Hydro Raindrop:
Autentikasi Publik di The Blockchain

Januari 2018

DAFTAR ISI

Abstrak

HYDRO: Etimologi - Dari bahasa Yunani Kuno ὑδρο- (hudro-), dari ὕδωρ (húdōr, "water")

Hydro memungkinkan sistem privat yang baru dan yang sudah ada untuk mengintegrasikan dan memanfaatkan secara bebas & transparan dari blockchain publik untuk meningkatkan keamanan aplikasi dan dokumen, manajemen identitas, transaksi, dan kecerdasan buatan.

Dalam makalah ini, sebuah kasus akan dibuat untuk sistem pribadi, seperti API, untuk menggunakan blockchain publik Hydro untuk meningkatkan keamanan melalui otentikasi publik.

Teknologi yang diusulkan disebut "Raindrop" - transaksi yang dilakukan melalui kontrak cerdas yang memvalidasi akses sistem swasta secara publik, dan dapat melengkapi metode otentikasi pribadi yang ada. Teknologi ini dimaksudkan untuk memberikan keamanan tambahan untuk data keuangan yang sensitif yang semakin berisiko dari peretasan dan pelanggaran.

Implementasi awal Hydro Raindrop dilakukan pada Platform API Hidrogen. Perangkat API modular ini tersedia untuk perusahaan dan pengembang secara global untuk membuat prototipe, membangun, menguji, dan menerapkan platform dan produk teknologi keuangan canggih.

Hydro Raindrop akan tersedia bagi komunitas pengembang dunia sebagai perangkat lunak open source, untuk memungkinkan pengembang mengintegrasikan Hydro Raindrop dengan REST API.

Blockchain & Ethereum

Hydro diimplementasikan pada jaringan Ethereum. Sebelum memberikan detail lebih lanjut tentang proyek, penting untuk memahami beberapa gagasan mendasar tentang blockchain dan Ethereum.

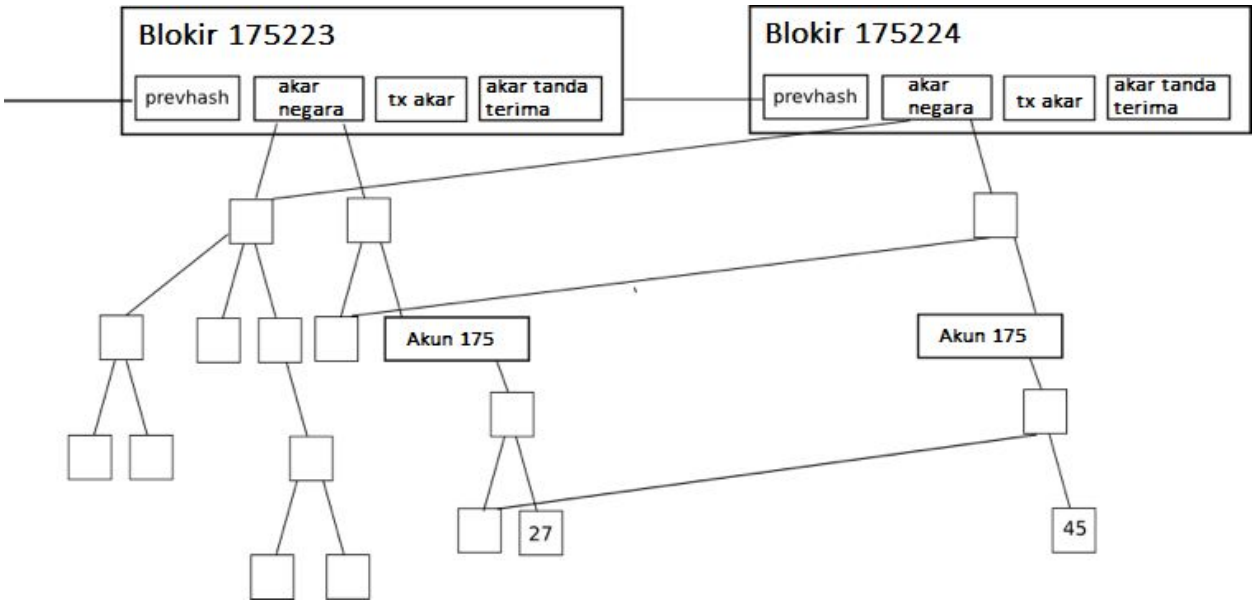
Membangun Ethereum

Sama seperti aplikasi seperti Snapchat yang dibangun dengan Swift dan alat lain yang ditawarkan di atas platform Apple iOS, aplikasi blockchain juga dapat dibangun di atas Ethereum. Snap Inc. tidak perlu membangun iOS, ia menggunakannya sebagai infrastruktur untuk meluncurkan aplikasi media sosial yang mengubah permainan.

Proyek Hydro serupa. Itu bergantung pada ribuan pengembang secara global yang bekerja untuk membuat teknologi blockchain yang mendasarinya lebih cepat, lebih kuat, dan lebih efisien. Hydro memanfaatkan infrastruktur yang terus membaik ini dengan mengembangkan interaksi yang berfokus pada produk di sekitar teknologi blockchain yang dapat menawarkan manfaat nyata bagi aplikasi layanan keuangan.

Pohon Merkle

Pohon Merkle digunakan dalam sistem terdistribusi untuk verifikasi data yang efisien. Mereka efisien karena mereka menggunakan hash bukan file penuh. Hash adalah cara penyandian file yang jauh lebih kecil dari file yang sebenarnya.
Setiap header blok di Ethereum mengandung tiga Pohon Merkle untuk Transaksi, Penerimaan, dan Negara:



Sumber: Merkling di Ethereum; Vitalik Buterin, Ethereum Founder

Ini memudahkan klien ringan untuk mendapatkan jawaban atas pertanyaan yang dapat diverifikasi, seperti:

- Apakah akun ini ada?
- Berapa saldo saat ini?
- Apakah transaksi ini sudah termasuk dalam blok tertentu?
- Apakah peristiwa tertentu terjadi di alamat ini hari ini?

Kontrak Pintar

Konsep kunci yang dimungkinkan oleh Ethereum dan jaringan berbasis blockchain lainnya adalah kontrak pintar. Ini adalah blok kode self-executing yang dapat berinteraksi dengan banyak pihak, memotong kebutuhan untuk perantara yang tepercaya. Kode dalam kontrak cerdas dapat dilihat sebagai mirip dengan klausul hukum dalam kontrak kertas tradisional, tetapi juga dapat mencapai fungsi yang jauh lebih luas. Kontrak dapat memiliki aturan, ketentuan, penalti untuk ketidakpatuhan, atau dapat memulai proses lainnya. Ketika dipicu, kontrak dijalankan sebagaimana aslinya dinyatakan pada saat penyebaran pada rantai publik, menawarkan elemen-elemen ketidakmampuan dan desentralisasi yang tertanam di dalamnya.

Kontrak cerdas adalah alat vital untuk membangun infrastruktur Ethereum. Fungsi inti dari lapisan blockchain Hydro dicapai melalui kontrak khusus, seperti yang dibahas nanti dalam makalah ini.

Mesin Virtual Ethereum

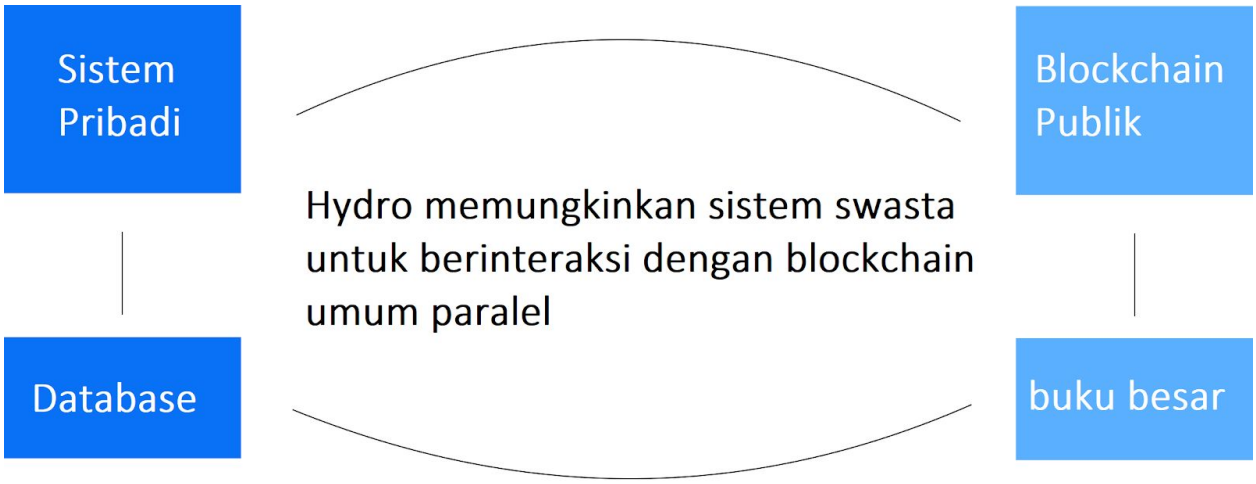
Ethereum Virtual Machine (EVM) adalah lingkungan runtime untuk kontrak cerdas di Ethereum. EVM membantu mencegah serangan Denial of Service (DoS), memastikan program tetap tanpa kewarganegaraan, dan memungkinkan komunikasi yang tidak dapat terganggu. Tindakan pada EVM memiliki biaya yang terkait dengan mereka, yang disebut gas, yang bergantung pada sumber daya komputasi yang diperlukan. Setiap transaksi memiliki jumlah maksimum gas yang dialokasikan kepadanya, yang dikenal sebagai batas gas. Jika gas yang dikonsumsi oleh transaksi mencapai batas, maka gas akan berhenti untuk melanjutkan pemrosesan.

Buku Besar Publik

Buku Besar Publik untuk Sistem Pribadi

Sistem yang menggerakkan platform layanan keuangan, situs web, dan aplikasi sering dapat digambarkan sebagai media aliran data - mereka mengirim, mengambil, menyimpan, memperbarui, dan mengolah data untuk entitas yang berinteraksi dengan mereka. Karena sifat data ini, dan layanan keuangan yang lebih umum, sistem ini sering melakukan operasi kompleks secara privat dan terpusat. Ketergantungan pada struktur pribadi, pada gilirannya, membuka pintu untuk berbagai keamanan, transparansi, dan peningkatan efisiensi yang bisa didapat dengan menggabungkan kekuatan eksternal yang melampaui jangkauan sistem internal.

Seperti halnya dengan Platform API Hidrogen. Hydro bertujuan untuk memanfaatkan keuntungan yang disebutkan di atas dengan memungkinkan pengguna Hidrogen untuk berinteraksi dengan blockchain dengan cara yang terintegrasi secara sempurna ke dalam ekosistem Hidrogen yang pada dasarnya bersifat privat.

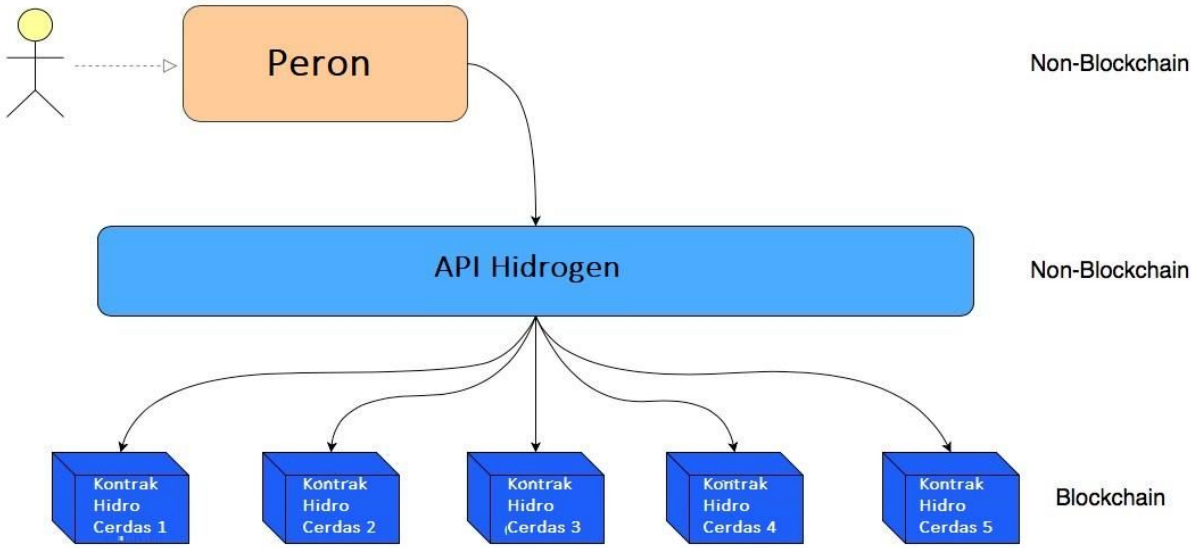


Operasi berbasis blockchain publik dapat terjadi sebelum, selama, atau setelah operasi pribadi. Interaksi antara elemen pribadi dan publik dapat berfungsi untuk memvalidasi, memberi stempel, merekam, atau meningkatkan proses dalam ekosistem.

Etos dari model ini adalah membuat proses lebih kuat dengan memanfaatkan keunggulan teknologi blockchain khususnya di mana ia dapat menghasilkan dampak yang paling positif. Sementara kerangka kerja hibrida ini mungkin tidak berlaku untuk semua platform, Hydro berfokus pada penyediaan nilai untuk kasus-kasus di mana itu.

Arsitektur untuk Adopsi

Hydro berbeda dari banyak inisiatif blockchain yang ada, karena dapat eksis secara independen dan lapisan di sekitar sistem baru atau yang sudah ada tanpa memerlukan perubahan sistemik. Alih-alih menggantikan, Hydro bertujuan untuk menambah. Platform dan institusi yang terhubung ke API Hidrogen dapat secara otomatis mengakses blockchain.



Ruang lingkup platform layanan keuangan yang dapat memanfaatkan Hidrogen luas. Platform ini dapat menghasilkan hampir semua pengalaman, menyimpan sejumlah layanan eksklusif, melakukan operasi data pribadi, dan menyebarkan di lingkungan apa pun. Ini dimungkinkan oleh modularitas struktural Hidrogen dan sinergis dengan Hydro, bertindak sebagai penggerak adopsi.

Titisan hujan

Dibangun di atas Hydro public ledger ini adalah layanan otentikasi berbasis blockchain, yang disebut "Raindrop." Ini menawarkan lapisan

keamanan yang berbeda, tidak berubah, dapat dilihat secara global yang memverifikasi permintaan akses berasal dari sumber resmi.

Protokol autentikasi pribadi seperti OAuth 2.0 menawarkan berbagai tingkat ketahanan dan kegunaan untuk spektrum kasus penggunaan yang ada. Ada sedikit kebutuhan untuk bersaing dengan atau mencoba mengganti protokol ini - Hydro menawarkan cara untuk meningkatkannya dengan menggabungkan mekanika blockchain sebagai komponen dari prosedur otentikasi. Ini dapat menambahkan lapisan keamanan yang berguna untuk membantu menggagalkan pelanggaran sistem dan kompromi data.

Sebelum memeriksa aspek teknis Raindrop, mari kita lihat masalah yang coba dipecahkan.

Keadaan Keamanan Keuangan

Munculnya usia data telah membawa peningkatan kerentanan, dan ini sangat penting untuk layanan keuangan. Platform keuangan seringkali merupakan gerbang ke sejumlah besar data pribadi dan sensitif seperti nomor ID pemerintah, kredensial akun, dan riwayat transaksi. Karena betapa pentingnya data ini, akses yang tidak beralasan biasanya dipenuhi dengan hasil bencana.

Perusahaan riset industri Trend Micro menerbitkan sebuah laporan yang menemukan item baris yang dicuri dari Informasi Identitas Pribadi (PII) yang dijual di Deep Web seharga $ 1, scan dokumen seperti paspor tersedia hanya dengan $ 10, dan kredensial login bank untuk sedikitnya $ 200, membuat distribusi data yang dicuri semakin terfragmentasi dan tidak dapat dilacak.

Sayangnya, sistem keuangan yang ada tidak memiliki rekam jejak yang tidak ada noda ketika datang untuk mencegah, mendiagnosis, dan mengkomunikasikan pelanggaran data dengan para pemangku kepentingannya.

- Menurut penelitian terbaru oleh Javelin Strategy & Research - *Studi Identitas Penipuan 2017* - $ 16 miliar dicuri dari 15,4 juta pelanggan AS pada tahun 2016 karena kegagalan sistem keuangan untuk melindungi Informasi Identitas Pribadi (PII).
- Pada April 2017, Symantec menerbitkan *Laporan Ancaman Keamanan Internet*, yang memperkirakan 1,1 miliar keping PII dikompromikan dalam berbagai kapasitas selama 2016.

- *Quickview Data Akhir Akhir Pelanggaran Tahun 2016* oleh Risk Based Security, menemukan bahwa 4.149 pelanggaran data terjadi dalam bisnis global pada tahun 2016, yang mengekspos lebih dari 4,2 miliar rekaman.

- *Laporan Ancaman Data Thales Tahun 2017* - Edisi Layanan Keuangan, survei terhadap profesional TI global dalam layanan profesional, menemukan bahwa 49% organisasi jasa keuangan telah mengalami pelanggaran keamanan di masa lalu, 78% menghabiskan lebih banyak untuk melindungi diri mereka sendiri, tetapi 73 % meluncurkan inisiatif baru terkait dengan teknologi AI, IoT, dan cloud sebelum menyiapkan solusi keamanan yang sesuai.

Equifax Breach

Pada 29 Juli 2017, Equifax, lembaga pelaporan kredit AS berusia 118 tahun, diretas. 143 juta konsumen terkena PII, termasuk Nomor Jaminan Sosial. 209.000 pelanggan memiliki data kartu kredit yang disusupi.

Apa penyebab dari pelanggaran ini?

Ini dimulai dengan salah satu teknologi backend yang digunakan oleh Equifax. Struts adalah framework open source untuk mengembangkan aplikasi web dalam bahasa pemrograman Java, yang dibangun oleh Apache Software Foundation. CVE-2017-9805 adalah kerentanan dalam Apache Struts terkait dengan menggunakan plugin Struts REST dengan handler XStream untuk menangani muatan XML. Jika dieksploitasi, itu memungkinkan penyerang tidak terautentikasi untuk menjalankan kode berbahaya pada server aplikasi untuk mengambil alih mesin atau meluncurkan serangan lebih lanjut darinya. Ini ditambal oleh Apache dua bulan sebelum pelanggaran Equifax.

Apache Struts berisi cacat di REST Plugin XStream yang dipicu karena program tidak secara hati-hati menonaktifkan input yang disediakan oleh pengguna dalam permintaan XML. Lebih khusus lagi, masalah terjadi dalam metode XStreamHandler toObject (), yang tidak memaksakan pembatasan apa pun pada nilai yang masuk saat menggunakan Deserialization XStream ke objek, yang menghasilkan kerentanan eksekusi kode arbitrer.

Bahkan jika plugin REST ini disusupi, apakah itu penting? Apakah ada cara untuk menggunakan teknologi blockchain untuk mengamankan

informasi keuangan dari 143 juta pelanggan ini sementara masih mengandalkan REST API dan sistem berbasis Java?

Menambahkan Layer Blockchain

Jelas bahwa integritas gateway data keuangan dapat ditingkatkan. Mari kita periksa bagaimana lapisan keamanan tambahan dicapai melalui Hydro.

Mekanisme konsensus mendasar dari jaringan Ethereum memastikan validitas transaksional karena peserta secara kolektif memproses transaksi yang ditandatangani dengan benar. Kenyataan ini mengarah pada desentralisasi dan kekekalan, tetapi, yang lebih penting, ia menyediakan vektor untuk mengurangi akses tidak sah ke gateway yang menangani data sensitif.

Dengan Hydro, otentikasi dapat didasarkan pada operasi transaksional pada blockchain. Sebuah API, misalnya, dapat memilih untuk memvalidasi pengembang dan aplikasi dengan mengharuskan mereka untuk memulai transaksi tertentu, dengan muatan data tertentu, antara alamat tertentu pada blockchain, sebagai prasyarat yang mendorong protokol otentikasi standar.

Hydro Raindrop

Hujan berisi paket air kental mulai dari 0,0001 hingga 0,005 sentimeter dengan diameter. Dalam hujan badai yang khas, ada miliaran paket ini, masing-masing ukuran acak, kecepatan, dan bentuk. Karena itu, seseorang tidak dapat memperkirakan dengan pasti sifat hujan yang tepat. Demikian pula, setiap transaksi otentikasi Hidro adalah unik dan hampir tidak mungkin terjadi secara kebetulan - itulah sebabnya kami menyebutnya Raindrops.

Platform layanan keuangan biasanya menggunakan verifikasi deposito mikro untuk memvalidasi akun klien. Konsepnya sederhana: platform membuat setumpuk kecil jumlah acak ke akun bank yang diklaim pengguna. Untuk membuktikan bahwa pengguna memang memiliki akun tersebut, ia harus meneruskan jumlah setoran kembali ke platform, yang kemudian divalidasi. Satu-satunya cara pengguna dapat mengetahui jumlah yang valid (selain menebak) adalah dengan mengakses rekening bank yang bersangkutan.

Verifikasi berbasis hujan dengan Hydro adalah analog. Alih-alih mengirim jumlah pengguna dan mengirimkannya kembali, kami mendefinisikan transaksi dan pengguna harus mengeksekusinya dari dompet yang dikenal. Satu-satunya cara pengguna dapat melakukan transaksi yang valid adalah dengan mengakses dompet yang bersangkutan.

Dengan menggunakan Raindrops, baik sistem dan pengakses dapat memantau upaya otorisasi pada buku besar publik abadi. Transaksi berbasis blockchain ini dipisahkan dari operasi sistem dasar, terjadi pada jaringan terdistribusi, dan tergantung pada kepemilikan kunci privat. Oleh karena itu, berfungsi sebagai vektor validasi yang berguna.

Tampilan Terperinci

Ada empat entitas yang terlibat dalam proses otentikasi Hidro:

1. Accessor - Pihak yang mencoba mengakses suatu sistem. Dalam kasus Hidrogen, pengakses adalah lembaga keuangan atau aplikasi yang memanfaatkan API Hidrogen untuk infrastruktur digital intinya.
2. Sistem - Sistem atau gateway yang sedang diakses oleh Accessor. Untuk Hidrogen, sistemnya adalah API Hidrogen itu sendiri.
3. Hidro - Modul yang digunakan oleh Sistem untuk berkomunikasi dan berinteraksi dengan blockchain.

Blockchain - Buku besar publik terdistribusi yang memproses transaksi HYDRO dan berisi kontrak cerdas Hydro, di mana informasi dapat didorong, ditarik, atau dioperasi.

Setiap Rintik Hujan, secara keseluruhan, adalah satu set lima parameter transaksional:

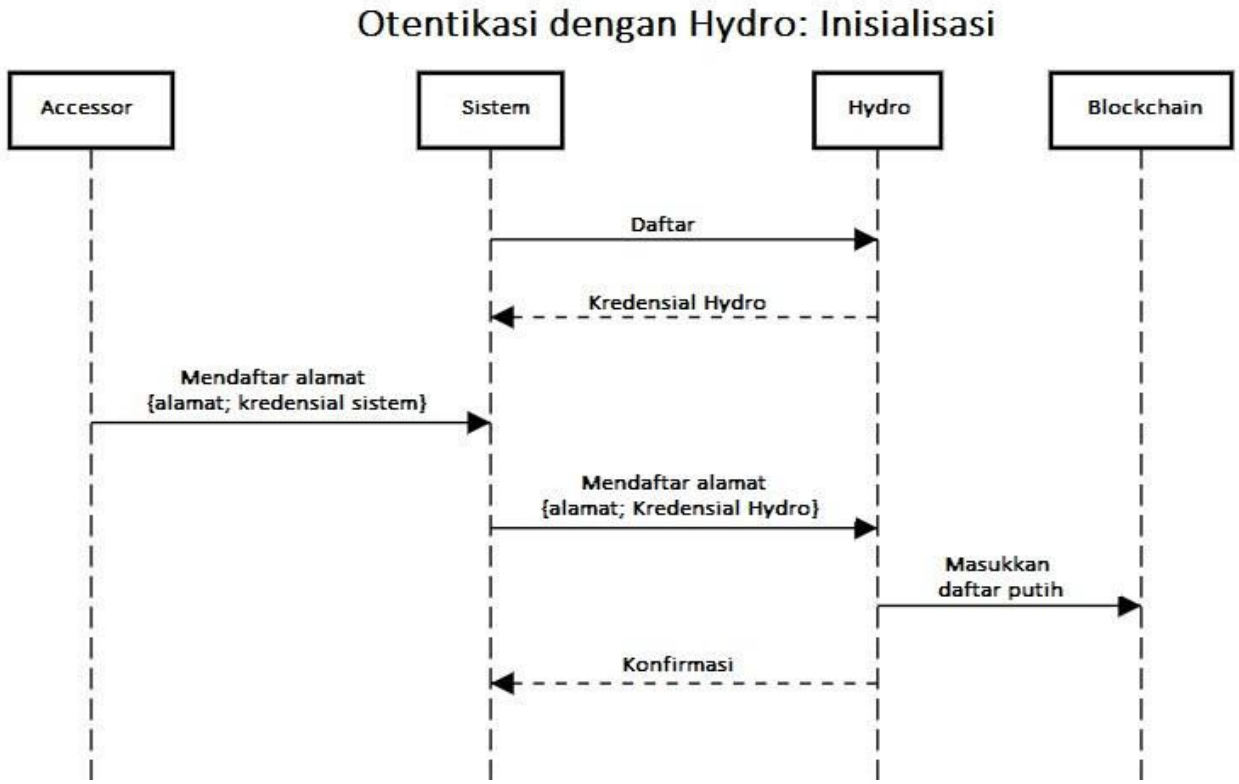
1. Pengirim - Alamat yang harus memulai transaksi.
2. Penerima - Tujuan transaksi. Ini sesuai dengan pemanggilan metode dalam kontrak cerdas Hydro.
3. ID - Identifier yang terkait dengan Sistem.
4. Kuantitas - Jumlah tepat HYDRO untuk dikirim.
5. Tantangan - String alfanumerik yang dihasilkan secara acak.

Di bawah ini adalah garis besar proses otentikasi, yang secara umum dapat diklasifikasikan menjadi tiga tahap:

1. Inisialisasi

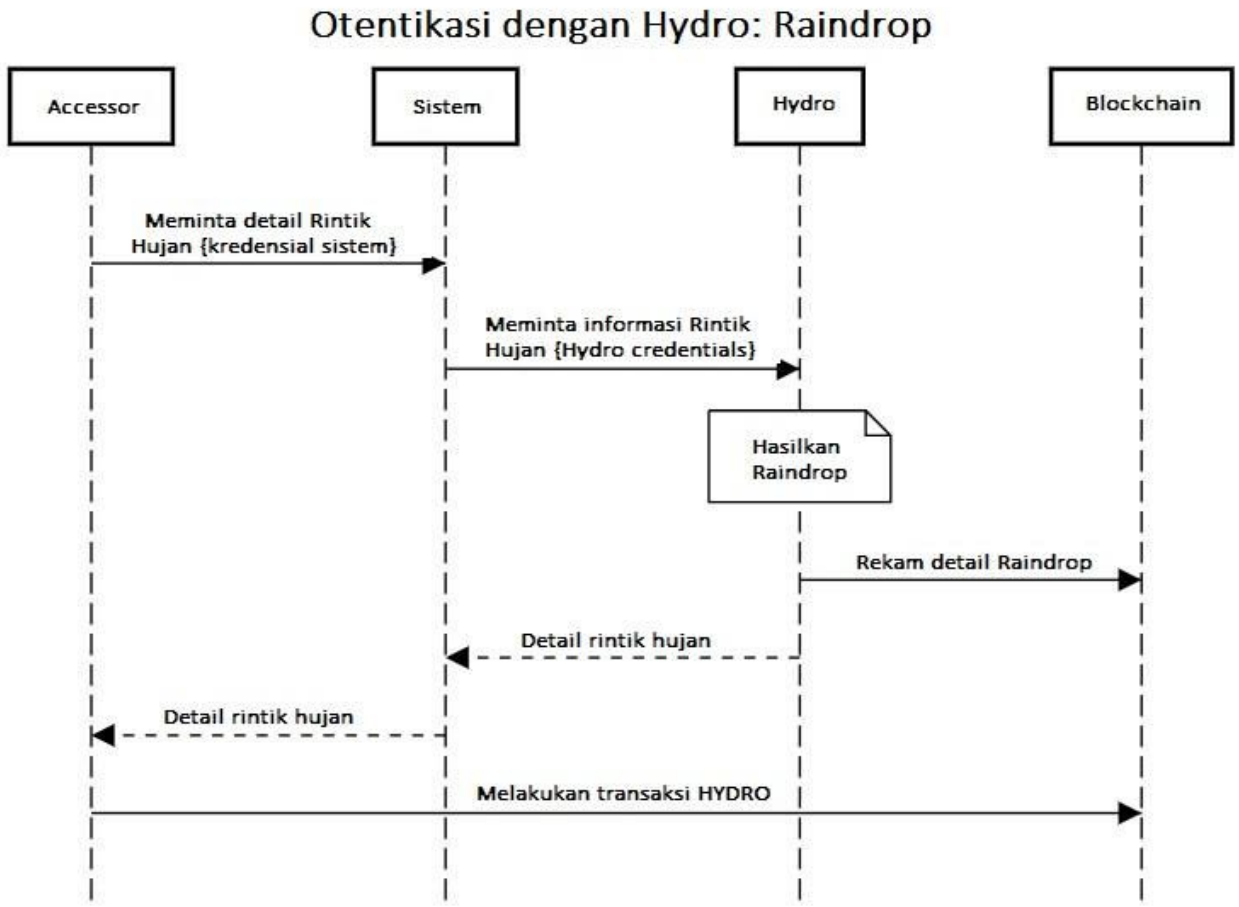
2. Raindrop
3. Validasi

Inisialisasi dimulai dengan Sistem (misalnya Hidrogen) yang mendaftar untuk menggunakan Hydro dan memperoleh kredensial, memungkinkan sistem untuk berkomunikasi dengan blockchain melalui modul Hydro. Sistem onboard, Accessor (misalnya lembaga keuangan) yang mendaftarkan alamat publik, dan kemudian meneruskan alamat terdaftar ke Hydro. Alamat ini ditulis secara permanen ke blockchain ke daftar putih yang disimpan dalam kontrak cerdas Hydro. Sistem menerima konfirmasi bahwa alamat itu masuk daftar putih, yang juga dapat diverifikasi sebagai acara yang dapat dilihat publik. Pendaftaran sistem hanya perlu dilakukan sekali, sedangkan daftar putih Accessor hanya perlu dilakukan sekali per Accessor.

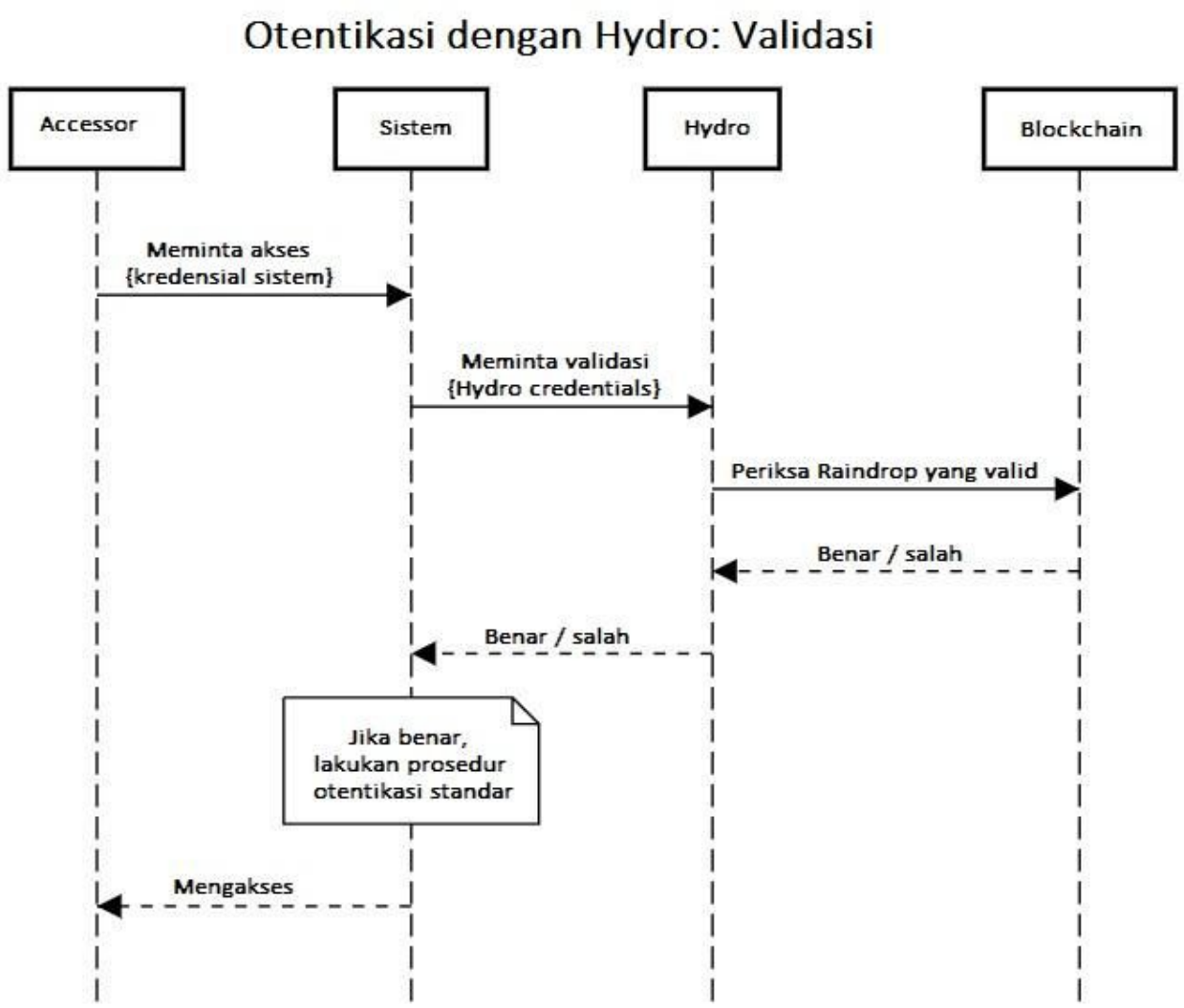


Setelah Inisialisasi selesai, inti dari proses otentikasi Hydro dapat dimulai. Accessor, yang harus menjalankan transaksi Raindrop, memulai proses ini dengan meminta detail Raindrop dari Sistem, dan Sistem mengarahkan permintaan ke Hydro. Hydro menghasilkan Raindrop baru, menyimpan detail tertentu pada blockchain, dan mengembalikan detail lengkap ke Accessor melalui Sistem. The Accessor, dilengkapi dengan semua informasi yang diperlukan, melakukan transaksi dari alamat terdaftar ke metode dalam kontrak cerdas Hydro. Jika alamat tidak masuk daftar putih, tindakan ditolak - jika tidak, dicatat dalam

kontrak pintar. Penting untuk dicatat bahwa transaksi ini harus terjadi di luar Sistem, langsung dari Accessor ke Blockchain, karena harus ditandatangani dengan kunci pribadi Accessor (yang hanya dapat diakses oleh Accessor).



Langkah terakhir dari proses ini adalah Validasi. Dalam langkah ini, Accessor secara resmi meminta akses ke Sistem melalui mekanisme yang ditetapkan Sistem. Sebelum menerapkan salah satu protokol otentikasi standar, Sistem meminta Hydro apakah Accessor telah melakukan transaksi Raindrop yang valid. Hydro berinteraksi dengan kontrak cerdas, memeriksa validitas, dan merespons dengan sebutan yang benar / salah. Sistem ini dapat memutuskan bagaimana harus melanjutkan berdasarkan penunjukan ini - jika salah, Sistem dapat menolak akses, dan jika itu benar, Sistem dapat memberikan akses.



Jika kita mempertimbangkan kredensial Sistem dasar - atau apa pun Protokol Sistem yang ada yang ada - untuk secara luas menjadi salah satu faktor otentikasi, penting bahwa lapisan Hydro memberikan faktor kedua yang bermanfaat. Dengan memeriksa dua vektor serangan utama, kita dapat dengan mudah mengkonfirmasi kegunaannya:

- Vektor 1 - Penyerang mencuri kredensial Sistem dasar Accessor
  - Penyerang berupaya mendapatkan akses ke Sistem dengan kredensial Sistem yang valid
  - Sistem memeriksa dengan Hydro untuk menentukan apakah transaksi yang valid dilakukan pada blockchain
  - Hydro mengembalikan false, dan Sistem menolak akses
- Vector 2 - Penyerang mencuri kunci privat (s) ke dompet Accessor
  - Penyerang berupaya melakukan transaksi Hydro dari alamat yang terdaftar, tanpa detail Raindrop yang diperlukan
  - Penyerang tidak dapat melakukan transaksi blockchain yang valid

- Penyerang juga tidak dapat meminta akses ke Sistem tanpa kredensial Sistem yang tepat

Jelas bahwa Penyerang harus mencuri kredensial Sistem dasar dan kunci dompet pribadi Accessor untuk mengakses Sistem. Dalam hal ini, Hydro telah berhasil menambahkan faktor tambahan otentikasi.

Membuka The Raindrop Untuk Publik

Meskipun layanan otentikasi berbasis blockchain ini dirancang untuk membantu mengamankan ekosistem API Hidrogen, ia dapat diterapkan secara luas ke berbagai platform dan sistem. Karena kami merasa bahwa orang lain dapat memperoleh manfaat dari lapisan verifikasi ini, kami membukanya untuk digunakan.

Sama seperti Hidrogen akan mengintegrasikannya sebagai prasyarat untuk akses ke ekosistem API-nya, demikian pula sistem apa pun dapat menambahkannya ke prosedur dan protokol yang ada. Platform apa pun - baik itu API, aplikasi, perangkat lunak perusahaan, platform game, dll. - dapat memanfaatkan Hydro untuk tujuan autentikasi. Dokumentasi formal akan tersedia di GitHub bagi mereka yang ingin menggabungkan lapisan blockchain ini ke dalam kerangka otentikasi atau REST API.

Studi Kasus - Raindrop Dengan OAuth 2.0

Ada banyak cara pelepasan Raindrop dapat digunakan oleh organisasi swasta. API, basis data, dan jaringan pribadi telah membuat sistem token, kunci, aplikasi, dan protokol yang rumit selama dekade terakhir, dalam upaya untuk mengamankan data sensitif. Google, misalnya, menjadi salah satu penyedia produk paling populer di pasar dengan aplikasi Google Authenticator. Seperti yang disebutkan sebelumnya, tidak ada alasan untuk bersaing atau mengganti protokol yang ada.

Sebagai studi kasus, di sini adalah gambaran singkat tentang bagaimana Hidrogen menerapkan otentikasi Hydro sebagai lapisan keamanan dalam kerangka keamanan API secara keseluruhan:

1. Mitra API Hidrogen harus terlebih dahulu memiliki alamat IP dari berbagai lingkungan mereka yang masuk daftar putih.
2. Mitra harus meminta ke daftar putih alamat Hydro publik.
3. Semua panggilan ke API Hidrogen dan transfer data dienkripsi dan dikirimkan melalui protokol HTTPS.

4. Mitra harus menyelesaikan transaksi hujan Hydro yang valid dari alamat Hydro yang terdaftar.
5. Mitra harus menggunakan validasi OAuth 2.0. OAuth (Otorisasi Terbuka) adalah standar terbuka untuk otentikasi dan otorisasi berbasis token. Hidrogen mendukung "Jenis Kredensial Sandi Pemilik Sumber Daya" dan "Kredensial Klien", dan setiap pengguna API harus memberikan kredensial untuk permintaan otentikasi.
6. Jika tidak ada dari lima elemen di atas dilanggar, mitra Hidrogen diberikan token unik, untuk diperiksa dan diverifikasi dengan setiap panggilan API.
7. Token berlaku selama 24 jam, setelah itu mitra harus memvalidasi diri lagi.

Jika salah satu dari langkah-langkah ini dilanggar, pengguna segera dikunci dari akses API. Seorang peretas tidak dapat melewati faktor keamanan ini dengan menebak secara acak, karena ada triliunan kombinasi unik.

Autentikasi berbasis blockchain Hydro merupakan komponen penting dari protokol keamanan Hidrogen. Tim Hidrogen mendorong mitra untuk menyiapkan dompet multi-tanda tangan, dan menyimpan kunci pribadi di beberapa lokasi aman secara terpisah dari kredensial lainnya, sehingga tidak ada satu pun titik kegagalan. Dompet multi-tanda tangan yang aman tidak hanya sulit untuk dicuri, tetapi sifat publik dari blockchain juga memungkinkan untuk pengenalan cepat dari setiap pencurian yang berkaitan dengan keamanan API.

Siapa pun dapat melihat upaya otentikasi untuk kontrak cerdas Hydro, yang berarti hari-hari platform yang dikompromi selama berbulan-bulan on-end dapat menjadi sesuatu dari masa lalu. Peretas API sekarang dapat digagalkan dengan lebih cepat karena kemampuan untuk mendeteksi upaya otorisasi yang tidak diharapkan secara waktu nyata, dari mana saja di dunia.

Risiko

Sama seperti teknologi yang baru lahir, seperti hari-hari awal media sosial, email, dan aplikasi streaming (yang bergantung pada konektivitas dial-up), penting bahwa tim pengembangan inti melacak perkembangan baru dalam kecepatan dan volume transaksi Ethereum. Bisakah Anda bayangkan YouTube mencoba meluncurkan pada tahun 1995? Atau Instagram pertama kali ditawarkan di Blackberry?

Pengembang Core Ethereum seperti Vitalik Buterin dan Joseph Poon telah mengusulkan [Plasma: Scalable Autonomous Smart Contracts] upgrade ke protokol Ethereum:

> **Plasma adalah kerangka yang diusulkan untuk insentif dan pelaksanaan kontrak cerdas yang dapat ditingkatkan untuk sejumlah besar pembaruan negara per detik (berpotensi miliaran) memungkinkan blockchain untuk dapat mewakili sejumlah besar aplikasi keuangan terdesentralisasi di seluruh dunia. Kontrak cerdas ini diberi insentif untuk melanjutkan operasi secara mandiri melalui biaya transaksi jaringan, yang pada akhirnya bergantung pada rantai blok yang mendasarinya (misalnya Ethereum) untuk menegakkan transisi status transaksional.**

Lainnya, seperti The Raiden Network, telah mengusulkan solusi skala off-chain yang dirancang untuk memberdayakan transaksi lebih cepat dan biaya lebih rendah. Pada saat ini, Raindrop akan memberikan tekanan yang sangat minim pada kerangka Ethereuem, sehingga skalabilitas merupakan risiko yang sangat kecil bagi keberhasilan teknologi.

Kesimpulan

Ketidakmampuan blockchain publik menawarkan cara-cara baru untuk meningkatkan keamanan sistem pribadi seperti API.

Makalah ini telah menunjukkan tiga hal penting:

1. Blockchains publik dapat menambah nilai dalam layanan keuangan.
2. Hydro Raindrop dapat meningkatkan keamanan sistem pribadi.
3. Ada aplikasi langsung dari Hydro Raindrop dalam platform API Hidrogen.

Tim Hydro percaya bahwa kerangka yang ditetapkan dapat menjadi infrastruktur keamanan standar untuk model baru sistem publik-swasta hibrida, yang akan menguntungkan semua pemangku kepentingan dalam industri jasa keuangan dan seterusnya.

Sumber:

Ethereum; Menimang di Ethereum
Trend Micro; Apa yang Dilakukan Peretas dengan Identitas Anda yang Dicuri?
Strategi & Penelitian Javelin; Studi Penipuan Identitas 2017
Symantec; Laporan Ancaman Keamanan Internet
Keamanan Berbasis Risiko; Tren Pelanggaran Data 2016 - Ulasan dalam Tahun
Thales; 2017 Thales Data Threat Report - Edisi Layanan Keuangan
Apache.org; Apache Struts 2 Dokumentasi - S2-052
Joseph Poon dan Vitalik Buterin; Plasma: Kontrak Pintar Otonom Skala Kecil