© 2017

Sumário Executivo

Executive Summary

blockchain Of Things

BCOT Global Holdings

Resumo

A Internet das Coisas (IoT) não é segura e planejamos corrigir este problema.

A Blockchain of Things, Inc. visa resolver o problema de segurança da IoT com o lançamento oficial da Catenis Enterprise, uma camada de serviços web fácil de usar codificada na blockchain do Bitcoin. Ao usar uma abordagem de camada de serviços da Web, a Catenis pode ser facilmente adaptada para suportar Ethereum, Hyperledger e muitas outras blockchains. A Catenis é uma rede ativa (em versão beta) com vários clientes corporativos ativos.

Neste artigo, primeiramente caracterizamos a natureza das ameaças de segurança da IoT e os principais obstáculos que elas representam para a adoção da IoT nas empresas. Em seguida, destacamos as vantagens de segurança da blockchain do Bitcoin quando comparadas às infraestruturas tradicionais da IoT. Em seguida, delineamos os obstáculos que impediram as organizações de usar a rede Bitcoin para uma comunicação segura do dispositivo IoT. Descrevemos como a Catenis Enterprise aborda esses obstáculos ao alavancar a segurança e a confiança da blockchain do Bitcoin. Finalmente, apresentaremos conceitos de verificação confiável e ativos inteligentes como atributos-chave que ampliam a funcionalidade do Catenis Enterprise para aplicativos que vão além do escopo tradicional da IoT.

Sumário executivo

A Internet das Coisas (IoT) não é segura e planejamos corrigir este problema.

A IoT não é segura: Uma pesquisa patrocinada pela Bain com mais de 500 compradores corporativos da IoT concluiu que a barreira n° 1 para acelerar a adoção industrial da IoT é uma segurança insuficiente[1]. As preocupações de segurança prejudicam o mercado tradicional de IoT em grande parte devido à atual dependência a servidores centralizados para a comunicação do dispositivo IoT. Mais especificamente, as vulnerabilidades da IoT podem ser agrupadas em três categorias:

- **Um ataque de negação de serviço (DoS):** Um ataque DoS pode perturbar indefinidamente os serviços habilitados para missão IoT.
- **Hacking:** Vários métodos de hackeamento, como a falsificação de dispositivos, os ataques homem no meio (man-in-the-middle) e os ataques de repetição (repay attacks) podem levar ao roubo de dados ou ao sequestro de dispositivos.
- **Insuficiência de auditoria:** A falta de uma pista de auditoria (audit trail) significa que os administradores de dispositivos podem ignorar uma intrusão por meses ou mesmo anos.

O **Bitcoin é seguro:** A blockchain do Bitcoin, a tecnologia mais antiga e mais experiente, resolve incondicionalmente esses problemas de segurança sem ter pontos centrais vulneráveis. A rede Bitcoin provou sua resistência a uma variedade de ataques de hackers e DoS, além de demonstrar suas capacidades de auditoria, tendo em vista a irreversibilidade dos registros do livro-razão. Como tal, é possível que um administrador ative e se comunique de forma segura com um dispositivo IoT, ligando-o a um endereço Bitcoin e usando a blockchain do Bitcoin para enviar mensagens (por exemplo, sinais de comando e controle) para esse endereço.

Catenis supera as limitações da IoT do Bitcoin: Apesar dessas vantagens de segurança, a blockchain do Bitcoin sofre de muitas limitações que impediram seu uso para a IoT. A Catenis Enterprise supera esses obstáculos, e faz isso de uma maneira que retém as vantagens de segurança do Bitcoin. Isso é possível uma vez que a Catenis é uma camada de serviços web codificada na blockchain do Bitcoin. Para aplicações industriais da IoT, as limitações da blockchain do Bitcoin e as características principais correspondentes da Catenis podem ser agrupadas em seis categorias:

- **Limite de tamanho de 80 bytes:** O campo de mensagem do Bitcoin é limitado em apenas 80 bytes, e não oferece a capacidade de enviar grandes cargas úteis de dados significativos entre dispositivos IoT. A Catenis resolve esse problema eliminando o limite de tamanho para que as mensagens possam incluir códigos de programação ou arquivos de dados de qualquer tipo ou tamanho.

- **Falta de autorização de acesso:** Se um dispositivo IoT estiver conectado a um endereço Bitcoin público, atores não autorizados podem ativar o dispositivo, já que o endereço está conectado para aceitar mensagens de qualquer pessoa. A Catenis resolve esta questão através da criação de uma rede autorizada codificada na blockchain aberta do Bitcoin.
- **Insuficiência de criptografia:** As mensagens enviadas através da blockchain do Bitcoin são visíveis para o mundo, uma vez que não são criptografadas. A Catenis resolve esse problema fornecendo criptografia de ponta a ponta. Os recursos de segurança não param por aí, uma vez que a Catenis também utiliza automaticamente um novo endereço Bitcoin atribuído ao dispositivo IoT sempre que o sistema envia uma mensagem para esse dispositivo. Como tal, todas as mensagens enviadas para os endereços Bitcoin utilizados anteriormente não terão impacto no dispositivo em questão. Isso garante completamente a Segurança Futura Perfeita (Perfect Forward Secrecy) [2], à medida que as mensagens viajam através de túneis temporários que existem apenas por um momento. Também impede que atores não autorizados conduzam análises para descobrir mensagens relacionadas.
- **Desafios de velocidade e escala:** O tempo de confirmação em Bitcoin é grande e a lockchain sofre de desafios de escala bem conhecidos. A Catenis resolve o problema trabalhando como uma segunda camada para a Rede Lightning[3], que permite a transferência de transações rápidas e escaláveis. No entanto, ao contrário da Rede Lightning, podemos trabalhar sem "risco de contraparte", uma vez que a Catenis é uma rede autorizada.
- **Difícil de usar para o CTO:** A blockchain do Bitcoin é difícil de usar, já que a maioria das equipes de TI não conhece os protocolos da blockchain. A Catenis resolve esse problema criando uma camada de serviços web e uma API fácil de usar pelos clientes.
- **Difícil de gerenciar para o CFO:** A blockchain do Bitcoin pode ser difícil de gerenciar para alguns CFO, uma vez que muitos não têm experiência no gerenciamento de criptografia. A Catenis resolve esses desafios implementando secretamente a transação de criptomoedas, mas, como resultado, remove a criptomoeda do ponto de vista do cliente corporativo.

Catenis facilita prova de autenticidade: O conjunto de recursos aprimorados da Catenis permite que aplicativos que ultrapassem o escopo tradicional da IoT incluam um sistema para atestado verdadeiro (prova de autenticidade a.k.a.). Com a Catenis, pode-se acompanhar a autenticidade dos produtos do mundo real para mitigar a fraude do produto de varejo e cadeia de suprimentos, um problema estimado em US$ 1,9 trilhão por ano.[4] Existem dois passos importantes para o processo de certificação:

- **Confirmar se o fabricante do produto possui um certificado de autenticidade:** Um fabricante pode registrar a impressão digital criptográfica de um certificado de autenticidade para a blockchain e fornecer ao revendedor/cliente uma identificação de referência que permita a confirmação criptográfica

independente de que o fabricante do produto possui o terminal que registrou o certificado de autenticidade.

- **Confirmar se o certificado de autenticidade é genuíno:** A Catenis pode exibir verificação de identidade criptográfica independente. O proprietário de um determinado terminal do dispositivo Catenis pode provar sua identidade, demonstrando o acesso ou a propriedade do domínio apropriado do site, registro do governo ou certificação de terceiros. A combinação dessas duas etapas possibilita a autenticidade na ausência de confiança, o que reduz a possibilidade de fraude, tanto para os fornecedores como para a rede de varejo.

Catenis habilita ativos customizáveis: A Catenis amplia ainda mais suas capacidades além do alcance tradicional da Internet das Coisas, ao capacitar os clientes a digitalizar mais coisas. Esse objetivo é alcançado ao capacitar os clientes a criar ativos inteligentes e transferi-los de um usuário para outro. Os recursos inteligentes da Catenis possuem toda a funcionalidade robusta e as capacidades de contratos inteligentes do Colored Coin Protocol[5], mas são ainda mais poderosos em quatro formas principais:

- **Opção de fornecer uma carga digital útil:** Os recursos inteligentes da Catenis, juntamente com suas funções de entrega de mensagens, nos permitem transmitir uma carga digital útil que contrastam com muitos outros projetos criptográficos em que um recurso digital é simplesmente uma referência à carga, apoiado pela promessa de um terceiro para transferi-lo sob demanda por meio de um sistema externo. Um recurso inteligente da Catenis pode ser configurado para transmitir o certificado de estoque real, escritura de imóvel ou arquivo MP3 para que a carga útil possa ser transferida de um usuário para outro.
- **Opção para criptografar a carga útil digital:** A carga útil digital que é transferida pelos recursos inteligentes da Catenis pode ser criptografada com a chave pública do terminal de destino para que apenas o terminal de destino possa acessá-la. Isso contrasta com os projetos criptográficos em que a carga útil não é criptografada e fica visível para o mundo.
- **Opção de reagir às mensagens:** Os recursos inteligentes da Catenis podem ser configurados para reagir a mensagens de outros terminais, o que contrasta com projetos criptográficos nos quais o recurso digital não responde. Por exemplo, um cliente da Catenis pode programar a criação e distribuição automáticas de ativos inteligentes condicionados ao recebimento de uma mensagem. Isso permite que a Catenis seja uma plataforma para a distribuição eficiente e transparente de qualquer recurso digital, incluindo, mas não limitado a vendas de token.
- **Rede com direito de acesso:** Como a Catenis é uma rede autorizada, os ativos inteligentes não reagirão às mensagens de terminais não autorizados. Isso contrasta com os projetos de criptografia que não possuem capacidades de autorização de acesso.

A **Catenis é uma plataforma para aplicativos de terceiros:** A Catenis é basicamente uma plataforma na qual os desenvolvedores de terceiros podem criar seus aplicativos usando a funcionalidade básica da Catenis (por exemplo, mensagens seguras, ativos inteligentes, etc.) como blocos de construção. Destacamos quatro das muitas categorias em que um terceiro programador poderia focar esforços em desenvolvimento futuros:

- **Aplicativos específicos da indústria para proteger a IoT:** Diferentes indústrias e diferentes partes de uma operação preferem alavancar a funcionalidade IoT segura da Catenis para diferentes casos de uso. Como tal, um terceiro desenvolvedor poderia criar um aplicativo específico do setor que aproveitasse a segurança da Catenis para trazer soluções personalizadas a diferentes segmentos do mercado de IoT.
- **Hardware como um serviço:** A Catenis permite o uso de hardware com base na tecnologia de bloqueio como serviço, uma vez que as chaves digitais sob a forma de um recurso inteligente podem incluir a funcionalidade de equipamentos remotos conectados aos terminais da Catenis. Um desenvolvedor de terceiros poderia criar aplicativos específicos do setor que aproveitassem essa funcionalidade de maneiras diferentes para diferentes indústrias.
- **Mercado de ingressos:** A Catenis permitirá que o emissor original de um ativo inteligente ganhe uma comissão em revenda desse ativo (isto é, ativos inteligentes baseados em taxas). Por exemplo, os emissores de bilhetes de concertos podem ganhar comissões se seus ingressos forem revendidos em um mercado secundário. Um terceiro desenvolvedor poderia comercializar essa funcionalidade criando um mercado de tickets com reconhecimento de ativos inteligentes que aproveita a camada da Catenis.
- **Mercado de ações:** A lei do estado de Delaware permite que as corporações dos EUA troquem ações em uma blockchain para agilizar o processo de liquidação de ações. A Catenis já possui a funcionalidade para codificar ativos inteligentes que podem transferir o certificado de estoque real. A Catenis também possui a funcionalidade de abstrair criptomoedas para que os investidores de capital próprio tradicionais possam comprar ações em empresas a partir da corretora regular sem ter que lidar diretamente com a criptomoeda. Um terceiro desenvolvedor poderia desenvolver um mercado de ações que agilizasse o processo de liquidação de ações.

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

2 Scott Helme May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

3 Joseph Poon, Thaddeus Dryja: “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf

4 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

5 Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki