Buku Putih XYO Network: Jaringan Lokasi Kriptografi Berbasiskan Proof-of-Origin

Oleh Arie Trouw*, Markus Levin†, Scott Scheper‡

Januari 2018

Abstraksi

Dengan semakin berkembangnya teknologi yang terkoneksi dan bergantung pada lokasi, privasi dan keselamatan kita sangat bergantung pada akurasi dan kesahihan informasi lokasi. Berbagai upaya telah dilakukan untuk meniadakan kebutuhan akan entitas sentral untuk mengontrol arus data lokasi, tapi semua upaya itu tergantung pada keandalan perangkat yang mengumpulkan data ini di dunia nyata. Kami mengusulkan suatu jaringan lokasi kriptografi yang trustless dengan formulasi baru yang mengandalkan bukti nol pengetahuan untuk menetapkan tingkat kepastian data yang tinggi mengenai informasi lokasi. XYO Network (XY Oracle Network) merupakan abstraksi yang memungkinkan verifikasi lokasi berlapis di berbagai kelas dan protokol perangkat. Pada titik intinya terdapat seperangkat mekanisme kriptografi baru yang dinamakan Proof of Origin & Bound Witness yang menyatukan kekuatan teknologi blockchain dengan pengumpulan data dunia nyata ke dalam sistem dengan penerapan langsung dewasa ini.

1 Pengantar

Dengan kelahiran kontrak cerdas trustless berbasis blockchain, kebutuhan akan layanan oracle yang menentukan hasil suatu kontrak telah tumbuh secara signifikan. Kebanyakan penerapan kontrak cerdas saat ini bergantung pada seperangkat oracle otoritatif tunggal atau teragregasi untuk menetapkan hasil suatu kontrak. Dalam kasus di mana kedua belah pihak sependapat tentang otoritas dan sifat tidak dapat dikorup pada oracle yang ditentukan, hal itu sudah cukup. Namun begitu, dalam kebanyakan kasus, tidak ada oracle yang tepat atau oracle tidak bisa dianggap otoritatif karena adanya kemungkinan salah atau korup.

Oracle lokasi masuk ke dalam kategori ini. Ramalan tentang lokasi item dunia fisik bergantung pada pelaporan, relai, penyimpanan, dan komponen pemrosesan pada oracle tertentu, di mana pada semuanya bisa terdapat kesalahan dan bisa dibuat korup. Risiko meliputi manipulasi data, polusi data, kehilangan data, dan kolusi.

Oleh karena itu terdapat masalah berikut ini: baik kepastian maupun keakuratan lokasi secara negatif terdampak oleh kurangnya oracle lokasi yang trustless dan terdesentralisasi. Platform seperti Ethereum dan EOS telah digunakan secara luas karena kekuatannya untuk menjadi perantara interaksi online secara aman di mana kasus penggunaan utama melibatkan escrow untuk penggalangan dana escrow dalam bentuk ICO. Namun hingga saat ini setiap platform telah berfokus sepenuhnya pada dunia online dan bukan pada dunia fisik karena integritas data pada saluran informasi saat ini yang terlalu gaduh dan dapat dikorup.

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

XYO Network telah mengupayakan konsep pemberdayaan pengembang, seperti mereka yang menulis kontrak cerdas untuk platform blockchain, untuk berinteraksi dengan dunia nyata seakan-akan itu adalah API. XYO Network adalah protokol oracle pertama di dunia yang memungkinkan dua entitas untuk bertransaksi di dunia nyata tanpa perlu adanya pihak ketiga sentral. Abstraksi kami memungkinkan kami membuat verifikasi lokasi menjadi trustless bagi pengembang, sehingga menciptakan suatu protokol dengan kasus penggunaan baru yang sebelumnya tidak mungkin.

XYO Network akan dibangun di infrastruktur yang ada saat ini pada 1.000.000 lebih perangkat yang beredar di dunia yang didistribusikan melalui bisnis findables mereka yang berhadapan langsung dengan konsumen. Perangkat Bluetooth dan GPS XY memungkinkan konsumen setiap hari menaruh beacon pelacakan fisik pada barang-barang yang ingin mereka lacak (seperti kunci, bagasi, sepeda dan bahkan hewan peliharaan).

---

2 Latar Belakang Historis & Pendekatan Sebelumnya

2.1 Bukti Lokasi

Konsep lokasi yang dapat dibuktikan telah ada sejak sekitar tahun 1960-an, dan bahkan bisa dirunut hingga tahun 1940-an dengan sistem navigasi radio berbasis darat, seperti LORAN [1]. Dewasa ini, terdapat layanan lokasi dengan medium verifikasi yang saling bertumpukan untuk membuat Bukti Lokasi melalui triangularisasi dan layanan GPS. Namun begitu, pendekatan ini belum menyentuh komponen paling krusial yang kita hadapi pada teknologi lokasi dewasa ini: merancang suatu sistem yang mendeteksi sinyal yang mengelabui dan menghalangi terjadinya pemalsuan (spoofing) data lokasi. Untuk alasan ini, kami mengusulkan agar platform lokasi kripto paling signifikan dewasa ini menjadi platform yang paling fokus dalam membuktikan asal sinyal lokasi fisik.

Yang mengejutkan, konsep penerapan verifikasi lokasi ke teknologi blockchain pertama kali mengemuka pada September 2016 di DevCon 2 Ethereum. Itu diperkenalkan oleh Lefteris Karapetsas, seorang pengembang Ethereum dari Berlin. Proyek Karapetsas, Sikorka, memungkinkan kontrak cerdas dikerahkan secara serta-merta di dunia nyata, dengan menggunakan apa yang disebutnya, “Bukti Kehadiran.” Penerapan yang dilakukannya dalam menjembatani lokasi dan dunia blockchain utamanya berfokus pada kasus penggunaan realitas tertambah; dan ia memperkenalkan konsep baru seperti pertanyaan tantangan dalam membuktikan lokasi seseorang [2].

Pada 17 September 2016, istilah, “Bukti Lokasi,” secara resmi mengemuka di komunitas Ethereum [3]. Itu kemudian diuraikan secara lebih terperinci oleh pengembang Ethereum Foundation, Matt Di Ferrante:

> *“Bukti Lokasi yang dapat Anda percayai sejujurnya merupakan salah satu hal yang paling sulit untuk diterapkan. Sekalipun Anda memiliki banyak peserta yang dapat saling membuktikan lokasi masing-masing, tidak ada jaminan bahwa mereka tidak akan menerka saja suatu saat nantinya, dan karena Anda selalu mengandalkan pelaporan mayoritas, itu adalah kelemahan yang sangat serius. Jika Anda dapat mensyaratkan sejenis perangkat keras khusus yang memiliki teknologi anti-tamper (tidak bisa diotak-atik) seperti misalnya kunci privat yang hancur ketika seseorang mencoba membukanya atau mengubah firmware yang terdapat padanya, maka Anda mungkin dapat memiliki keamanan yang lebih besar, tapi pada saat yang sama, tampaknya bukan hal yang tidak mungkin untuk memalsukan sinyal GPS. Penerapan hal ini secara tepat mengharuskan begitu banyak pengembalian (fallback) dan begitu banyak data yang berbeda sehingga tidak bisa didapatkan kepastian akurasi sehingga proyek ini benar-benar harus didanai dengan sangat baik.”[3]*
>
> *—Matt Di Ferrante, Pengembang, Ethereum Foundation*

2.2 Bukti Lokasi: Kekurangan

Secara ringkas, Bukti Lokasi dapat dipahami sebagai pemanfaatan fitur mumpuni blockchain, seperti pemberian cap waktu dan desentralisasi, serta menggabungkannya dengan perangkat luar rantai, yang mengerti lokasi, yang diharapkan resisten terhadap pemalsuan. Kami menyebut dunia teknologi lokasi kriptografi sebagai "lokasi kripto." Lebih lanjut, mirip dengan bagaimana kelemahan kontrak cerdas berkisar pada oracle dengan menggunakan satu sumber kebenaran (dan oleh karenanya memiliki satu sumber kegagalan), sistem lokasi kripto juga menghadapi masalah yang sama. Kerentanan teknologi lokasi kripto saat ini berkisar pada perangkat luar rantai yang melaporkan kembali lokasi objek. Dalam kontrak cerdas, sumber data luar rantai ini adalah oracle. Di XYO Network, sumber data luar rantai bergerak di dunia nyata sebagai suatu jenis oracle khusus yang kami sebut Sentinel. Inovasi inti seputar XYO Network berkisar pada bukti berbasis lokasi tanpa identitas yang mendasari komponen sistem kami untuk membuat protokol lokasi kripto yang trustless.

---

3 XY Oracle Network

> *"Kebutuhan akan sistem yang sulit didisrupsi untuk melengkapi GPS telah diketahui selama bertahun-tahun. GPS luar biasa akurat dan dapat diandalkan, namun jamming, pemalsuan, serangan siber dan bentuk interferensi lainnya semakin berkembang frekuensi dan keparahannya. Ini berpotensi menghancurkan kehidupan dan aktivitas ekonomi kita." [4]*
>
> *— Dana Goward, President, RNT Foundation*

3.1 Pengantar

Tujuan XYO Network adalah menciptakan suatu sistem oracle lokasi yang trustless dan terdesentralisasi yang tahan serangan dan menghasilkan tingkat kepastian yang setinggi mungkin ketika dikirimi kueri mengenai data yang tersedia. Kami mencapai hal ini melalui seperangkat abstraksi sangat mengurangi risiko pemalsuan lokasi melalui rantai bukti nol pengetahuan beserta komponen sistem.

3.2 Tinjauan Jaringan

Sistem kami memberikan titik entri ke protokol perangkat terhubung yang memberikan tingkat kepastian yang tinggi tentang data lokasi melalui rantai bukti kriptografi. Pengguna dapat mengeluarkan transaksi, yang dinamakan "kueri," untuk mengambil data lokasi di platform blockchain mana pun yang memiliki fungsionalitas kontrak cerdas.[1] Agregator dari XYO Network kemudian mendengarkan kueri yang dikeluarkan untuk kontrak dan mengambil jawaban yang memiliki tingkat akurasi tertinggi dari suatu set perangkat terdesentralisasi yang merelai bukti kriptografi kembali agregator ini. Agregator ini kemudian mengumpan jawaban tersebut kembali ke kontrak cerdas setelah mencapai konsensus mengenai jawaban dengan skor terbaik. Jaringan komponen ini memungkinkan untuk menentukan apakah suatu objek berada di suatu koordinat XY tertentu pada suatu waktu, dengan tingkat kepastian trustless yang bisa dibuktikan semaksimalnya.

---

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counterparty, Monax and others

XYO Network memiliki empat komponen utama: Sentinel (Pengumpul Data), Bridge (Perelai Data), Archivist (Penyimpan Data), dan Diviner (Agregator Jawaban). Sentinel mengumpulkan informasi lokasi melalui sensor, radio dan sarana lain. Bridge mengambil data ini dari Sentinel dan menyediakannya bagi Archivist. Archivist menyimpan informasi ini untuk dianalisis oleh Diviner. Diviner menganalisis heuristik lokasi dari Archivist untuk menghasilkan jawaban terhadap kueri dan menetapkan skor akurasi terhadapnya. Diviner kemudian merelai jawaban ini kembali ke kontrak cerdas (dengan demikian, Diviner bertindak sebagai oracle). Rantai ini menjamin dua data atau lebih yang berasal dari sumber yang sama tanpa mengungkapkan informasi yang melatarinya. Setiap komponen di sepanjang jalur kueri menghasilkan kuerinya sendiri yang kemudian dirantaikan ke setiap komponen yang direlainya dengan data. Proof of Origin adalah suatu formulasi baru yang membangun rantai jaminan kriptografi di sepanjang jalur perelai di jaringan untuk menawarkan tingkat keyakinan yang tinggi mengenai data dunia nyata. Proof of Origin Chain ini meringkas keyakinan yang kita miliki pada suatu data lokasi hingga ke perangkat pertama yang mengumpulkan data itu. Kita akan mengeksplorasi bagaimana cara kerja Proof of Origin secara mendalam pada bagian berikut ini.

Untuk menetapkan mekanisme konsensus terdesentralisasi di antara Diviner, XYO Network akan bergantung pada blockchain publik abadi yang disebut XYOMainChain yang menyimpan transaksi kueri beserta data yang dikumpulkan dari Diviner dan skor asalnya yang terkait. Sebelum kita menelaah rincian fungsionalitas seluruh sistem, kita akan menetapkan secara jelas tanggung jawab masing-masing komponen di jaringan kita.

3.2.1 Sentinel

Sentinel adalah saksi lokasi. Sentinel mengawasi heuristik data dan menjamin kepastian serta keakuratan heuristik tersebut dengan membuat ledger sementara. Aspek terpenting Sentinel adalah menghasilkan ledger yang meyakinkan komponen lain bahwa itu berasal dari sumber yang sama. Sentinel melakukan ini dengan menambahkan Proof of Origin ke rantai relai bukti kriptografi. Mengingat XYO Network merupakan sistem trustless, Sentinel harus diberi insentif agar memberikan informasi lokasi yang jujur. Hal ini dilakukan dengan menggabungkan komponen reputasi dengan komponen pembayaran. Sentinel diberi hadiah XYO Network Token (XYO) ketika informasinya digunakan untuk menjawab kueri. Untuk meningkatkan kemungkinan diberi hadiah, sentinel harus membuat ledger yang konsisten dengan ledger peer-nya dan memberikan Proof of Origin untuk mengidentifikasi diri sebagai sumber informasi lokasi.

3.2.2 Bridge

Bridge adalah transcriber data lokasi. Bridge secara aman merelai ledger lokasi dari Sentinel ke Archivist. Aspek terpenting sebuah Bridge adalah meyakinkan Archivist bahwa ledger heuristik yang diterima dari suatu Bridge belum diubah sedikit pun. Aspek terpenting kedua adalah Bridge memberikan Proof of Origin tambahan. Mengingat XYO Network merupakan sistem trustless, Bridge harus diberi insentif agar menyediakan relai heuristik yang jujur. Hal ini dilakukan dengan menggabungkan komponen reputasi dengan komponen pembayaran. Bridge diberi hadiah XYO Network Token (XYO) ketika informasi yang telah direlainya digunakan untuk menjawab kueri. Untuk meningkatkan kemungkinan diberi hadiah, bridge harus membuat ledger yang konsisten dengan ledger peer-nya dan memberikan Proof of Origin untuk mengidentifikasi diri sebagai relai heuristik.

3.2.3 Archivist

Archivist menyimpan informasi lokasi dari Bridge dalam bentuk yang terdesentralisasi dengan tujuan agar semua ledger historis tersimpan. Meskipun ada data yang hilang atau sementara waktu tidak tersedia, sistem terus berfungsi, hanya saja akurasinya menurun. Archivist juga mengindeks ledger agar bisa secara mudah mengembalikan string data ledger jika dibutuhkan. Archivist menyimpan data mentah saja dan mendapat bayaran Token XYO Network hanya untuk pengambilan data dan penggunaan selanjutnya. Penyimpanan selalu gratis.

Archivist merupakan tersusun dalam suatu jaringan, sehingga meminta satu Archivist akan mengakibatkan Archivist itu meminta Archivist yang lain untuk data yang tidak dimilikinya. Archivist dapat memilih untuk menyimpan informasi ledger yang dikembalikan kepadanya. Hal ini kemungkinan besar akan memunculkan dua jenis Archivist: satu yang berada pada pinggir produksi data “awan” dan satu lagi pada pinggir konsumsi data “awan.” Archivist yang berada di tengah adalah hibrida. Pilihan untuk menyimpan data tidak diberlakukan, tapi dapat secara mudah

dilakukan melalui IPFS atau solusi penyimpanan lain yang terdesentralisasi. Setiap kali data diteruskan dari satu Archivist ke yang lain, Proof of Origin tambahan dilampirkan untuk melacak pembayaran, karena semua Archivist mendapatkan pembayaran. Untuk pengambilan, level Proof of Origin minimum dapat ditetapkan untuk meningkatkan validitas. Kepentingan Sentinel, Bridge, dan Archivist harus diselaraskan untuk mencegah pembengkakan data.

3.2.4 Diviner

Diviner adalah bagian paling kompleks dari XYO Network. Secara keseluruhan tujuan Diviner adalah mengambil data paling akurat untuk kueri dari XYO Network dan merelai data itu kembali ke penerbit kueri. Diviner meminta suara dari platform blockchain platform yang berlaku (misalnya., Ethereum, Stellar, Cardano, IOTA, dll.) untuk kueri yang dikeluarkan bagi kontrak cerdas XYO. Kemudian, diviner mencari jawaban terhadap kueri dengan berinteraksi langsung dengan jaringan Archivist untuk mengambil jawaban dengan skor keakuratan/keyakinan paling tinggi. Diviner melakukan ini dengan menilai saksi yang memiliki Proof of Origin terbaik. Diviner yang mengambil jawaban dengan skor terbaik dalam waktu yang paling singkat akan memiliki kemampuan untuk membuat blok di blockchain XYO utama (XYOMainChain) melalui Proof-of-Work. Kueri diprioritaskan berdasarkan ukuran dan kompleksitas hadiah, jadi semakin banyak XYO yang ditawarkan untuk suatu jawaban, maka semakin tinggi pula prioritas kueri tersebut.

Diviner lain mencapai konsensus mengenai kesahihan blok dan secara digital menandatangani blok. Diviner yang merupakan alamat coinbase di blok itu kemudian akan mengirimkan transaksi ke kontrak cerdas yang mengandung jawaban beserta skor keakuratannya. Diviner juga akan mengirim daftar tanda tangan Diviner yang lain untuk mencegah penyerang mengeluarkan informasi palsu ke dalam blockchain dengan berpura-pura sebagai Diviner. Kontrak cerdas kemudian dapat memverifikasi integritas informasi ini dengan memeriksa daftar tanda tangan payload.

3.3 Fungsionalitas Menyeluruh

Setelah tanggung jawab masing-masing komponen itu diuraikan, berikut ini adalah contoh lengkap cara kerja sistem:

1. **Sentinel Mengumpulkan Data**
    - Sentinel mengumpulkan heuristik lokasi dunia nyata dan menyiapkan Proof of Origin miliknya untuk dirantaikan ke node di atasnya.
2. **Bridge Mengumpulkan Data dari Sentinel**
    - Bridge mengumpulkan data yang diperlukan dari Sentinel online dan melampirkan Proof of Origin ke rantainya. Bridge kemudian menjadi tersedia bagi Archivist di Jaringan.
3. **Archivist Mengindeks/Mengumpulkan Data dari Bridge**
    - Bridge secara terus-menerus mengirim informasi kepada Archivist yang kemudian disimpan secara terdesentralisasi beserta indeks heuristik lokasi.
4. **Diviner Mengambil Kueri Pengguna**
    - Diviner meminta suara untuk kueri yang dikirim ke kontrak cerdas Ethereum dan memutuskan untuk memulai proses formulasi jawaban.
5. **Diviner Mengumpulkan Data dari Archivist**
    - Diviner kemudian memutuskan untuk menjawab kueri dengan mengambil informasi sesuai yang diperlukan dari jaringan Archivist.
6. **Diviner Merumuskan Jawaban**

- Diviner akan memilih Best Answer terhadap kueri dari jaringan Archivist yang mengandung Origin Chain Score terbaik.

7. **Diviner Mengusulkan Blok**
    - Diviner kemudian mengusulkan blok diXYOMainChain yang mengandung konten jawaban, kueri, dan Token XYO (XYO) yang dibayarkan melalui Proof of Work. Diviner lain di jaringan akan menandatangani konten blok secara digital, lalu nonce akun Diviner coinbase diperbarui untuk memperlihatkan Proof of Work-nya dalam sistem begitu konsensus mengenai blok yang sah tercapai.
8. **Diviner Mengembalikan Hasil ke Pemrakarsa Kueri**
    - Diviner mengemas jawaban, Origin Chain Score, dan seperangkat tanda tangan digitalnya lalu mengirimnya ke komponen adaptor yang secara aman terhubung ke kontrak cerdas XYO. Adaptor yang bertugas memastikan integritas Diviner belum diretas dan mengirim serangkaian jawaban yang ditandatangani secara digital ke kontrak cerdas. Hal ini terjadi langsung setelah proses pembuatan blok. Diviner coinbase kemudian dibayar atas upayanya.
9. **Komponen XYO Diberi Hadiah atas Hasil Kerjanya**
    - Komponen di sepanjang Proof of Origin Chain dibayar untuk keterlibatannya dalam mengambil jawaban terhadap kueri. Sentinel, Bridge, Archivist, dan Diviner semuanya diberi hadiah atas hasil kerjanya.

Dalam kasus kueri yang sama diminta lebih dari sekali, mungkin jawaban yang dihasilkan lebih dari satu karena jawaban yang dihasilkan pada suatu waktu tertentu didasarkan atas heuristik yang tersedia yang dapat ditawarkan sistem pada saat itu. Mengirimkan jawaban ke blockchain akan memerlukan dua langkah. Pertama, suatu analisis harus dilakukan untuk menentukan Best Answer terhadap kueri. Jika ada banyak jawaban yang dihasilkan oleh sistem, maka node akan membandingkan jawaban dan akan selalu memilih jawaban yang lebih baik. Contoh kueri yang sederhana adalah seperti ini: “Di mana node di jaringan pada waktu tertentu di masa lalu?”

3.4 Blockchain sebagai Suatu Kebenaran Tunggal

Pada titik intinya, Diviner hanya sekadar mengubah data relatif menjadi data mutlak. Diviner mampu mengeksplorasi seluruh jaringan Archivist untuk menkonkretkan jawaban mutlak terhadap kueri di XYO Network. Diviner juga merupakan node yang mengusulkan dan menambahkan blok ke XYOMainChain, dan mendapatkan hadiah untuk Proof-of-Work-nya. Karena jaringan Archivist adalah tempat penyimpanan data yang belum diproses dan blockchain adalah tempat penyimpanan data mutlak yang telah diproses, jaringan pada akhirnya dapat menggunakan informasi terkini di XYOMainChain untuk menjawab kueri mendatang sehingga tidak bergantung pada komputasi mahal Jaringan Archivist.

Karena blok di XYOMainChain menyimpan Proof of Origin Chain dan grafik komponen yang digunakan untuk menjawab kueri, Diviner mendatang dapat mengeksplorasi data mutlak ini untuk mencapai hasil yang akurat dengan penggunaan bandwidth yang lebih rendah. Dengan demikian, XYOMainChain secara perlahan-lahan akan menjadi sumber kebenaran sistem paling penting. Namun begitu, jaringan Archivist masih akan diharuskan menjaga kemutakhiran informasi mengenai heuristik lokasi yang dikumpulkan oleh Sentinel.

3.5 Kerangka XYO Network untuk Memilih Bakal Best Answer

Kami mendefinisikan Best Answer sebagai jawaban tunggal, di antara Daftar Bakal Jawaban, yang mengembalikan skor kesahihan tertinggi dan memiliki skor keakuratan yang lebih tinggi dibandingkan keakuratan minimum yang disyaratkan. Skor kesahihan didasarkan atas Origin Chain Score. Sistem mengetahui Origin Score tertinggi, yang adalah 100 persen hingga nanti dicapai skor yang lebih tinggi, yang kemudian akan menjadi 100 persen yang baru. XYO Network memungkinkan pemilihan Best Answer Algorithm untuk menentukan Best Answer. Hal ini akan memberikan pengembangan untuk riset mendatang mengenai algoritme alternatif.

Ketika data dikecualikan dari suatu jawaban karena dianggap buruk atau salah, data itu akan diedarkan ke archivist agar dapat dibersihkan dari tempat penyimpanannya yang terdesentralisasi.

3.6 Integrasi Awal dengan Blockchain Publik

XYO Network dirancang untuk menjadi abstraksi yang dapat berinteraksi dengan blockchain publik dan kapabel kontrak cerdasseperti Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano dan yang lain. Untuk berinteraksi dengan XYO Network, pengguna di Ethereum, misalnya, dapat mengeluarkan kueri untuk kontrak cerdas XYO kami dan membayar dalam Token XYO (ERC20). Node di Blockchain XYO kami sendiri, yang dinamakan Diviner, akan terus-menerus meminta suara Ethereum untuk semua kueri ini dan akan diberi hadiah dalam mata uang asli Blockchain XYO kami (disebut juga Token XYO). Di masa mendatang, kami akan melakukan konversi langsung (one-to-one) dari pemilik token ERC20 kami ke mata uang asli blockchain kami untuk memberikan biaya transaksi bagi platform kami yang mendukung ketentuan pembayaran mikro yang diperlukan untuk kasus penggunaan IoT yang terukur. Dalam kasus ini, kami akan mengizinkan pengguna untuk mengeluarkan kueri langsung ke blockchain kami alih-alih berinteraksi melalui kontrak cerdas publik.

---

4 Proof of Origin

Dengan jaringan fisik yang terdiri atas node yang tak tepercaya, dimungkinkan untuk menentukan kepastian data yang telah disediakan oleh node tepi berdasarkan bukti nol pengetahuan bahwa dua data atau lebih berasal dari sumber yang sama. Dengan menggunakan seperangkat data ini, yang dikombinasikan dengan sejumlah rangkaian data serupa dan pengetahuan mengenai minimal satu lokasi mutlak node, lokasi mutlak node lain dapat dipastikan.

4.1 Pengenalan Proof of Origin

Ini sesuai asumsi bahwa node di jaringan yang menandatangani data dimaksud memang aman secara fisik maupun virtual. Namun begitu, jika kunci privat diretas, maka kemampuan membuktikan asal menjadi limbung.

Ketika menerapkan konsep trustless pada Internet of Things, harus diasumsikan bahwa node tepi pada jaringan tidak aman secara fisik atau virtual. Hal ini memunculkan kebutuhan untuk mengidentifikasi node tepi tanpa penggunaan ID unik dan untuk, sebagai gantinya, menilai data yang dihasilkan olehnya sebagai data jujur dan sahih tanpa pengetahuan apa pun dari luar jaringan.

4.2 Titik Inti Proof of Origin: Bound Witness

Proof of Origin mengandalkan konsep Bound Witness. Mengingat sumber data tidak tepercaya yang digunakan untuk menyelesaikan kontrak digital (oracle) tidak bermanfaat, kami bisa secara signifikan meningkatkan kepastian data yang disediakan dengan pertama-tama menetapkan keberadaan bukti lokasi dua arah. Heuristik lokasi dua arah utama adalah proksimitas, karena kedua pihak bisa memvalidasi kemunculan dan rentang interaksi dengan turut menandatangani interaksi. Hal ini memungkinkan bukti nol pengetahuan bahwa dua node saling berdekatan.

Kami kemudian perlu menentukan kepastian bahwa oracle menyaksikan node di sistem trustless mengumpulkan data yang dibaginya. Dalam suatu sistem trustless, node saksi bisa karena cacat atau korup menghasilkan data yang salah. Data yang tidak valid bisa dideteksi dan dihapus jika itu berada di luar rentang yang diizinkan untuk heuristik itu. Data yang valid namun salah (yaitu data palsu) jauh lebih sulit dideteksi.

4.3 Heuristik Lokasi Satu Arah vs. Dua Arah

Sebagian besar data yang terkait dengan dunia fisik (heuristik) bersifat satu arah. Hal ini berarti bahwa unsur yang sedang diukur tidak bisa mengukur balik, sehingga menjadikan data heuristik satu arah sangat sulit untuk divalidasi. Heuristik dua arah adalah lokasi di mana unsur yang diukur dapat melaporkan kembali pengukurannya ke pihak lain, sehingga validasi dimungkinkan. Lokasi adalah heuristik langka karena bisa bersifat dua arah, di mana dua node tepi saling melapor. Contohnya di dunia nyata adalah dua orang yang berdekatan melakukan swafoto, mencetak foto untuk dipegang masing-masing, dan kemudian keduanya menandatangani hasil swafoto tersebut. Proses ini akan memberi kedua belah pihak Bukti Proksimitas. Satu-satunya cara bagi kedua orang ini untuk mendapatkan “data” ini adalah karena keduanya sama-sama berada di lokasi yang sama.

Selanjutnya, mari kita bahas efek jaringan: Bayangkan suatu sistem di mana setiap node tepi diperkirakan akan senantiasa menghasilkan “swafoto” ini ketika berkeliling, dan menyimpannya di binder. Node itu juga diperkirakan akan menyimpan binder itu sesuai urutan waktu dan tidak pernah diizinkan untuk menghapus satu pun. Hal ini akan menetapkan perekam proksimitas untuk masing-masing node tepi yang dapat dirujuk silang dengan perekam node tepi lain.

4.4 Node Non-Tepi

Semua node dianggap “saksi,” termasuk node Bridge, relai, penyimpanan, dan analisis. Hal ini memungkinkan diikatnya setiap data yang direlai dari satu node ke node berikutnya. Inilah konsep Bound Witness.

4.5 Rujukan Silang

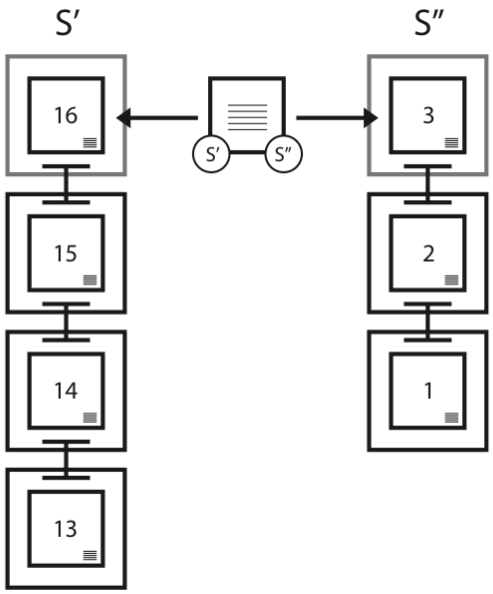
Penganalisisan setiap set “swafoto” yang dihasilkan dan dirantai bersama oleh setiap node tepi akan memungkinkan sistem untuk menghasilkan Best Answer dari proksimitas relatif semua node yang ada di jaringan. Jika setiap node melaporkan secara jujur dan akurat, pemetaan semua posisi relatif node tepi akan mencapai kepastian dan keakuratan semaksimum mungkin: 100 persen. Sebaliknya, jika setiap node tidak jujur atau cacat, kepastian dan keakuratan dapat mencapai minimum 0 persen.

Berdasarkan seperangkat data dan kueri yang dilaporkan untuk posisi relatif salah satu node tepi, perkiraan posisi dapat dihasilkan beserta koefisien untuk kepastian dan keakuratan.

Berdasarkan seperangkat data dan algoritme analisis yang sama, setiap kalkulasi harus tiba pada perkiraan posisi yang sama dan koefisien yang sama untuk kepastian dan keakuratan.

4.6 Diagram

S’ dan S” (Gambar 1.) masing-masingnya adalah Sentinel (node tepi) yang mengumpulkan heuristik. Ketika saling kontak, sentinel itu saling bertukar data heuristik dan kunci publik. Keduanya membangun arsip lengkap mengenai interaksi tersebut dan menandatangani interaksi yang dihasilkan. Arsip yang ditandatangani itu kemudian menjadi entri berikutnya di kedua ledger lokalnya (16 untuk S’ dan 3 untuk S”). Tindakan ini mengikat kedua saksi itu karena berada dalam suatu proksimitas satu sama lain.



Gambar 1. Contoh Pengikatan Saksi antara Dua Sentinel

4.7 Origin Chain

Setiap asal mempertahankan ledger-nya sendiri dan menandatanganinya untuk membuat Proof of Origin Chain. Begitu informasi tentang Proof of Origin Chain telah dibagi, maka itu akan menjadi permanen. Hal itu karena pencabangan (fork) yang terjadi setelah hal berbagi tersebut mengakhiri rantai dan membuat semua data mendatang dari saksi akan diperlakukan seakan-akan itu berasal saksi baru. Untuk menghasilkan mata rantai di Proof of Origin Chain, asal (origin) akan menghasilkan pasangan kunci publik/privat. Itu kemudian menandatangani blok sebelumnya dan berikutnya dengan pasangan yang sama setelah menyertakan kunci publik di kedua blok. Segera setelah tanda tangan dibuat, kunci privat pun dihapus. Dengan penghapusan segera kunci privat, risiko kehilangan atau penggunaan kembali kunci menjadi sangat kecil.

Proof of Origin Chain merupakan kunci untuk memastikan bahwa ledger yang masuk ke XYO Network memang valid. ID unik untuk sumber daya tidak bersifat praktis karena bisa dipalsukan. Penandatanganan kunci privat tidak bersifat praktis karena sebagian besar komponen XYO Network sulit atau mustahil aman secara fisik, sehingga sangat besar kemungkinan pencurian kunci privat oleh pelaku kejahatan. Untuk mengatasi ini, XYO Network menggunakan Transient Key Chains. Keuntungan penggunaannya adalah mustahil memalsukan rantai asal data. Namun, begitu rantai terputus, maka itu akan terputus selamanya dan tidak bisa diteruskan, sehingga membuatnya menjadi sebuah pulau (island).

Setiap kali ledger heuristik diteruskan di XYO Network, penerima akan melampirkan Proof of Origin miliknya, sehingga membuat Proof of Origin Chain menjadi lebih panjang dan menghasilkan Proof of Origin Intersection. Proof of Origin Chain dan Proof of Origin Intersection merupakan indikator utama yang digunakan oleh Diviner untuk memverifikasi kesahihan ledger. Persamaan Reputasi Ledger pada intinya adalah persentase dari XYO Network yang terlibat dalam membuat Proof of Origin Ball yang terkait dengannya. Secara teoretis, jika 100 persen arsip XYO Network terkait dengan Proof of Origin dan kemudian dianalisis sepenuhnya, kemungkinan kesahihannya adalah 100 persen. Jika 0 persen dari arsip XYO Network tersedia untuk dianalisis, maka kesahihannya jatuh menjadi 0 persen.

Untuk keamanan tambahan, kunci publik untuk Chain Link tidak disediakan sebelum entri kedua untuknya disediakan. Hal ini juga memungkinkan adanya interval waktu antar entri atau data lain yang akan disimpan di mata rantai sebelumnya atau berikutnya.

4.8 Origin Chain Score

Origin Chain Score dikalkulasikan sebagai berikut (algoritme default):

- PcL = Panjang Proof of Origin Chain
- PcD = Kesulitan Proof of Origin Chain
- Pc' Pc" O = Tumpang-tindih Proof of Origin Chain untuk Pc' dan Pc"

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

4.9 Origin Tree

Origin Tree digunakan untuk menghitung kesahihan perkiraan jawaban. Origin Tree menggunakan data yang dikumpulkan untuk menghasilkan Pohon yang Ideal, yakni pohon yang paling cocok dengan data untuk jawaban tertentu yang diberikan. Jika node N terletak di lokasi X,Y,Z,T, kesalahan di seluruh data di dalam set harus memiliki nilai tertentu. Untuk menghitung kesalahan ini, kami akan menghitung MIN, MAKS, RERATA, MEDIAN, dan JARAK RATA-RATA DARI RERATA.

Berdasarkan seperangkat S dari semua skor s, kesulitan Proof of Origin Chain PcD, dan kesalahan faktor kesalahan, Best Answer akan ditentukan sebagai berikut ini:

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

Dengan kata lain, jawaban yang diberikan yang memiliki Best Answer Score adalah Best Answer. Dengan Proof of Origin Tree, kita dapat mengidentifikasi dan memangkas cabang-cabang yang tidak mungkin (pencilan).

4.10 Transient Key Chaining

Serangkaian paket data dapat dirantai bersama dengan kunci privat sementara untuk menandatangani dua paket secara berturut-turut. Ketika kunci publik yang dipasangkan dengan kunci privat disertakan dalam paket data, penerima dapat memverifikasi bahwa kedua paket ditandatangani oleh kunci privat yang sama. Data di paket tidak bisa diubah tanpa merusak tanda tangan, sehingga memastikan bahwa paket yang ditandatangani tidak diubah oleh pihak ketiga, seperti node Bridge atau penyimpanan.

4.11 Kedalaman Mata Rantai

Secara minimum, sebuah node menghasilkan kunci publik/privat baru untuk setiap mata kunci di Proof of Origin Chain, yang memiliki Kedalaman Mata Kunci 1. Mungkin terdapat N entri di tabel mata kunci untuk Entri Ledger tertentu, di mana setiap entri menyebutkan jarak di waktu mendatang ketika bagian kedua dari mata kunci akan ditambahkan. Tidak ada dua mata kunci yang dapat memiliki urutan ukuran yang sama pada skala dasar 2. Misalnya, entri [1,3,7,12,39] akan diizinkan, tetapi [1,3,7,12,15] tidak akan diizinkan.

Kedalaman mata kunci 1 dibuat, digunakan dan dihapus ketika blok sebelumnya diterbitkan. Namun, mata kunci kedalaman yang lebih besar dari 1 akan dihasilkan pasangannya saat blok sebelumnya sedang ditandatangani, dan penandatanganan kedua tidak terjadi hingga N blok kemudian, yang setelahnya kunci privat akan dihapus. Untuk alasan ini, mata rantai kedalaman yang lebih besar dari 1 selalu dianggap kurang aman dibandingkan mata rantai dengan kedalaman 1, tapi itu semua dapat digunakan untuk meningkatkan kinerja dan mengurangi data yang hilang dengan risiko keamanan tersebut.

4.12 Urutan Tetap

Unsur utama dalam menentukan urutan ledger adalah urutan pelaporannya. Karena tidak mungkin bagi suatu perangkat untuk mengubah urutan ledger yang ditandatangani Proof of Origin, urutan mutlak dapat ditetapkan dengan memperhatikan semua ledger secara kolektif.

4.13 Penerbitan Kedua Terakhir

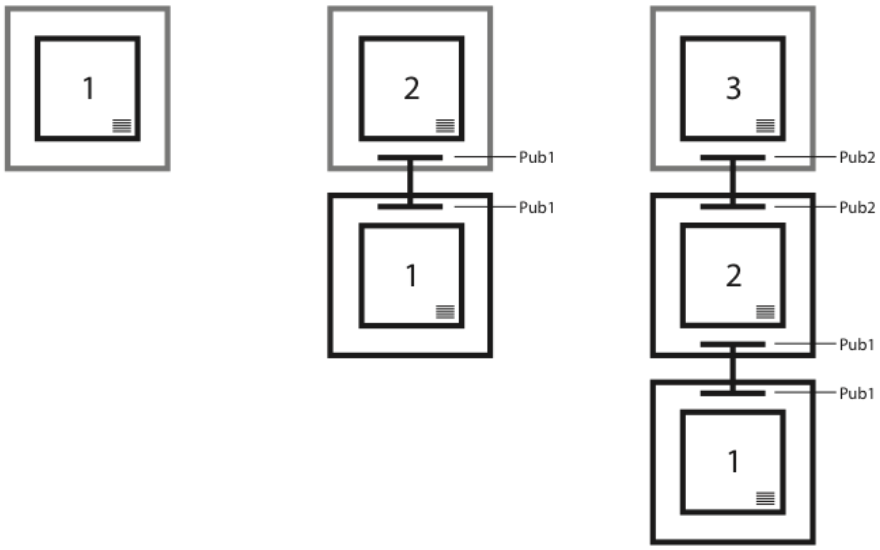
Metode utama untuk menetapkan Proof of Origin didasarkan pada fakta bahwa Sentinel selalu melaporkan blok kedua terakhir tanpa melaporkan blok terakhir. Hal ini memungkinkan blok terakhir untuk memiliki mata rantai ke pendahulunya yang ditandatangani sebagai bukti mata rantai.

4.14 Mata Rantai Kosong

Agar Proof of Origin Chain menjadi lebih aman, rantai harus diperbarui tidak lebih dari sekali dalam setiap sepuluh detik dan tidak kurang dari sekali dalam setiap enam puluh menit. Dalam kasus data baru tidak tersedia, blok kosong akan ditambahkan ke rantai.

4.15 Diagram

Karena waktu bergerak dari kiri ke kanan (Gambar 2.), Proof of Origin Chain yang terbangun menjadi lebih panjang. Pada saat kapan pun, produsen rantai hanya akan memberi kepada pemanggil entri yang memiliki batas gelap, dan akan menunggu penandatanganan entri yang kedua sebelum menyediakannya. Sebagai contoh, pada kolom ke-3, hanya entri 2 dan 1 yang akan dikembalikan sebagai bagian dari rantai.



Gambar 2. Penyertaan mata rantai di Proof of Origin Chain

4.16 Ringkasan

Berdasarkan serangkaian paket data yang ditandatangani dalam pasangan yang berurutan dengan kunci privat sementara dan menyertakan kunci publik yang disandingkan, maka dapat ditentukan dengan kepastian mutlak bahwa paket berasal dari asal yang sama.

5 Pertimbangan Keamanan

5.1 Serangan Diviner Palsu

Serangkaian tanda tangan digital dikirim ke kontrak cerdas XYO karena kontrak mesti memverifikasi integritas Diviner yang mengirim jawaban. Kontrak kemudian dapat memverifikasi Diviner lain yang menandatangani daftar ini dalam interval kepercayaan yang tinggi. Tanpa hal ini, oracle yang merelai akan menjadi sumber kegagalan dan risiko tunggal di dalam sistem.

5.2 Serangan DDoS Sentinel

Serangan lain untuk dipertimbangkan adalah (DDoS) di antara node Sentinel di wilayah tertentu. Penyerang dapat mencoba membuat sejumlah besar sambungan ke Sentinel untuk mencegahnya merelai informasi yang benar atau merelai informasi apa pun ke Bridge. Kami dapat mengakali masalah ini dengan mengharuskan dipecahkannya teka-teki kriptografi kecil oleh siapa pun yang mencoba terhubung ke Sentinel. Karena sebuah kueri tidak akan melibatkan sambungan dalam jumlah yang sangat besar ke Sentinel, maka ini tidak akan terlalu membebani sistem relai XYO, dan akan mengharuskan penyerang menghabiskan sumber daya yang besar untuk bisa melakukan DDoS terhadap jaringan kami. Pada waktu tertentu kapan pun, Proof of Origin Chain dapat diverifikasi oleh siapa pun karena tersimpan di XYOMainChain. Hal ini memastikan bahwa jika suatu entitas tunggal di sepanjang rantai diretas, maka keakuratan jawaban kueri (Origin Chain Score) akan jatuh menjadi 0.

---

6 Ekonomi Token XYO

Oracle menjadi bagian yang signifikan dari kekuatan dan kebutuhan infrastruktur akan aplikasi terdesentralisasi, di mana sebagian besar fokus berkisar pada konektivitas dan agregasi oracle otoritatif. Kami meyakini bahwa kebutuhan akan sistem oracle yang sepenuhnya terdesentralisasi dan trustless diperlukan untuk aplikasi desentralisasi guna mencapai potensi maksimumnya.

6.1 Ekonomi Kripto XYO Network

Kami menggunakan Token XYO untuk memberi insentif kepada perilaku yang diinginkan dalam menyediakan heuristik lokasi yang akurat dan andal. Token XYO dapat dianggap sebagai “bensin” yang diperlukan untuk berinteraksi dengan dunia nyata guna memverifikasi koordinat XY objek yang ditentukan.

Cara kerja prosesnya seperti ini: Pemilik token pertama kali mengirim kueri ke XYO Network dengan kueri (misalnya., “Di mana paket pesanan eCommerce saya dengan Alamat XYO 0x123456789…?”). Kueri itu kemudian dikirim ke antrean, menunggu untuk diproses dan dijawab. Pengguna dapat menetapkan tingkat keyakinan dan harga bensin XYO yang diinginkan pada saat pembuatan kueri. Biaya sebuah kueri (di Token XYO) ditentukan oleh jumlah data yang diperlukan untuk memberikan jawaban terhadap kueri serta dinamika pasar. Semakin banyak data yang dibutuhkan, maka semakin mahal pula kueri dan semakin tinggi pula harga bensin XYO. Kueri terhadap XYO Network berpotensi menjadi sangat besar dan mahal. Misalnya, sebuah perusahaan angkutan truk dan logistik dapat mengirim kueri ke XYO Network untuk bertanya, “Di manakah lokasi setiap mobil di armada kita?”

Begitu pemilik Token XYO mengirim kueri ke XYO Network dan membayar bensin yang diminta, seluruh Diviner yang bekerja untuk tugas tersebut akan memanggil Archivist relevan untuk mengambil data terkait yang diperlukan untuk menjawab kueri tersebut. Data yang dikembalikan berasal dari Bridge, yang awalnya mengumpulkan data tersebut dariSentinel. Sentinel pada dasarnya adalah perangkat atau sinyal yang memverifikasi lokasi objek. Ini mencakup entitas seperti pelacak Bluetooth, pelacak GPS, pelacakan geo-lokasi yang ditanamkan ke perangkat IoT, teknologi pelacakan satelit, pemindai kode QR, pemindaian RFID dan banyak lagi yang lain. XY Findables telah merintis dan meluncurkan bisnis Bluetooth dan GPS konsumennya, yang telah memungkinkannya untuk menguji dan memproses heuristik lokasi dunia nyata. Segenap upaya yang dikerahkan dalam mengembangkan bisnis konsumen XY Findables telah membantu secara signifikan dalam merancang Protokol Blockchain XYO Network.

Jika data yang disediakan perangkat Sentinel (seperti Beacon Bluetooth) digunakan untuk menjawab kueri, maka keempat komponen yang terlibat dalam transaksi menerima sebagian bensin XYO yang dibayar oleh pemilik token: Diviner (yang mencari jawaban), Archiver (yang menyimpan data), Bridge (yang mengirim data) dan Sentinel (yang merekam data lokasi). Distribusi bensin antara 3 dari 4 komponen XYO Network selalu diberikan proporsi yang sama. Namun hal itu dikecualikan pada Diviner, yang keterlibatannya dalam proses penyediaan jawaban adalah lebih ekstensif. Di dalam setiap komponen, bensin didistribusikan secara merata.

6.2 Hadiah untuk Independensi

Perangkat yang mengumpulkan lokasi merupakan blok atom jaringan, dan suatu perangkat tunggal dapat berfungsi sebagai salah satu komponen, atau lebih, dari empat komponen sistem. Namun begitu, hal ini langka, khususnya di XYO Network besar, apabila perangkat memiliki lebih dari dua komponen ini. Lebih lanjut, ledger blockchain yang memiliki lebih banyak Proof of Origin independen akan mendapatkan perhatian lebih besar, jadi ada hukuman ekonomi kripto untuk perangkat yang berfungsi sebagai multi komponen.

6.3 Hadiah untuk Integritas Stasionaritas

Sentinel di XYO Network diberikan koefisien stasionaritas untuk kuantitas gerakan di sepanjang siklus hidup. Semakin sedikit gerakan Sentinel dalam suatu periode waktu, maka semakin banyak pula datanya yang dapat dipercayai. Archivist melacak dan menganalisis koefisien stasionaritas ini ketika mempertimbangkan kepada Sentinel manakah kueri akan diarahkan.

6.4 Memberi Insentif untuk Penggunaan Token

Suatu sistem di mana pemilik token didorong untuk tidak menggunakan tokennya akan menimbulkan masalah jangka panjang bagi ekonomi yang menopangnya. Hal itu akan menciptakan suatu ekosistem dengan simpanan nilai yang sangat langka dan akan memicu dorongan alamiah untuk membuat alasan agar tidak menggunakan token, melainkan mendorong utilitas dan likuiditas.

Masalah yang terdapat pada sebagian besar insentif ekonomi kripto adalah bahwa fokusnya terlalu ditekankan pada penambang token (misalnya., Sentinel, Bridge, Archivist, Diviner), sama sekali bukan pada pengguna token. Token XYO mempertimbangkan kedua belah sisi.

Model Token XYO memberi insentif kepada penambang untuk tidak hanya menyediakan data yang akurat, tapi juga mengetahui kapan untuk tidak menyediakan data sama sekali. Pengguna akhir diberi hadiah untuk bertransaksi lebih banyak ketika likuiditas jaringan rendah, dibandingkan ketika likuiditas jaringan tinggi. Oleh karena itu, ekosistem Token XYO memiliki kemampuan untuk tetap seimbang, cair dan tangguh.

6.5 Spesifikasi Token XYO

Penjualan token publik memiliki struktur harga bertingkat yang dimulai pada 1 ETH: 100.000 XYO dan maksimal di 1 ETH: 33.333 XYO.

- Platform kontrak cerdas: Ethereum
- Jenis Kontrak：ERC-20
- Token：XYO
- Nama Token：Token Utilitas XYO Network
- Alamat Token：0x55296f69f40ea6d20e478533c15a6b08b654e758
- Total penerbitan：Terbatas dan dibatasi pada jumlah yang tercapai setelah Penjualan Utama Token
- Batas Token XYO yang Diproyeksikan: $48 Juta
- Token yang Tidak Terjual dan Tidak Dialokasikan：Dibakar setelah acara penjualan token. Tidak ada token XYO lebih lanjut yang akan dibuat setelah Penjualan Utama berakhir.

---

7 Kasus Penggunaan XYO Network

Penggunaan XYO Network sangat banyak diterapkan di berbagai industri. Misalnya, sebuah perusahaan eCommerce yang dapat menawarkan layanan bayar-di-tempat (bayar saat barang diantar) kepada pelanggan premiumnya. Agar dapat menawarkan layanan ini, perusahaan eCommerce memanfaatkan XYO Network (yang menggunakan Token XYO) untuk menulis kontrak cerdas (yakni, di platform Ethereum). XYO Network lalu dapat melacak lokasi paket yang dikirim ke konsumen sepanjang tahapan proses pemenuhan, dari gudang sortir hingga kurir pengiriman, sampai ke rumah konsumen, berikut setiap lokasi di antaranya. Dengan begitu, peritel dan situs web eCommerce dapat memverifikasi secara trustless, bahwa paket itu tidak hanya sudah berada di depan pintu pelanggan, tapi memang sudah dibawa masuk ke dalam rumah. Setelah paket sudah di dalam rumah pelanggan (dipastikan dan diverifikasi oleh Koordinat XY spesifik), pengiriman dianggap sudah selesai dan pembayaran ke vendor pun dicairkan. Dengan integrasi XYO Network ke dalam eCommerce, maka merchant dapat dilindungi dari aksi penipuan (fraud) dan memastikan konsumen hanya membayar barang yang memang sudah tiba di rumah mereka.

Bayangkan suatu integrasi XYO Network yang sepenuhnya berbeda ke dalam situs ulasan hotel, yang saat ini memiliki masalah di mana ulasan di situs tidak bisa dipercaya. Biasanya pemilik hotel akan terdorong untuk memperbaiki ulasannya dengan biaya berapa pun. Bagaimana jika seseorang dapat mengatakan dengan tingkat keyakinan yang sangat tinggi bahwa seseorang yang di San Diego, terbang ke sebuah hotel di Bali dan menginap di sana selama dua minggu, lalu kembali ke San Diego dan menulis ulasannya tentang menginap di hotel di Bali? Ulasan tersebut akan memiliki reputasi yang sangat tinggi, khususnya jika ditulis oleh seorang pengulas yang kerap menulis dan telah menulis banyak ulasan dengan data lokasi yang terverifikasi.

---

8 Ekspansi XYO Network

Kami beruntung memiliki bisnis konsumen yang telah sukses membangun jaringan dunia nyata dengan lebih dari satu juta (1.000.000) perangkat Bluetooth dan GPS di dunia. Sebagian besar jaringan lokasi gagal mencapai fase ini dan mendapatkan massa kritis yang diperlukan untuk membangun suatu jaringan ekstensif. Jaringan Sentinel yang telah kami bentuk barulah titik awal. XYO Network adalah suatu sistem terbuka yang dapat dimasuki operator perangkat lokasi mana pun dan mulai mendapatkan Token XYO.

Secara umum, semakin besar kardinalitas Sentinel di XYO Network, maka akan semakin andal. Untuk lebih mengembangkan jaringannya, XYO Network berkolaborasi dengan bisnis lain untuk memperluas jaringan Sentinel-nya melampaui jaringan beacon XY Findables-nya sendiri.

---

9 Ucapan terima kasih

Buku Putih ini merupakan produk dari upaya inspiratif tim yang hanya mungkin terwujud berkat keyakinan pada visi kami dari orang-orang berikut ini: Raul Jordan (Harvard College, Thiel Fellow dan Penasihat XYO Network); atas kontribusinya dalam membuat buku putih kami menjadi lebih ringkas dan membantu kami menyampaikan rincian teknisnya ke seluruh dunia secara elegan. Ucapan terima kasih juga kami sampaikan kepada Christine Sako atas etos kerjanya yang luar biasa dan peninjauannya yang sangat detail atas karya kami. Konsistensi struktur dan praktik terbaik yang terdapat dalam buku putih kami tak lepas dari sumbangsih Christine. Kami menyampaikan ucapan terima kasih kepada Johnny Kolasinski atas riset dan kompilasi kasus penggunaan yang aplikatif. Terakhir tidak lupa juga kami haturkan terima kasih kepada John Arana atas peninjauan yang cermat dan masukannya yang kreatif .

References

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

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

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

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

Glosarium

akurasi
Kadar keyakinan bahwa titik data atau heuristik berada dalam margin kesalahan spesifik.

Archivist
Archivist menyimpan heuristik sebagai suatu bagian dari kumpulan data terdesentralisasi yang tujuannya menyimpan semua ledger lama, tapi tanpa keharusan itu. Meskipun ada data yang hilang atau sementara waktu tidak tersedia, sistem terus berfungsi, hanya saja akurasinya menurun. Archivist juga mengindeks ledger agar bisa mengembalikan string data ledger jika dibutuhkan. Archivist menyimpan data mentah saja dan mendapat bayaran hanya untuk pengambilan data. Penyimpanan selalu gratis.

Best Answer
Kami mendefinisikan Best Answer sebagai jawaban tunggal, di antara Daftar Bakal Jawaban, yang mengembalikan skor kesahihan tertinggi dan memiliki skor keakuratan yang lebih tinggi dibandingkan keakuratan minimum yang disyaratkan.

Best Answer Algorithm
Sebuah algoritme digunakan untuk menghasilkan Best Answer Score ketika Diviner memilih jawaban. XYO Network mengizinkan penambahan algoritme khusus dan memperbolehkan pelanggan untuk menentukan algoritme yang akan digunakan. Algoritme ini diharuskan menghasilkan skor yang sama ketika dijalankan di Diviner mana pun yang diberi seperangkat data yang sama.

Bound Witness
Bound Witness adalah suatu konsep yang dicapai dengan keberadaan heuristik dua arah. Mengingat sumber data tak tepercaya untuk penggunaan penyelesaian kontrak digital (oracle) tidak berguna, ada peningkatan yang substansial dalam kepastian data yang disediakan melalui pembentukan heuristik tersebut. Heuristik dua arah utama adalah proksimitas karena kedua pihak bisa memvalidasi kemunculan dan rentang interaksi dengan turut menandatangani interaksi. Hal ini memungkinkan bukti nol pengetahuan bahwa dua node saling berdekatan.

Bridge
Sebuah Bridge merupakan transcriber heuristik. Meneruskan secara aman ledger heuristik dari Sentinel ke Diviner.
Aspek terpenting sebuah Bridge adalah meyakinkan Diviner bahwa ledger heuristik yang diterima dari suatu Bridge sama sekali tidak berubah sedikit pun. Aspek terpenting kedua sebuah Bridge adalah menambahkan metadata tambahan Proof of Origin.

kepastian
Takaran kemungkinan titik data atau heuristik bebas dari korupsi atau pengotakatikan.

lokasi kripto
Dunia teknologi lokasi kriptografi.

kriptoekonomi
Disiplin formal yang mengkaji protokol yang mengatur produksi, distribusi, dan konsumsi barang dan jasa dalam perekonomian digital desentralisasi. Kriptoekonomi merupakan ilmu praktis yang fokus pada desain dan karakterisasi protokol tersebut.

Diviner
Diviner menjawab kueri yang diberikan dengan menganalisis data lama yang telah disimpan oleh XYO Network. Heuristik yang disimpan di XYO Network harus memiliki Proof of Origin level tinggi agar dapat menentukan validitas dan akurasi heuristik. Diviner mendapatkan dan memberikan jawaban dengan menilai saksi berdasarkan Proof of Origin-nya. Mengingat XYO Network merupakan sistem trustless, Diviner harus diberi insentif agar menyediakan analisis heuristik yang jujur. Tidak seperti Sentinel dan Bridge, Diviner menggunakan Proof of Work untuk menambahkan jawaban ke blockchain.

heuristik
Titik data dunia nyata terkait dengan posisi Sentinel (proksimitas, suhu, cahaya, gerakan, dsb...).

oracle
Bagian dari sistem DApp (aplikasi terdesentralisasi) yang bertanggung jawab untuk menyelesaikan kontrak digital dengan memberikan jawaban dengan keakuratan dan kepastian. Istilah “oracle” berasal dari kriptografi yang menunjukkan sumber yang benar-benar acak (misalnya., angka acak). Hal itu menyediakan pintu gerbang yang diperlukan dari penyamaan kripto ke dunia di luarnya. Oracle memberi umpan informasi kontrak cerdas dari luar rantai (dunia nyata, atau luar rantai). Oracle adalah antarmuka dari dunia digital ke dunia nyata. Sebagai contoh yang agak ekstrem, bayangkan sebuah kontrak untuk Surat Wasiat Terakhir & Surat Warisan. Ketentuan Surat Wasiat dilaksanakan begitu adanya penetapan bahwa pewaris sudah meninggal. Layanan oracle dapat dibangun untuk memicu Surat Wasiat dengan menyusun dan mengumpulkan data relevan dari sumber resmi. Oracle itu kemudian digunakan sebagai umpan atau titik akhir yang bisa dipanggil kontrak cerdas untuk memeriksa apakah orang tersebut meninggal atau tidak.

Origin Chain Score
Skor yang ditetapkan untuk Origin Chain guna menentukan kredibilitasnya. Penilaian ini akan mempertimbangkan panjang, tangle, tumpang-tindih, dan redundansi.

Origin Tree
Seperangkat data entri ledger yang diambil dari berbagai Origin Chain untuk menetapkan asal entri ledger heuristik dengan tingkat kepastian khusus.

Proof of Origin
Proof of Origin merupakan kunci untuk memastikan bahwa ledger yang masuk ke XYO Network memang valid. ID unik untuk sumber daya tidak bersifat praktis karena bisa dipalsukan. Penandatanganan kunci privat tidak bersifat praktis karena sebagian besar komponen XYO Network sulit atau mustahil aman secara fisik, sehingga sangat besar kemungkinan pencurian kunci privat oleh pelaku kejahatan. Untuk mengatasi ini, XYO Network menggunakan Perantaian Kunci Sementara. Keuntungannya adalah mustahil memalsukan rantai asal data. Namun, begitu rantai terputus, maka itu akan terputus selamanya dan tidak bisa diteruskan, sehingga membuatnya menjadi sebuah pulau (island).

Proof of Origin Chain
Suatu Transient Key Chain yang mengaitkan serangkaian entri ledger heuristik Bound Witness.

Proof of Work
Proof Pekerjaan adalah data yang memenuhi persyaratan tertentu, dan sulit untuk dihasilkan (mis., mahal, makan waktu), tapi mudah diverifikasi orang lain. Produksi Proof of Work bisa menjadi proses acak dengan kemungkinan pembuatan yang rendah sehingga uji coba yang ketat rata-rata diperlukan sebelum Proof of Work yang sah dibuat.

Sentinel
Sebuah Sentinel merupakan saksi heuristik. Mengamati heuristik dan menegaskan kepastian dan akurasi heuristik tersebut dengan membuat ledger sementara. Aspek terpenting sebuah Sentinel adalah menghasilkan ledger yang meyakinkan Diviner itu berasal dari sumber yang sama dengan menambahkan Proof of Origin ke ledger tersebut.

kontrak cerdas
Protokol yang dicetuskan oleh Nick Szabo sebelum Bitcoin, kira-kira pada 1994 (sehingga ada yang percaya dia sebenarnya Satoshi Nakamoto, penemu mistis dan anonim Bitcoin). Ide di balik kontrak cerdas adalah mengodifikasi perjanjian legal dalam suatu program dan menggerakkan komputer desentralisasi melaksanakan ketentuannya, bukan manusia yang harus menafsirkan dan bertindak berdasarkan kontrak. Kontrak cerdas menyatukan uang (contoh, Ether) dan kontrak ke dalam konsep sama. Karena kontrak cerdas bersifat deterministik (seperti program komputer) dan sepenuhnya transparan serta dapat dibaca, kontrak cerdas ampuh menggantikan perantara dan broker.

Transient Key Chain
Transient Key Chain mengaitkan serangkaian paket data dengan Transient Key Cryptography.

trustless
Karakteristik di mana semua pihak dalam suatu sistem bisa mencapai konsensus tentang apa kebenaran bersama itu. Power dan trust disebarkan (dibagikan) di antara pemangku kepentingan jaringan (misalnya., pengembang, penambang, dan konsumen), bukan terkonsentrasi pada satu individu atau entitas (mis. bank, pemerintah, dan lembaga keuangan). Ini merupakan istilah umum yang mudah sekali disalahpahami. Blockchain tidak benar-benar meniadakan trust. Yang terjadi sebenarnya adalah diminimalkannya jumlah trust yang diperlukan dari satu pelaku dalam sistem. Blockchain melakukan ini dengan menyebarkan trust di antara para pelaku yang berbeda melalui permainan ekonomi yang memberi insentif kepada pelaku tersebut agar mau mematuhi peraturan yang ditetapkan protokol itu.

XY Oracle Network
XYO Network.

XYO Network
XYO Network XYO Network kependekan dari “XY Oracle Network.” Itu terdiri atas seluruh sistem berupa komponen/node berkemampuan XYO yang meliputi Sentinel, Bridge, Archivist, dan Diviner. Fungsi utama XYO Network adalah bertindak sebagai portal agar kontrak cerdas digital dapat dilaksanakan melalui konfirmasi geolokasi dunia nyata.

XYOMainChain
Suatu blockchain abadi di XYO Network yang menyimpan transaksi kueri beserta data yang dikumpulkan dari Diviner dan skor asalnya yang terkait.