Raindrop hidro

Autenticação pública sobre o Blockchain

Janeiro de 2018

TABELA DE CONTEÚDOS

Resumo

Blockchain & Ethereum
- Edifício em Ethereum
- Árvores de Merkle
- Contratos inteligentes
- Máquina Virtual de Ethereum

Contabilidade pública
- Um livro de contabilidade público para sistemas privados Arquitetar para adoção

Gota de chuva
- O estado de segurança financeira
- Violação da Equifax
- Adicionando uma camada de Blockchain
- A gota de chuva hidro
- Um olhar detalhado
- Abertura ao público o pingo de chuva
- Estudo de caso - pingo de chuva com OAuth 2.0

Riscos

Conclusão

Resumo

HYDRO: etimologia - Do grego antigo ὑδρο - (*hudro* -), de ὕδωρ (*húdōr*, "água")

Hidro permite que novos e existentes sistemas privados perfeitamente integrar e alavancar a dinâmica imutável & transparente de um blockchain público para melhorar a aplicação e a segurança de documentos, gerenciamento de identidades, transações e inteligência artificial.

Neste trabalho, será feito um caso para sistemas privados, como APIs, usar a hidro blockchain pública para melhorar a segurança através de autenticação pública.

A tecnologia proposta é chamada "Pingo" - uma transação realizada por meio de um contrato inteligente que valida o acesso do sistema privado ao público e pode complementar os métodos de autenticação privada existentes. A tecnologia destina-se a fornecer segurança adicional para dados financeiros confidenciais que está cada vez mais em risco de pirataria e violações.

A implementação inicial da gota de chuva a Hydro é executada na plataforma API de hidrogênio. Este conjunto modular de APIs está disponível para empresas e desenvolvedores globalmente para o protótipo, construir, testar e implantar produtos e plataformas de tecnologia financeira sofisticada.

A gota de chuva Hydro estarão disponível para a comunidade de desenvolvedores do mundo como software de código aberto, para permitir aos desenvolvedores integrar as gotas da hidro com qualquer API REST.

Blockchain & Ethereum

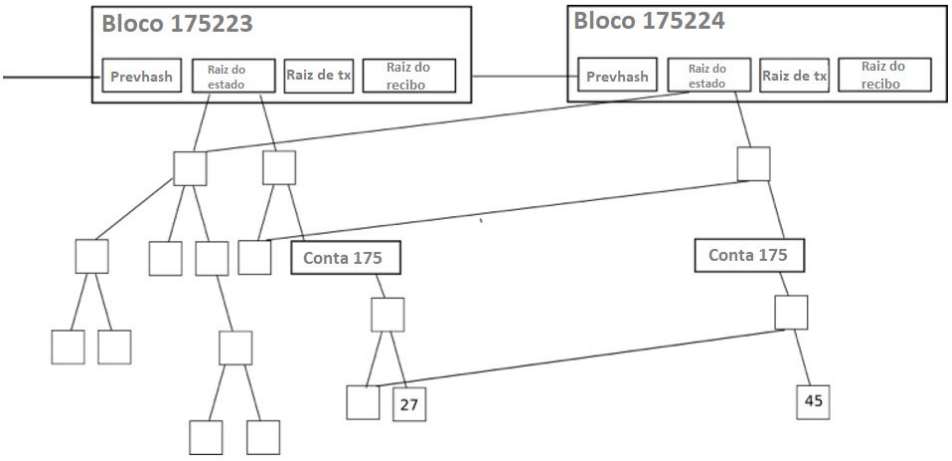
Hidro é implementado na rede Ethereum. Antes de fornecer mais detalhes sobre o projeto, é importante compreender algumas ideias fundamentais sobre blockchain e Ethereum. *Edifício em Ethereum*

Tanto quanto apps como Snapchat foram construídos com rápida e outras ferramentas oferecidas em cima da plataforma iOS da Apple, então também podem blockchain aplicativos criados em cima de Ethereum. Inc. snap não precisa construir iOS, ele é usado como infra-estrutura para lançar um jogo de mudança aplicação de meios de comunicação social.

Projeto hidro é semelhante. Ele conta com milhares de desenvolvedores globalmente que estão trabalhando para tornar a tecnologia subjacente blockchain mais rápido, mais forte e mais eficiente. Hidro aproveita isto melhorar constantemente a infra-estrutura por interações de produto com foco em desenvolvimento com a tecnologia blockchain que pode oferecer benefícios tangíveis para aplicativos de serviços financeiros.

Árvores de Merkle

Árvores de Merkle são utilizadas em sistemas distribuídos para verificação de dados eficiente. Eles são eficientes, porque eles usam hashes em vez de arquivos completos. Hashes são formas de codificação de arquivos que são muito menores do que o próprio arquivo real.
Cada cabeçalho de bloco em Ethereum contém três árvores de Merkle para transações, recibos e Estados:



Fonte: Merkling em Ethereum; Vitalik Buterin, fundador de Ethereum

Isto torna mais fácil para um cliente leve para obter respostas verificáveis para consultas, tais como:

- Será que existe essa conta?
- Qual é o saldo atual?
- Essa transação foi incluída em um bloco especial?
- Um determinado evento aconteceu nesse endereço hoje?

Contratos inteligentes

Um conceito-chave habilitado por Ethereum e outras redes baseadas em blockchain é o de *contratos inteligentes*. Estas são auto execução de blocos de código que múltiplas partes podem interagir com, corte fora a necessidade de intermediários confiáveis. Código em um contrato inteligente pode ser visto como semelhante para o judiciário cláusulas em um papel tradicional de contrato, mas também pode atingir a funcionalidade muito mais expansiva. Contratos podem ter regras, condições, sanções por incumprimento, ou pode kickstart outros processos. Quando acionado, contratos executam originalmente declarado no momento da implantação da cadeia pública, oferecendo elementos internos de imutabilidade e descentralização.

O contrato inteligente é uma ferramenta vital para construir a infra-estrutura de Ethereum. Funcionalidade principal da camada blockchain hidro é conseguida através de contratos personalizados, conforme discutido posteriormente neste artigo.

Máquina Virtual de Ethereum

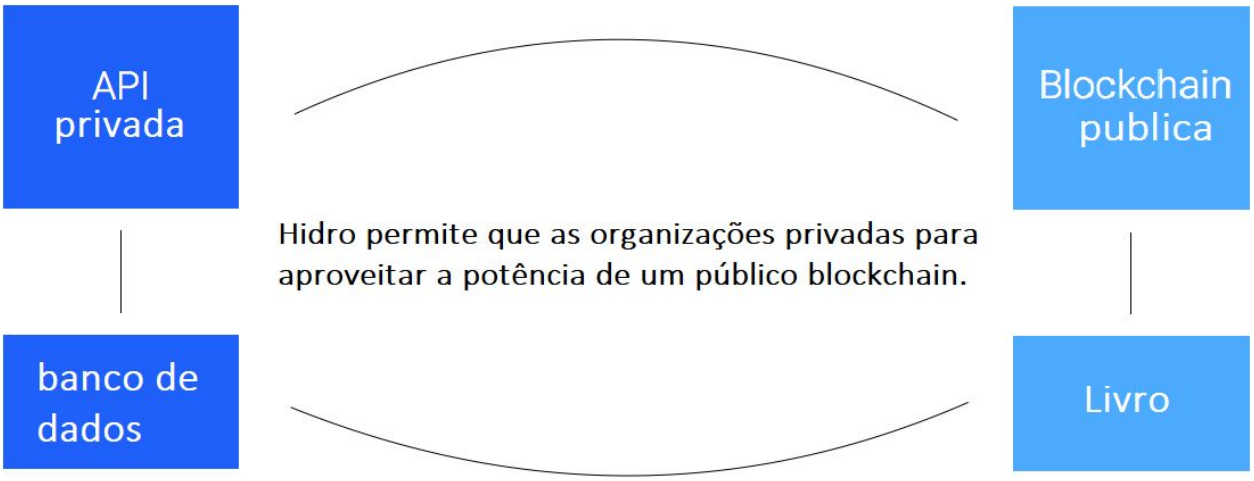
A máquina Virtual de Ethereum (EVM) é o ambiente de tempo de execução para contratos inteligentes na Ethereum. O EVM ajuda a prevenir ataques de negação de serviço (DoS), garante programas permanecem sem monitoração de estado e permite a comunicação de que não pode ser interrompida. As acções sobre o EVM têm custos associados a eles, chamado *gás*, que dependem dos recursos computacionais necessários. Cada transação tem uma quantidade máxima de gás atribuídas a ele, conhecido como um *limite de gás*. Se o gás consumido por uma transação atinge o limite, isso vai deixar de continuar o processamento.

Contabilidade pública

Um livro de contabilidade público para sistemas privados

Os sistemas que aplicativos, sites e plataformas de serviços financeiros de energia muitas vezes podem ser descritos como médiuns de fluxo de dados - eles enviar, recuperar, armazenam, atualizar e processam dados para as entidades de interface com eles. Devido à natureza destes dados e de serviços financeiros em geral, estes sistemas muitas vezes de casa operações complexas de forma privada e centralizada. Dependência de estruturas privadas, por sua vez, abre a porta para uma variedade de ganhos de eficiência a ser tido pela incorporação de forças externas que excedem o alcance do sistema interno, transparência e segurança.

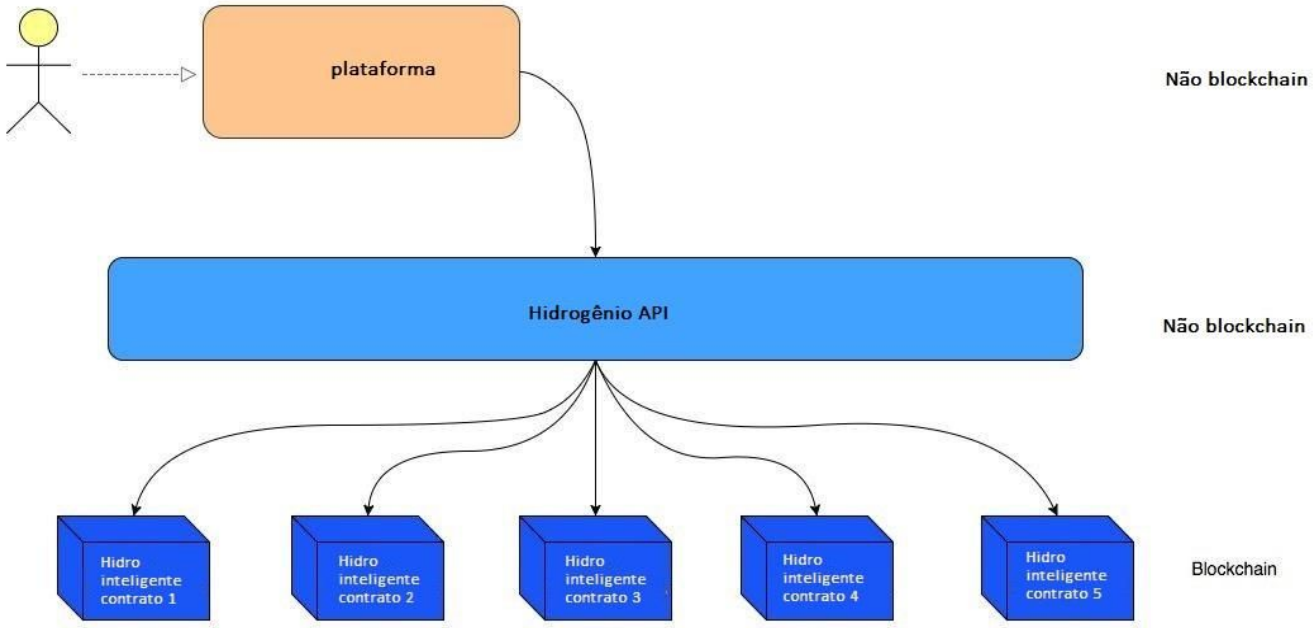
Tal é o caso com plataforma de API do hidrogênio. Hidro visa explorar os ganhos acima mencionados, permitindo que os usuários de hidrogênio fazer interface com um blockchain de maneiras que são perfeitamente integradas ao ecossistema de hidrogênio fundamentalmente privado.



Operações baseadas em blockchain públicas podem ocorrer antes, durante ou depois de operações privadas. A interação entre públicos e privados elementos pode servir para validar, carimbar, gravar ou melhorar processos dentro de um ecossistema.
O ethos deste modelo está fazendo processos mais robustos, tocando para os benefícios da tecnologia de blockchain especificamente onde pode produzir o impacto mais positivo. Enquanto este quadro híbrido pode não ser aplicável a todas as plataformas, Hydro centra-se no fornecimento de valor para os casos em que é.

Arquitetar para adoção

Hidro difere de muitas iniciativas já existentes de blockchain, porque pode existir independentemente e camada ao redor de sistemas novos ou existentes, sem a necessidade de mudança sistêmica. Em vez de substituir, Hydro visa aumentar. Plataformas e instituições que conecte as APIs de hidrogênio podem acessar automaticamente o blockchain.



O escopo de plataformas de serviços financeiros que pode alavancar o hidrogênio é amplo. Essas plataformas podem virtualmente qualquer experiência de poder, qualquer número de serviços do proprietários da casa, executar qualquer operação de dados privados e implantar em qualquer ambiente. Isso é habilitado pela modularidade estrutural do hidrogênio e é sinérgico com Hydro, agindo como um condutor complementar de adoção.

Gota de chuva

Construído em cima deste livro público hidro é um serviço de autenticação baseada em blockchain, chamado "Pingo". Isto oferece uma camada distinta,

imutável, globalmente visível de segurança que verifica se uma solicitação de acesso está vindo de uma fonte autorizada.

Protocolos de autenticação privada como OAuth 2.0 oferecem diversos níveis de robustez e utilidade para o espectro de casos de uso existentes. Há pouca necessidade de competir com ou tentar substituir estes protocolos - hidro oferece uma maneira de melhorá-los, incorporando blockchain mecânica como um componente de um processo de autenticação. Isto pode adicionar uma camada útil de segurança para ajudar a impedir falhas de sistema e compromissos de dados.

Antes de examinar os aspectos técnicos da gota de chuva, primeiro vamos dar uma olhada no que está a tentar resolver o problema. *O estado de segurança financeira*

O aumento da idade dados trouxe com um aumento da vulnerabilidade, e isto é particularmente importante para os serviços financeiros. Plataformas financeiras são frequentemente gateways para grandes quantidades de dados privados e confidenciais, como números de identificação de governo, credenciais de conta e histórias de transação. Por causa de como criticamente esses dados são importante, injustificados acesso normalmente é conhecido com resultados catastróficos.

Indústria de pesquisa empresa Trend Micro publicou um relatório que os itens de linha roubados encontrados de pessoalmente identificável informações (PII) é vendido na Web profunda por tão pouco quanto $1, scans de documentos como passaportes estão disponíveis para o tão pouco quanto $10 e banco de credenciais de logon para como pouco $200, fazendo a distribuição de dados roubados, cada vez mais fragmentada e indetectável.

Infelizmente, o sistema financeiro existente não tem um histórico impecável quando se trata de prevenção, diagnóstico e comunicar violações de dados com seus stakeholders.

- De acordo com um estudo recente da Javelin Strategy & Research - *2017 o Estudo de fraude de identidade* -US $ 16 bilhões foi roubado de 15,4 milhões E.U. consumidores em 2016 devido a falhas do sistema financeiro para proteger informações pessoalmente identificáveis (PII).
- Em abril de 2017, Symantec publicou o seu *Relatório de ameaça de segurança de Internet*, que estima 1,1 bilhões de pedaços de PII foram comprometidos em várias capacidades ao longo de 2016.

- ➢ *2016 ano final Quickview violação de dados* de segurança com base no risco, revelaram que violações de 4.149 dados ocorreram em empresas globalmente em 2016, expondo mais 4,2 bilhões de registros.
- ➢ *2017 Thales dados ameaça relatório – Financial Services Edition*, uma pesquisa da globais profissionais em serviços profissionais, descobriu que 49% das organizações de serviços financeiros têm sofreu uma falha de segurança no passado, 78% estão gastando mais para se protegerem, mas 73% a lançar novas iniciativas relacionadas com tecnologias de nuvem, AI e muito antes de preparar as soluções de segurança adequadas.

Violação da Equifax

Em 29 de julho de 2017, Equifax, um crédito E.U. 118 ano de idade, relata a agência, foi hackeado. 143 milhões de consumidores tinham PII exposto, incluindo números de Segurança Social. 209.000 clientes tinham dados de cartão de crédito comprometidos.

Qual foi a causa desta brecha?

Começa com uma das tecnologias de backend utilizadas pela Equifax. Struts é um framework open source para desenvolvimento de aplicações web em linguagem, construída pela Apache Software Foundation de programação Java. CVE-2017-9805 é uma vulnerabilidade no Apache Struts relacionados ao uso do plugin de resto Struts com o manipulador XStream para lidar com cargas XML. Se explorada, permite que um invasor remoto não autenticado executar código mal-intencionado no servidor de aplicativos para assumir a máquina ou ainda lançar ataques dele. Isto foi corrigido pelo Apache dois meses antes da Equifax violar .

Apache Struts contém uma falha no resto Plugin XStream disparado como o programa inseguro de-serializes entrada fornecida pelo usuário em solicitações XML. Mais especificamente, o problema ocorre no método de toObject() do XStreamHandler, que não impõe qualquer restrição sobre o valor da entrada ao usar XStream desserialização em um objeto, resultando em vulnerabilidades de execução de código arbitrário.

Mesmo se este plugin de resto foi comprometido, deve importado? Existe uma maneira de usar a tecnologia blockchain para proteger a informação financeira destes clientes 143 milhões enquanto ainda depender incumbente API REST e sistemas baseados em Java?

Adicionando uma camada de Blockchain

É claro que a integridade das portas de entrada de dados financeiros pode ser melhorada. Vamos examinar como uma camada adicional de segurança é alcançada através de hidro.
Os mecanismos de consenso fundamentais da rede Ethereum garantir validade transacional, porque os participantes coletivamente processam transações que são devidamente assinadas. Esta realidade leva a descentralização e a imutabilidade, mas, mais importante, ele fornece um vetor para moderar o acesso não autorizado a um gateway que lida com dados confidenciais.

Com hidro, autenticação pode ser baseada em operações transacionais no blockchain. Uma API, por exemplo, pode escolher validar os desenvolvedores e aplicações, exigindo-lhes para iniciar transações particulares, com cargas de dados específico, entre particular aborda sobre o blockchain, como condição prévia que kickstarts um padrão Protocolo de autenticação.

A gota de chuva hidro

Chuva contém pacotes de água condensada, variando de 0,0001 a 0,005 centímetros de diâmetro. Em uma típica tempestade, existem bilhões desses pacotes, cada um de forma, velocidade e tamanho aleatório. Por causa disso, um confiável não pode prever a natureza exata da chuva. Da mesma forma, todas as transações de autenticação hidro são única e virtualmente impossível ter ocorrido por acaso - é por isso que lhes chamamos *pingos de chuva*.

Plataformas de serviços financeiros comumente utilizam *microdepósito* verificação para validar as contas do cliente. O conceito é simples: a plataforma faz pequenos depósitos de quantias aleatórias em contas bancárias alegado de um usuário. A fim de provar que o usuário realmente possui tal conta, ele ou ela deve retransmitir os montantes de depósito para a plataforma, que posteriormente são validados. A única maneira que o usuário pode saber os montantes válidos (além de adivinhar) está acessando as contas do banco em questão.

Verificação baseada na gota de chuva com Hydro é análoga. Ao invés de enviar o usuário uma quantidade e tê-lo retransmitidas volta, definimos uma transação e o usuário deve executá-lo de uma carteira de conhecidos. A única maneira que o usuário pode realizar uma transação válida é acessando a carteira em questão.

Por meio de gotas de chuva, o sistema e o acessador podem monitorar tentativas de autorização em uma contabilidade pública imutável. Esta transação baseada em blockchain é desassociada as operações básicas do

sistema, ocorre em uma rede distribuída e depende da posse de chaves privadas. Portanto, ele serve como um vetor de validação útil.

Um olhar detalhado

Existem quatro entidades envolvidas no processo de autenticação de hidromassagem:

1. *Acessador* - A festa que a tentativa de acessar um sistema. No caso do hidrogênio, o acessador é uma instituição financeira ou app utilizando as APIs do hidrogênio para sua infra-estrutura digital de núcleo.
2. *Sistema* –O sistema ou o gateway que está sendo acessado pelo acessador. Para o hidrogênio, o sistema é a própria API de hidrogênio.
3. *Hydro* –O módulo que é utilizado pelo sistema para se comunicar e interagir com o blockchain.
4. *Blockchain* –O livro público distribuído que processa transações hidroeléctricas e contém os contratos inteligentes Hydro, através do qual a informação pode ser empurrada, puxado, ou caso contrário operado.

Cada gota de chuva, em sua totalidade, é um conjunto de cinco parâmetros transacionais:

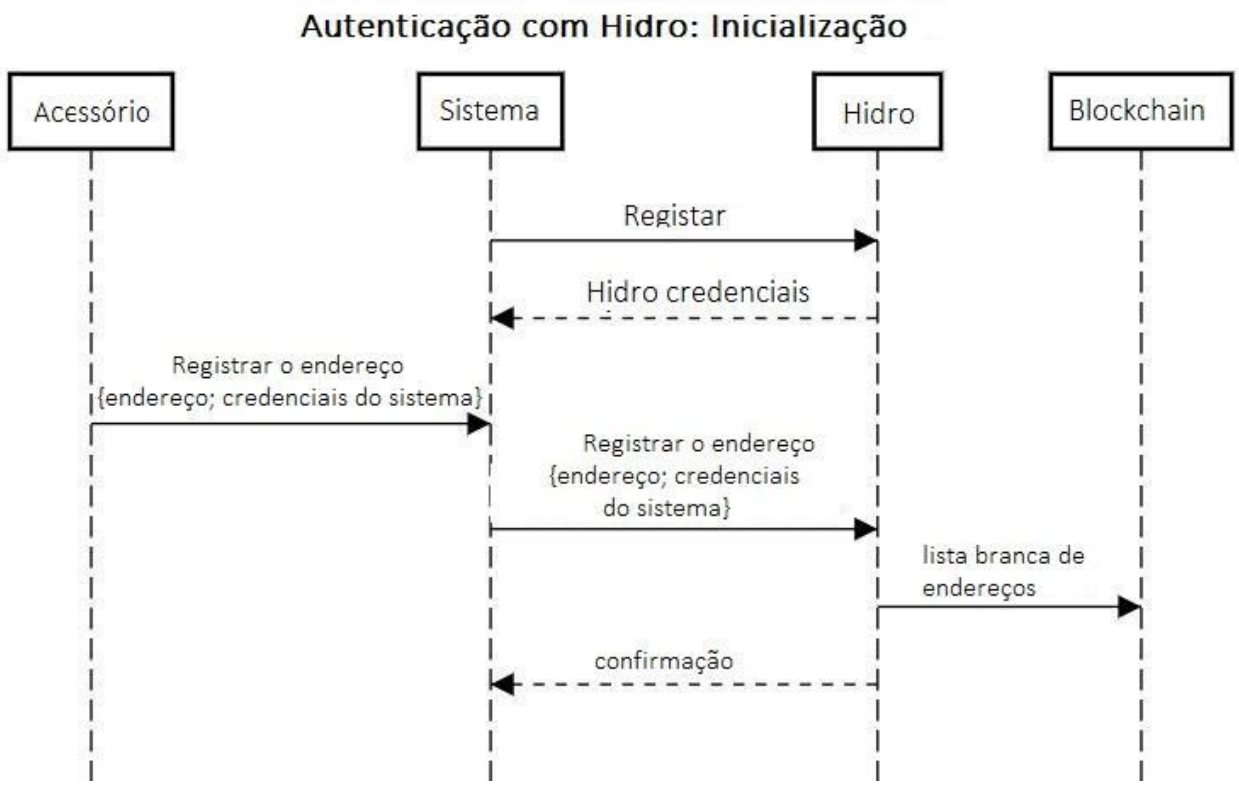
1. *Remetente* –O endereço que deve iniciar a transação.
2. *Receptor* –Destino da transação. Isso corresponde ao chamar um método em um contrato de hidromassagem inteligente.
3. *ID* - Uma identificador que está associado com o sistema.
4. *Quantidade* –Um número preciso de hidro para enviar.
5. *Desafio* –A aleatoriamente gerada a sequência de caracteres alfanumérica.

Abaixo está um resumo do processo de autenticação, que pode ser geralmente classificado em três estágios:

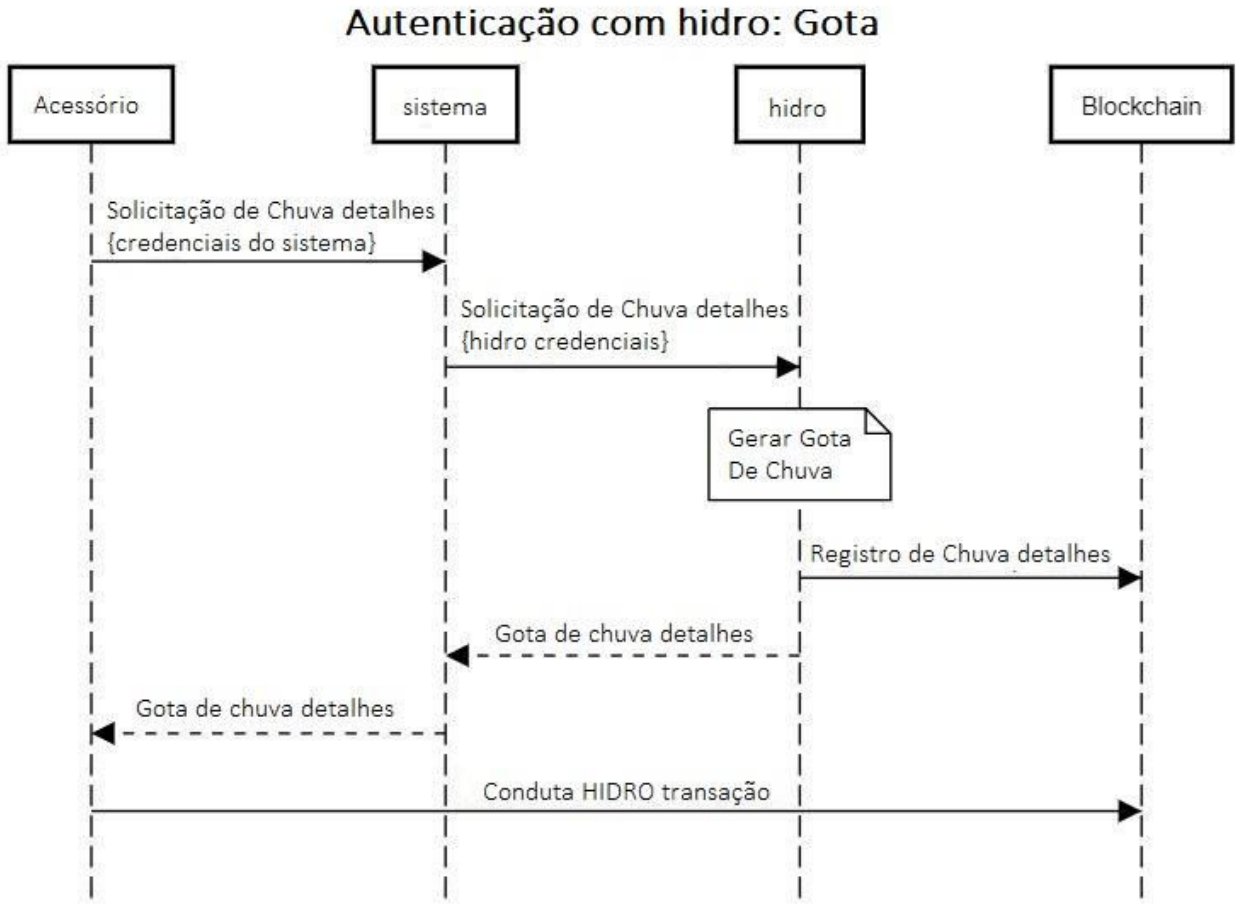
1. Inicialização
2. Gota de chuva
3. Validação

Começa a inicialização com um sistema (por exemplo, hidrogênio) registrando para usar hidroeléctricas e obtenção de credenciais, permitindo que o sistema para se comunicar com o blockchain através do módulo hidro. O sistema onboards um acessador (por exemplo, uma instituição financeira), que registra

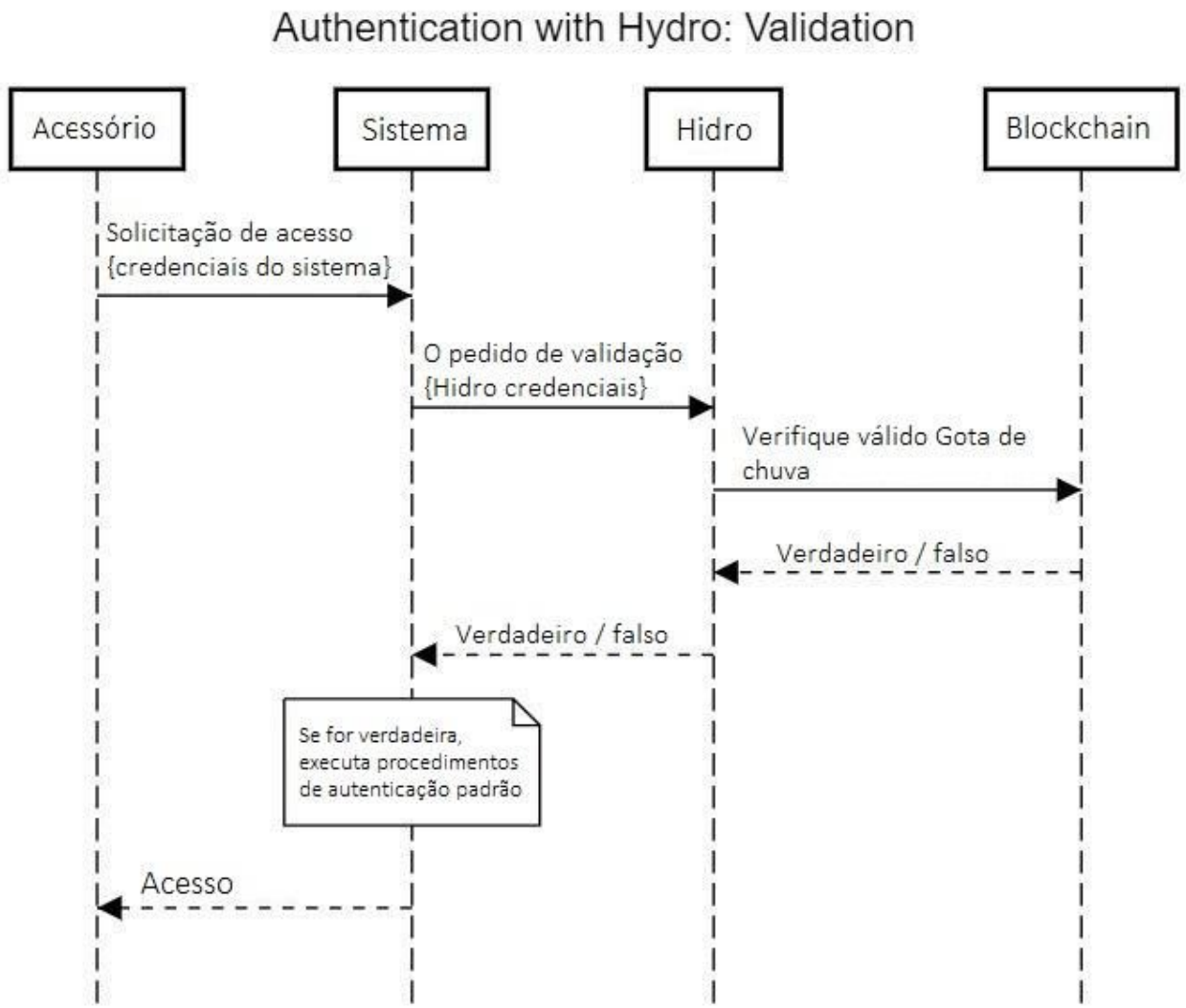
um endereço público e em seguida, passa o endereço registrado para hidro. Este endereço é imutavelmente escrito para o blockchain para um whitelist armazenado em um contrato de hidromassagem inteligente. O sistema recebe uma confirmação de que o endereço era na lista branca, que também pode ser verificada como um evento publicamente visível. Registro do sistema precisa ocorrer somente uma vez, enquanto whitelisting acessador precisa ocorrer somente uma vez por acessador.



Depois que a inicialização for concluída, o núcleo do processo de autenticação hidro pode começar. O acessador, que deve executar uma transação de gota de chuva, jumpstarts este processo solicitando detalhes Raindrop do sistema e o sistema encaminha a solicitação para Hydro. Hidro gera uma nova gota de chuva, armazena certos detalhes imutavelmente no blockchain e retorna os dados completos para o acessador via sistema. O acessador, equipado com todas as informações, realiza uma transação a partir do endereço registrado para um método no contrato de hidromassagem inteligente. Se o endereço não estiver na lista branca, a ação é rejeitada - caso contrário, está registrado no contrato inteligente. É importante notar que esta transação deve ocorrer fora do sistema, diretamente do acessador para a Blockchain, como ele deve ser assinado com chave privado do acessador (que só o acessador deve ser capaz de obter).



É a etapa final do processo de validação. Nesta etapa, o acessador oficialmente solicita acesso ao sistema via mecanismo estabelecido do sistema. Antes de implementar qualquer um dos seus protocolos de autenticação padrão, o sistema perguntará Hydro ou não o acessador realizou uma transação válida de gota de chuva. Hydro interfaces com o contrato inteligente, verificações de validade e responde com uma designação de verdadeiro/falso. O sistema é capaz de decidir como deve proceder com base nesta designação - se for false, o sistema pode negar acesso e se é verdade, o sistema pode conceder acesso.



Se considerarmos as credenciais do sistema base - ou qualquer protocolo de sistema existente que está no lugar - a amplamente ser um fator de autenticação, é importante que a camada de hidro fornece um segundo factor útil. Examinando-se os dois vetores de ataque primário, podemos facilmente confirmar sua utilidade:

- Vetor 1 - invasor rouba credenciais do sistema base do acessador
  - Invasor tenta ganhar acesso à rede com credenciais válidas do sistema
  - Sistema verifica com hidro para determinar se uma transação válida foi feita sobre o blockchain
  - Hidro retorna false, e o sistema nega acesso

- Vector 2 - atacante rouba as chaves privadas a carteira do acessador
    - Invasor tenta realizar uma transação hidro do endereço registrado, sem detalhes necessários Raindrop
    - Atacante não pode fazer uma transação válido blockchain
    - Atacante também não pode solicitar o acesso ao sistema sem as credenciais apropriadas do sistema

É claro que o atacante deve roubar tanto as credenciais do sistema base e carteira privada chave (s) do assessor para acessar o sistema. A este respeito, Hydro foi adicionado com sucesso um fator adicional de autenticação.

Abertura ao público o pingo de chuva

Embora este serviço de autenticação baseada em blockchain foi projetado para ajudar a proteger o ecossistema de API de hidrogênio, é amplamente aplicável para diferentes plataformas e sistemas. Porque sentimos que outros potencialmente podem beneficiar desta camada de verificação, vamos abrir isso para uso.

Assim como o hidrogênio vai integrá-lo como uma condição prévia para o acesso ao seu ecossistema de API, então também pode qualquer sistema adicioná-lo aos protocolos e procedimentos existentes. Qualquer plataforma - seja uma API, o aplicativo de software da empresa, plataforma de jogos, etc.-podem aproveitar a energia hidráulica para fins de autenticação. Documentação formal será disponível no GitHub para aqueles que desejam incorporar esta camada de blockchain em uma estrutura de autenticação ou API REST.

Estudo de caso - pingo de chuva com OAuth 2.0

Existem dezenas de maneiras que a liberação da gota de chuva pode ser usada por organizações privadas. APIs privadas, bancos de dados e redes criaram sistemas elaborados de fichas, chaves, apps e protocolos na última década, em uma tentativa de proteção de dados confidenciais. Google, por exemplo, se tornou um dos mais populares provedores de produto no mercado com o Google Authenticator app. Como mencionado anteriormente, há pouca ou nenhuma razão para competir com ou substituir esses protocolos existentes.

Como um estudo de caso, aqui está uma breve visão geral de como o hidrogênio implementa autenticação hidro como uma camada de segurança em seu quadro geral de segurança de API:

1. Parceiros de hidrogênio API primeiro temos os endereços IP dos seus vários ambientes whitelisted.
2. Parceiros devem solicitar à branca um endereço público de hidro.
3. Todas as chamadas para as APIs de hidrogênio e transferências de dados são criptografadas e transmitidas através do protocolo HTTPS.
4. Parceiros devem concluir uma transação de gota de chuva hidro válido do hidro endereço registrado.
5. Parceiros devem usar OAuth 2.0 validação. OAuth (autorização de abrir) é um padrão aberto para tokens de autenticação e autorização. Hidrogênio suporta as "Credenciais de senha de proprietário de recurso" e "cliente Concessão de credenciais"tipos, e cada usuário API deve fornecer as credenciais para uma solicitação de autenticação.
6. Se nenhum dos cinco elementos acima são violados, o parceiro de hidrogênio é concedido um token único, para ser checado e verificado com cada chamada de API.
7. O token é válido por 24 horas, após o qual o parceiro deve validar se novamente.

Se qualquer uma dessas etapas é violada, o usuário é bloqueado imediatamente de acesso à API. Um hacker não pode ignorar estes fatores de segurança por adivinhar aleatoriamente, pois existem trilhões de combinações únicas.

Autenticação baseada em blockchain hidro é um componente importante do protocolo de segurança de hidrogênio. A equipe de hidrogênio incentiva parceiros configurar assinatura várias carteiras, e armazenar chaves privadas em vários locais seguros, independentemente de outras credenciais, então não há um único ponto de falha. Uma carteira multi assinatura devidamente protegida não é apenas difícil de roubar, mas a natureza pública do blockchain também permite o rápido reconhecimento de qualquer roubo no que se refere à segurança da API.
Qualquer um pode ver uma tentativa de autenticação no contrato inteligente Hydro, que significa que os dias de plataformas sendo comprometidas por meses na ponta podem ser uma coisa do passado. Os hackers API agora podem ser contrariados com mais imediatismo devido a capacidade de detectar tentativas de autorização inesperada em tempo real, de qualquer lugar no mundo.

Riscos

Tanto como qualquer tecnologia emergente, tais como os primeiros dias de mídias sociais, e-mail e streaming de aplicativos (que eram dependentes de conectividade dial-up), é importante que a equipe de desenvolvimento do núcleo estreitamente acompanhar novos desenvolvimentos em velocidades de transação Ethereum e volumes. Você poderia imaginar YouTube tentando lançar em 1995? Ou Instagram, primeiro a ser oferecido no Blackberry?

Ethereum os desenvolvedores do núcleo tais como Vitalik Buterin e Joseph Poon propuseram a Plasma: Scalable autónoma contratos inteligente atualização do protocolo de Ethereum:

> **O plasma é um quadro proposto para a execução forçada e incentivada de contratos inteligentes que é escalável para uma quantidade significativa de estado atualizações por segundo (potencialmente bilhões), permitindo que o blockchain ser capaz de representar uma quantidade significativa de descentralizado financeira aplicações em todo o mundo. Estes contratos inteligentes são incentivados para continuar a operação de forma autônoma através de taxas de transação de rede, que é em última análise, dependentes da blockchain subjacente (por exemplo, Ethereum) para impor estado transacional transições.**

Outros, tais como a rede de Raiden, tem proposto uma solução dimensionamento fora da cadeia, projetada para operações mais rápidas de poder e tarifas mais baixas. Neste momento, a gota de chuva **vai colocar muito mínima tensão** sobre o quadro de Ethereuem, assim, a escalabilidade é um risco muito pequeno para o sucesso da tecnologia.

Conclusão

A imutabilidade de um blockchain público oferece novas maneiras para melhorar a segurança dos sistemas privados como APIs.

Este papel tem mostrado três coisas importantes:

1. Blockchains pública pode agregar valor em serviços financeiros.
2. As gotas de energia hidráulica pode melhorar a segurança dos sistemas privados.
3. Existem aplicações imediatas das gotas da hidro dentro da plataforma API de hidrogênio.

A equipa de hidro acredita que a estrutura estabelecida pode ser a infra-estrutura de segurança padrão para um novo modelo de sistemas híbridos público-privadas, que irá beneficiar todas as partes interessadas no sector dos serviços financeiros e além.

Fontes:

Ethereum; Merkling em Ethereum

Trend Micro; o que Hackers faz com sua identidade roubada?

Javelin Strategy & Research; *O estudo de fraude de identidade de 2017*

Symantec; *Relatório de ameaças de segurança na Internet*

Risco com base em segurança; *Dados de 2016 romper tendências - ano em revista*

Thales; *2017 Thales dados ameaça relatório – edição de serviços financeiros*

Apache.org; Apache Struts 2 documentação - S2-052

Joseph Poon e Vitalik Buterin; Plasma: Scalable autónomos contratos inteligentes