрібно розглянути – це розподілена відмова в обслуговуванні серед вузлів **стража** у визначеному регіоні. Зловмисник може спробувати встановити велику кількість з'єднань зі стражами для того, щоб завадити їх передачі вірної інформації або взагалі всієї інформації на **міст**. Ми можемо обійти цю проблему, вимагаючи, щоб кожен, хто намагається підключитися до стража, повинен буде вирішити маленьку криптографічну загадку. Оскільки запит не включатиме дуже велику кількість підключень до стражів, це не призведе до сильного впливу на систему ретрансляції XYO і вимагатиме від зловмисника витрат великої кількості ресурсів для успішної DDoS-атаки на нашу мережу. В заданий момент часу, **ланцюжок доказу походження** може бути підтверджений будь-ким, оскільки він зберігається в **XYOMainChain**. Це гарантує, що якщо одна одиниця в ланцюжку була скомпрометована, точність відповіді запиту (**оцінка ланцюжка походження**) впаде до 0.

6 Система винагород токенами XYO

Оракули становлять значну частину потреб у потужності та інфраструктурі для децентралізованих застосувань, при цьому більша частина уваги обертається навколо взаємодії та агрегації авторитетних оракулів. Ми вважаємо, що для того, щоб децентралізовані програми досягли максимального потенціалу, необхідна повністю децентралізована система оракулів, що не потребує довіри.

6.1 Криптоекономіка Мережі XYO

Ми використовуємо токени XYO для стимулювання бажаної поведінки надання точної, надійної **евристики** геолокації. Токени XYO можна розглядати як «паливо», необхідне для взаємодії з реальним світом для перевірки XY-координат певного об'єкта.

Процес працює таким чином: Власник токену спочатку надсилає в **мережу XYO** запит (наприклад, «*Де моя посилка електронної комерції з XYO адресою 0x123456789 ...?*»). Потім запит надсилається у чергу, де він чекає обробки та відповіді. Користувач може встановлювати свій бажаний рівень довіри та ціну палива XYO при створенні запиту. Вартість запиту (в токенах XYO) визначається обсягом даних, необхідних для надання відповіді на запит, а також динамікою ринку. Чим більше даних потрібно, тим дорожче запит, і тим вище ціна на паливо XYO. Запити в мережу XYO можуть бути дуже великими та дорогими. Наприклад, логістична компанія могла б надіслати в мережу XYO запит: «Де зараз знаходиться *кожен автомобіль з нашого парку?»*

Коли власник токенів XYO запитує мережу XYO і сплачує запитуване паливо, всі **провидці,** що працюють над завданням, звертаються до відповідних **архіваріусів,** щоб отримати відповідні дані, необхідні для відповіді на запит. Повернені дані отримуються з **мостів**, які спочатку отримали дані у **стражів**. Стражі є, по суті, пристроями або сигналами, які перевіряють місцезнаходження об'єктів. До них відносяться такі об'єкти, як Bluetooth та GPS трекери, геолокаційні компоненти, вбудовані в пристрої IoT, технологія супутникового відстеження, сканери QR-кодів, RFID-сканування та багато інших. Компанія XY Findables стала першопрохідцем і запустила свій бізнес споживчих Bluetooth і GPS присторів, що дозволило їй випробувати та обробити геолокаційну евристику реального світу. Всі зусилля, спрямовані на розвиток спрямованого на споживачів бізнесу XY Findables, значно допомогти у розробці протоколу блокчейн мережі XYO.

Якщо дані, надані пристроєм страж (наприклад, маячок Bluetooth), використовуються для відповіді на запит, то всі чотири компоненти, що беруть участь у транзакції, отримують частину палива XYO, що сплачується власником токенів: провидець (той, хто шукав відповідь), архіваріус (той, що зберігав дані), міст (той, що передавав дані) та страж (той, що записав дані про місцезнаходження). Розподіл палива між 3 з 4 компонентів мережі XYO завжди відбувається в однакових пропорціях. Винятком є провидці, участь яких у процесі надання відповіді є більш широкою. В межах кожного компонента паливо розподіляється порівну.

6.2 Винагорода за незалежність

Пристрої для збору інформації про місцезнаходження є атомними блоками мережі, а окремий пристрій може виступати як один або декілька з чотирьох компонентів системи. Однак нечасто пристрої будуть мати більше двох з цих компонентів, особливо у великій **мережі XYO**. Крім того, блокчейн реєстр, що має більш незалежний **доказ походження,** буде отримувати більше уваги, тому існує **криптоекономічне** покарання для пристрою, який виконує роль декількох компонентів.

6.3 Винагорода за незмінність

Стражам в **мережі XYO** призначається коефіцієнт незмінності за кількість їх руху протягом всього свого життєвого циклу. Чим менше страж рухається протягом певного періоду часу, тим більше його даним можна довіряти. **Архіваріуси** стежать та аналізують ці коефіцієнти незмінності, коли вирішують до яких стражів направляти запити.

6.4 Стимулювання використання токенів

Система, в якій власники токенів заохочуються *не* використовувати свої токени, створює довгострокову проблему для економіки, що лежить в основі системи. Це створює екосистему з дуже малими запасами вартості і викликає природний імпульс винайдення причин *не* використовувати токен замість підвищення практичної цінності та ліквідності.

Проблема більшості **криптоекономічних** стимулів полягає в тому, що фокус занадто сильно зміщений на майнерів токенів (наприклад, **стражі**, **мости**, **архіваріуси**, **провидці**), а не на користувачів токенів. Токен XYO враховує обидва цих аспекти.

Модель токену XYO стимулює майнерів не просто надавати точні дані, але також знати, коли взагалі не надавати дані. Кінцевий користувач стимулюється проводити більше трансакцій тоді, коли ліквідність мережі є низькою, ніж коли ліквідність мережі висока. Таким чином, екосистема токену XYO має здатність залишатися добре збалансованою, життєздатною та надійною.

6.5 Технічні дані токену XYO

Публічний продаж токенів має багаторівневу структуру ціноутворення, яка починається з 1 ETH: 100 000 XYO і досягає межі на 1 ETH: 33 333 XYO. Детальна інформація щодо нашого об'єму та структури ціноутворення з часовим критерієм буде оголошена найближчим часом.

Платформа смарт-контрактів: Ethereum

- Тип контракту: ERC20
- Токен: XYO
- Назва токену: Utility-токен XYO Network
- Адреса токену: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- Сумарна емісія: визначена та обмежується сумою, досягнуту після основного продажу токенів
- Прогнозована капіталізація токену XYO: 48 млн. доларів США
- Нерозпродані та нерозподілені токени: згорають після продажу токенів. Після основного продажу не буде згенеровано ні одного нового токену XYO.

7 Приклади застосування Мережі XYO

Мережа XYO має широке застосування, що охоплює безліч галузей промисловості. Візьмемо, наприклад, компанію електронної комерції, яка зможе запропонувати своїм преміум-клієнтам послугу оплати після доставки. Для того, щоб запропонувати цю послугу, компанія електронної комерції зможе використати мережу XYO (яка використовує токени XYO) для написання **смарт-контракту** (на платформі Ethereum). Мережа XYO зможе потім відстежувати місцезнаходження посилки, яка відправляється споживачеві, на кожному кроці виконання замовлення; від складської полиці до кур'єра, до дому споживача та будь-якого місця між цими пунктами. Це дозволить операторам роздрібної електронної комерції та веб-сайтам перевіряти не тільки той факт, чи з'явилась посилка на порозі клієнта, але і чи безпечно вона дісталась його дому, у спосіб, що не потребує довіри. Після того, як посилка прибула до дому замовника (визначається та підтверджується конкретними XY-координатами), вона вважається виконаною, і проводиться платіж. Таким чином, інтеграція мережі XYO в електронну комерцію дає змогу захистити оператора роздрібної торгівлі від шахрайства та гарантувати, що споживачі платять тільки за товари, що доходять до їх дому.

Розглянемо зовсім іншу інтеграцію мережі XYO в сайт оцінювання готелів, чия проблема полягає в тому, що відгукам часто не довіряють. Природно, що власники готелів стимульовані покращувати свої відгуки за будь-яку ціну. А що, якщо можна буде сказати з надзвичайно високою **достовірністю,** що хтось дійсно був у Сан-Дієго, вилетів на Балі і прожив там у готелі протягом двох тижнів, повернувся в Сан-Дієго, а потім написав відгук про своє перебування на Балі? Відгук матиме дуже високу репутацію, особливо якщо це було написано особою, яка постійно пише відгуки з підтвердженими даними про місцезнаходження.

---

8 Розширення мережі XYO

Нам пощастило побудувати споживчий бізнес, який успішно створив мережу з більш ніж мільйону (1 000 000) Bluetooth і GPS пристроїв в реальному світі. Більшість геолокаційних мереж не можуть досягти цієї фази і наростити критичну масу, необхідну для побудови розгалуженої мережі. Мережа стражів – це лише відправна точка. **Мережа XYO** – це відкрита система, до якої може підключитися будь-який оператор геолокаційних пристроїв і починати заробляти токени XYO.

Як правило, чим більша потужність стражів у мережі XYO, тим надійніше вона. Для подальшого розширення своєї мережі, мережа XYO співпрацює з іншими компаніями для того, щоб розширити мережу стражів за межі власної мережі маячків XY Findables.

9 Подяка

Даний проектний документ є результатом зусиль надихаючої команди, що став можливим завдяки вірі в наше бачення таких осіб, як: Raul Jordan (Рауль Джордан) (випускник Гарвард-коледжу, стипендіат програми Thiel Fellowship та радник **XYO Network**); за його внесок у підготовку більш стислого варіанту нашого проектного документу, що допомогло нам елегантно повідомити його технічні деталі світові. Ми дякуємо Christine Sako (Крістін Сако) за її виняткову робочу етику та увагу до деталей в оцінці нашої роботи. Цілісність структури та слідування успішному досвіду у нашому проектному документі, є результатом зусиль Крістін. Ми дякуємо Johnny Kolasinski (Джонні Коласинські) за його дослідження та підбір прикладів застосування. На завершення, ми дякуємо John Arana (Джон Арана) за ретельну оцінку та творчий внесок.

Посилання

[1] Бланшар, Уолтер. Гіперболічні системи авіаційної радіонавігації. Журнал навігації, 44(3), вересень 1991 р.

[2] Карапетсас, Лефтеріс. Sikorka.io. http://sikorka.io/files/devcon2.pdf. Шанхай, 29 вересня 2016 р.

[3] Ді Ферранте, Метт. Доказ місцезнаходження.
https://www.reddit.com/r/ethereum/comments/539o9c/proof.of.location/. 17 вересня 2016 р.

[4] Говард, Дана. RNT Foundation дає показання перед Конгресом. Слухання в Палаті представників: «Пошук свого шляху: Майбутнє федеральних систем навігації» Вашингтон, ОК, 4 лютого 2014 р.

Словник

Точність Міра впевненості в тому, що точка даних або евристики знаходиться в межах певної похибки.

Архіваріус Архіваріус зберігає евристику як частину децентралізованих даних з метою зберігання всієї історії реєстрів, але без цієї вимоги. Навіть якщо деякі дані втрачаються або стають тимчасово недоступними, система продовжує функціонувати, лише зі зниженою точністю. Архіваріуси також

індексують реєстри, щоб вони за необхідності могли повертати рядок даних реєстру. Архіваріуси зберігають лише вихідні дані та отримують оплату виключно за отримання даних. Зберігання завжди безкоштовне.

Найкраща відповідь Ми визначаємо найкращу відповідь як єдину відповідь серед списку кандидатів на відповідь, яка повертає найвищу оцінку достовірності і має більшу оцінку точності, ніж мінімальна необхідна точність.

Алгоритм найкращої відповіді Алгоритм, який використовується для створення оцінок найкращої відповіді, коли провидець обирає відповідь. Мережа XYO дозволяє додавати спеціалізовані алгоритми і дозволяє споживачу вказувати, який алгоритм використовувати. Потрібно, щоб цей алгоритм отримав таку саму оцінку, як і при опрацюванні будь-яким провидцем за умови однакового набору даних.

Пов'язаний свідок Пов'язаний свідок є концепцією, досягнутою існуванням двонаправленої евристики. Враховуючи, що ненадійне джерело даних не підходить для виконання цифрового контракту (оракул), шляхом встановлення такої евристики суттєво збільшується достовірність даних. Основна двонаправлена евристика є близькістю, оскільки обидві сторони можуть підтвердити виникнення та діапазон взаємодії, підписуючи взаємодію. Це дозволяє отримати доказ з нульовим розповсюдженням про те, що два вузли знаходились в безпосередній близькості один від одного.

Міст Міст – це транскриптор евристики. Він безпечно передає евристичні реєстри від стражів до провидців. Найважливішим аспектом моста є те, що провидець може бути впевненим в тому, що евристичні реєстри, отримані від мосту, ніяким чином не були змінені. Другий найважливіший аспект мосту – це прикріплення додаткових метаданих доказу походження.

Достовірність Оцінка ймовірності того, що точка даних або евристика не була скомпрометована або зламана.

Криптолокація Область застосування технології криптографічного місцезнаходження.

Криптоекономіка Формальна дисципліна, яка вивчає протоколи, які керують виробництвом, розподілом та споживанням товарів і послуг в умовах децентралізованої цифрової економіки. Криптоекономіка – це практична наука, яка фокусується на розробці та характеристиці цих протоколів.

Провидець Провидець відповідає на надісланий запит, аналізуючи попередні дані, що зберігаються в мережі XYO. Евристика, що зберігається в мережі XYO, повинна мати високий рівень доказу походження для визначення достовірності та точності евристики. Провидець отримує та надає відповідь, виходячи з оцінки свідка на підставі його доказу походження. Враховуючи те, що мережа XYO не потребує довіри, провидці повинні бути зацікавленими у забезпеченні чесного аналізу евристики. На відміну від стражів та мостів, для додавання відповідей у блокчейн провидці використовують доказ виконаної роботи.

Евристика Точка даних про реальний світ по відношенню до позиції стража (близькість, температура, світло, рух тощо ...).

Оракул Частина DApp (децентралізованого додатку), яка відповідає за виконання цифрового контракту, надаючи точну та достовірну відповідь. Термін «оракул» походить з криптографії, де він означає істинно випадкове джерело (наприклад, випадкового числа). Він забезпечує необхідні ворота між крипто рівнянням та світом за його межами. Оракули надсилають на смарт-контракти інформацію з-поза ланцюжка (з реального світу). Оракули – це інтерфейси між цифровим та реальним світами. В якості сумного прикладу, розглянемо договір про заповіт. Умови заповіту виконуються після підтвердження того, що заповідач помер. Шляхом компонування та агрегування відповідних даних з офіційних джерел, можна вбудувати оракул, який давав би старт виконанню заповіту. Оракул потім може використовуватися як канал або кінцева точка, до якої звертався б смарт-контракт, щоб перевірити, чи померла людина.

Оцінка ланцюжка походження Оцінка, яка присвоюється ланцюжку походження для визначення його достовірності. Ця оцінка бере до уваги довжину, переплетення, перекриття та надмірність.

Дерево походження Набір даних записів реєстру, взятих з різних ланцюжків походження для визначення походження евристики реєстру з певним рівнем достовірності.

Доказ походження Доказ походження – це ключовий фактор перевірки того, що реєстри, що входять в **мережу XYO**, є дійсними. Унікальний ідентифікатор для джерела даних не є практичним, оскільки його можна підробити. Підпис секретного ключа не є практичним, оскільки більшість частин мережі XYO важко або неможливо фізично захистити, тому можливість того, що нечесний учасник викраде секретний ключ, є надто реалістичною. Для вирішення цієї проблеми мережа XYO використовує ланцюжки змінного ключа. Перевагою їх використання є те, що неможливо сфальсифікувати ланцюжок походження даних. Проте, як тільки ланцюжок розірваний, він рветься назавжди, без можливості продовження, і в результаті перетворюється на острів.

Ланцюжок доказу походження Ланцюжок перехідних ключів, який зв'язує разом серію пов'язаних свідків евристичних записів реєстру.

Доказ виконаної роботи Доказ виконаної роботи – це частина даних, що відповідає певним вимогам, її важко створити (тобто дорого, забирає багато часу), але легко перевірити будь-кому. Створення доказів виконаної роботи може бути випадковим процесом із низькою ймовірністю генерації, щоб для створення достовірного доказу виконаної роботи необхідно було застосувати ретельний метод проб та помилок.

Страж Страж – це евристичний свідок. Він спостерігає за евристикою та відповідає за достовірність і точність, створюючи тимчасові реєстри. Найважливіший аспект стража полягає в тому, що він створює реєстри, у яких провидці можуть бути впевнені в тому, що вони походять з одного й того ж джерела, додаючи до них доказ походження.

Смарт-контракт Протокол, сформульований Ніком Сабо задовго до Bitcoin, приблизно у 1994 році (саме тому дехто вважає, що він і є Сатоші Накамото – містичний і невідомий винахідник Bitcoin). Ідея смарт-контрактів полягає в кодифікації правової угоди в рамках програми, щоб

децентралізовані комп'ютери виконували її умови замість того, щоб інтерпретувати та виконувати їх приходилось людям. Смарт-контракти вкладають гроші (наприклад, Ether) та контракти в одну концепцію. Враховуючи те, що смарт-контракти є детерміністичними (як комп'ютерні програми) і повністю прозорими та зрозумілими, вони служать потужним замінником для посередників та брокерів.

Ланцюжок змінних ключів Ланцюжок змінних ключів об'єднує серію пакетів даних за допомогою криптографії зі змінним ключем

Не потребує довіри Така характеристика, коли всі сторони в системі можуть досягти консенсусу щодо того, що є канонічною істиною. Потужність та довіра розподіляються (або поширюються) серед зацікавлених сторін мережі (наприклад, розробники, майнери та споживачі), а не концентруються в одній фізичній чи юридичній особі (наприклад, в банках, урядах та фінансових установах). Це загальний термін, який легко можна неправильно зрозуміти. Блокчейни насправді не усувають довіру. Їх робота полягає в мінімізації кількості довіри, яка вимагається від будь-якого окремого учасника системи. Це досягається шляхом поширення довіри серед різних учасників системи через економічну гру, яка стимулює суб'єктів співпрацювати за правилами, визначеними протоколом.

XY Oracle Network XYO Network

Мережа XYO Мережа XYO розшифровується, як «Мережа оракулів XY». Вона включає всю систему компонентів/вузлів XYO, до складу яких входять стражі, мости, архіваріуси та провидці. Основна функція мережі XYO – бути порталом, за допомогою якого цифрові смарт-контракти можуть виконуватися через підтвердження географічного розташування в реальному світі.

XYOMainChain Незмінний блокчейн в мережі XYO, який зберігає транзакції запитів разом з даними, отриманими від провидців, та пов'язаним з ними балом походження.