A tecnologia *blockchain* vai perturbar o mundo dos sistemas de controle industrial (ICS)?

Blockchain poderia ter aplicação em sistemas de controle industrial

Por Steve Mustard, PE, Eur. Ing., CAP, and Mark Davison, MIET

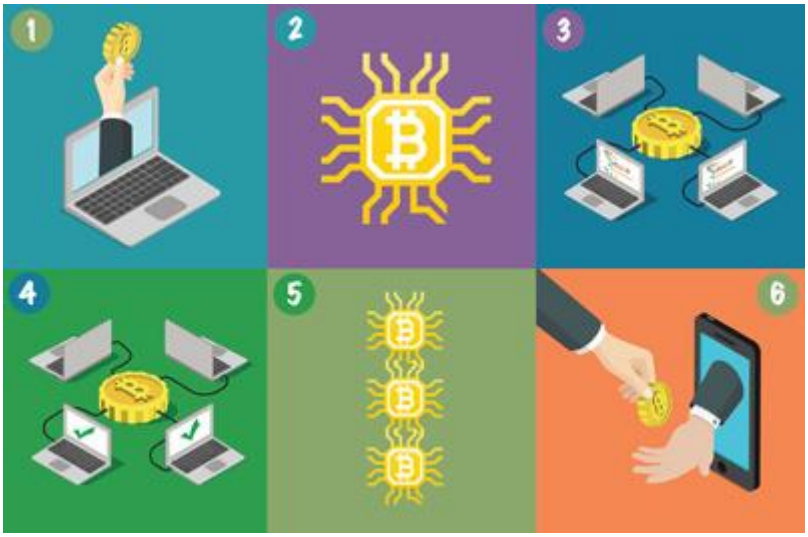
Blockchain é uma tecnologia inovadora que os principais lideres da indústria preveem que causará grandes distúrbios em muitas indústrias existentes, incluindo bancos, imobiliárias, cadeias de suprimentos e gerenciamento de energia. As grandes empresas americanas como a IBM, a Samsung, a UBS e a Barclays, já estão trabalhando em projetos e serviços relacionados a blockchain, e centenas de start-ups estão desenvolvendo seus próprios aplicativos de risco. A tecnologia Blockchain também pode perturbar o mundo dos sistemas de controle industrial (ICS), por isso vale a pena olhar agora, para ver o que pode vir e como isso pode nos afetar.

A tecnologia Blockchain

A tecnologia Blockchain é um método descentralizado para registrar transações. Essas transações são registradas em um ledger (registro) distribuído (conhecido como o blockchain) que é armazenado em milhares de computadores em todo o mundo.

As transações são registradas no ledger agrupadas em blocos. Eles são protegidos usando uma forma de criptografia chamada "hashing". Como o ledger é distribuído e seguro usando hashing, é teoricamente impossível fazer alterações uma vez que algo é gravado.

Hashing converte os dados em um bloco em um hash, um formato que não pode ser descriptografado para obter os dados originais. Ele é único, de modo que qualquer alteração nos dados originais produza um resultado diferente. Os blocos em uma cadeia de blocos incorporam o hash do bloco anterior e, portanto, manipular ou forjar transações, alterando dados em um bloco, é facilmente identificado e impedido.



1. Alguém quer enviar dinheiro para outra pessoa.
2. Um bloco é criado online para representar a transação.
3. O novo bloco é transmitido para todos os mineiros de blockchain na rede.
4. Os mineiros aprovam a transação e a validam.
5. O bloco é então adicionado ao blockchain, fornecendo um registro permanente. Neste ponto, a transação é válida. Todos os mineiros recebem uma cópia do blockchain atualizado, tornando evidente rapidamente qualquer discrepância.
6. O solicitante recebe o pagamento.

Onde o blockchain é usado?

O uso mais conhecido da tecnologia blockchain está na Bitcoin, uma moeda criptografada que permite aos usuários enviar e receber dinheiro eletronicamente. A Bitcoin usa a tecnologia blockchain para manter um registro de cada transação Bitcoin. Um número crescente de grandes empresas usa o Bitcoin, incluindo Microsoft, Subway e Whole Foods, bem como muitos pequenos restaurantes e comerciantes. O valor total de todos os Bitcoins existentes agora ultrapassa os US $ 20 bilhões (acima de US $ 2,7 bilhões em 2015), e milhões de dólares são trocados diariamente.

Novos Bitcoins são gerados através de um processo chamado de mineração. Este processo envolve indivíduos chamados mineiros, que usam software especial para "minerar" blocos, ou criam o hash necessário para atualizar o blockchain. Os mineiros recebem um certo número de Bitcoins em troca desse processamento. A mineração requer um poder de processamento significativo para executar o hash para se adequar às regras rigorosas conhecidas como prova de trabalho. O processamento complexo necessário para obter a prova de trabalho ajuda a gerenciar a taxa em que os Bitcoins são emitidos.

Os algoritmos Hashing produzem uma saída de tamanho fixo (chamado de código hash ou digest), independentemente dos dados serem hashed (ocultos). O Bitcoin usa um algoritmo de hash seguro (SHA) com 256 bits (32 bytes) em sua saída, ou SHA-256 para mensagens de valor máximo equivalente a 264 bits. Por exemplo, o SHA-256 hash de "Sociedade Internacional de Automação" (35 caracteres) é:

75b8e883214c8543f22fcf1adb6682666f5308fcb
9dcc896846b2d53fba2141e

E o SHA-256 hash para "Automation Federation" (21 caracteres) é:

8da363f674c49fa3f5b4bbdfac92610d0906ad
e2d58f38a39c8ee8faa74bad91

O primeiro bloco no registro Bitcoin (chamado de bloco genesis) tem o hash:

000000000019d6689c085ae165831e934f
f763ae46a2a6c172b3f1b60a8ce26f

No processo de prova de trabalho, o mineiro é colocado na presença de uma série de dados, incluindo:

- o hash SHA-256 que representa o bloco anterior na cadeia;

- detalhes das transações atuais a serem processadas, como um carimbo de data / hora (criado pelo mineiro);

- informações pertinentes às transações propriamente ditas.

O mineiro combina todos esses dados em um hash. Isso é referido como o desafio. A tarefa do mineiro é produzir o que é conhecido como uma prova, de modo que o hash SHA-256 do desafio e prova resulte em um hash que tenha um número fixo de zeros iniciais (do total de 256 bits no hash).

Devido à natureza unidirecional única dos algoritmos de hash, a única maneira pela qual o mineiro pode determinar a prova (também conhecida como "nonce", um termo comumente usado em criptografia para um número que é usado apenas uma vez) é tentar todas as permutações possíveis até a resposta ser encontrada. O número de zeros iniciais no hash determina o número de permutações possíveis. Por exemplo, se fosse necessário ter os primeiros 40 bits do hash como zero, haveria aproximadamente 1 trilhão de combinações possíveis (2^{40}). Variando o número de zeros divide ou duplica a quantidade de trabalho (2^{39} = 549 bilhões, 2^{41} = 2,2 trilhões).

Em Bitcoin, a prova de trabalho é projetada para levar aproximadamente 10 minutos para executar. No presente, isso resulta em um hash com 18 zeros dianteiros, ou 262.144 possíveis permutações (2^{18}). Uma vez que um mineiro determina a prova, o hash resultante é armazenado no bloco de transação, e esse hash será posteriormente usado no processamento do próximo bloco.

Os motivos pelos quais a tecnologia blockchain pode gerenciar com sucesso US $ 20 bilhões de moeda também são razões pelas quais ele pode ser útil em outros aplicativos de gerenciamento de transações:

- Devido à sua natureza descentralizada, a tecnologia blockchain não possui um ponto central de falha e é mais capaz de suportar ataques maliciosos.

- Mudanças nos blockchain públicos são publicamente visíveis por todas as partes, criando transparência e as transações não podem ser alteradas ou excluídas.

O Bitcoin talvez ganhou mais notoriedade do que o respeito do público em geral até a data porque os hackers o usaram para cobrar suas taxas de resgate sobre ataques. As transações Bitcoin envolvem transferências entre endereços anônimos e a falta de controle central torna difícil, mas não impossível, rastrear. No entanto, a tecnologia blockchain pode ser uma força para o bem.

Já disruptiva

A tecnologia Blockchain já está sendo usada em uma grande variedade de indústrias. Mais de US$ 500 milhões foram investidos em blockchain em empresas em capital de risco em 2016. Algumas aplicações de alto perfil incluem:

- A indústria do diamante para rastrear diamantes individuais indo direto da mina para o consumidor. Isso aborda falsificação, perda de receita, fraude de seguros e detecção de conflitos de diamantes.

- A indústria médica para manter um backup do DNA de uma pessoa que pode ser acessado prontamente e de forma segura para aplicações médicas.

- No varejo para registrar todas as ações que acontecem em uma cadeia de fornecimento de varejo e disponibilizar todos os dados pesquisáveis em tempo real para os consumidores. Isso permite ao consumidor escanear um código QR em uma lata no supermercado e descobrir onde o alimento interno foi obtido, quem o certificou, onde estava enlatado, etc.

- Prova para bloquear um vídeo ou fotografia, por isso sendo impossível mudar um pixel sem registro da transação, permitindo usos como gravação de reivindicações incontestáveis de segurança ou brutalidade policial.

- Gerenciamento de energia para permitir aos clientes comprar e vender energia diretamente, sem passar por um provedor central.

Caseiramente, a IBM está trabalhando em parceria com a Samsung para desenvolver uma "Internet of Things" (IoT) descentralizada. A telemetria autônoma descentralizada peer-to-peer (ADEPT) usa a tecnologia blockchain para garantir transações entre dispositivos. A IBM e a Samsung estão planejando redes de dispositivos que podem se manter de forma autônoma através da transmissão de transações entre pares, em oposição ao modelo atual de todos os dispositivos que se comunicam apenas com serviços centralizados ou em nuvem.

Central para este conceito é o registro de dispositivos IoT em uma cadeia de blocos mantida publicamente, criando um nível de confiança que não pode ser alcançado para dispositivos desonestos.

Blockchain no mundo ICS

A tecnologia Blockchain possui outras aplicações potenciais para ICS, como a proteção e verificação de firmware do dispositivo e atualizações de software de aplicativos. À medida que os usuários do ICS asseguraram suas redes, os atacantes partiram para outros métodos para infiltrar sistemas. Um desses métodos envolve a inserção de malware Trojan no software ICS, que é baixado pelos usuários para instalação em suas redes. Em 2014, uma variante do malware Havex continha código que escaneava redes para dispositivos compatíveis com OPC. Ele então coletou informações sobre a configuração da tag e enviou-a para um servidor externo. Este Trojan foi encontrado em software para download em sites de fornecedores ICS. O registro de firmware e software em uma cadeia de blocos poderia fornecer um registro imutável de código, tornando impossível um ataque como o exemplo do Havex OPC. Outros potenciais aplicativos baseados em ICS são:

- Autenticação, autorização e não modificação da configuração do dispositivo e das alterações do programa.

- Proteção, verificação e não modificação de dados críticos, como dados de historiadores ou relatórios oficiais.

Desafios

Um dos desafios para as soluções de Blockchain não-Bitcoin é que o benefício chave de um registro verdadeiramente distribuído só é possível se houver algum ganho financeiro óbvio para os mineiros. Os exemplos acima, como o firmware do ICS ou o registro do software, só podem ser alcançáveis com um fornecedor privado (por exemplo, executado por um fornecedor de ICS apenas para seus produtos) ou um consórcio blockchain (talvez gerenciado por um coletivo de fornecedores de ICS).

Nesta aplicação, ainda pode haver algumas preocupações sobre a segurança dos registros, mas, no caso do firmware ICS e da verificação de software, um consórcio blockchain ou privado ainda proporcionaria muito mais segurança do que os métodos existentes.

Tal como acontece com todas as tecnologias disruptivas, é impossível prever com certeza o que acontecerá. Tudo o que podemos fazer é assistir ao andamento. O que é certo é que a tecnologia blockchain não está indo embora em breve.

Sobre os Autores

Steve Mustard, PE, Eur. Ing., CEng, CAP, GICSP, FIET, é um consultor de automação industrial com ampla experiência técnica e de gerenciamento em vários setores. Especialista amplamente reconhecido em cybersecurity industrial e membro do comitê de Normas de Segurança do ISA99. Mustard participa ativamente de grupos de trabalho de segurança cibernética formados pela Automation Federation.

Mark Davidson, MIET é um engenheiro de software com mais de 30 anos de experiência. Atualmente é proprietário / diretor da Terzo Digital, uma empresa de consultoria de software especializada em IoT e telemetria. Davison é um membro atual do comitê para a Water Industry Telemetry Standards (WITS) Protocol Standards Association, ajudando a desenvolver novos padrões na arena do IoT, visando mais do que apenas a Water Industry.
