Material SENAI Blockchain

# **Módulo 1**

Neste módulo, você conheceu o conceito da tecnologia Blockchain, sua estrutura e funcionamento.

Você viu que cada transação (criptomoedas, contratos, compra e venda) é realizada diretamente entre as partes (peer-to-peer), validada por todos nós (nodes) e incluída na Blockchain pelos mineradores (miners), formando uma cadeia de blocos com informações criptografadas (hash) que ficam registradas e armazenadas em toda a rede, funcionando como uma “livro-caixa digital” (ledger), tornando-se um histórico para a próxima vez que houver negociação.

Essa estrutura de compartilhamento de informações criptografadas por meio de uma rede de dados distribuída permite mais segurança nas transações, uma vez que não há um controle central. Como todos os usuários integram o processo e são responsáveis pela autenticidade das informações, a Blockchain torna-se uma rede protegida contra fraudes que ocorrem em ambientes digitais. Por isso, tem despertado o interesse de governos, bancos e empresas.

No próximo módulo, você vai conhecer mais detalhes sobre o trabalho de mineração para inclusão de novos blocos na cadeia.

Avance para continuar seus estudos.

# **FLUXO DA INFORMAÇÃO NA BLOCKCHAIN**

## **01 - Solicitação**

Você solicita a compra daquele imóvel (ou uma transação com criptomoedas, contratos, bens etc.)

## **02 - Transmissão Rede Distribuída**

A solicitação é transmitida para nós chamados mineradores, os quais irão buscar validá-la e incluí-la na Blockchain.

## **03 - Mineração de Dados**

Os nós “mineram os dados” da transação para verificar se as suas informações, do imóvel e do vendedor estão corretas, a fim de validar a negociação.

Competição

Como essas informações são protegidas por chaves criptográficas, os mineradores competem para decodificá-las e disponibilizá-las na rede primeiro.

Super computadores

Para isso, é necessário investir em computadores com alto poder de processamento de cálculos, com rapidez e eficiência.

Recompensa

O trabalho da mineração é remunerado com criptomoedas.

## **04 - Solução**

O primeiro computador que resolver o cálculo, disponibiliza o bloco de informações com a solução na rede, para os demais nós checarem se a solução é válida.

Alguns nós da rede possuem o histórico ou cópia completa de todas as transações da Blockchain.

Eles são chamados fullnodes (ou nós completos).

Os demais nós se conectam aos fullnodes para obter as informações necessárias para que as transações sejam processadas.

## **05 - Validação**

Após validado pela maioria da rede, o novo bloco de dados é adicionado à cadeia de blocos, de modo permanente e inalterável.

Cada novo bloco contém 2 códigos chamados hash: um que traz informações referentes ao bloco anterior e outro que representa a sua identificação, que será utilizada pelo próximo bloco.

Os hashes trazem segurança às informações, pois sempre que uma solução é encontrada e validada, confirma, ao mesmo tempo, o novo bloco e todos os anteriores.

Quanto mais antigo for o bloco, mais seguro ele será, pois teve mais validações.

É muito difícil fraudar a rede Blockchain e adulterar um bloco de informações. Para isso, seria necessário que um hacker adulterasse as cópias de todos os blocos em toda a rede, para que o bloco falso fosse validado pela maioria dos nós.

## **06 - Conclusão**

A transação é concluída. O imóvel passa a ser seu.

Este bloco de informações fica registrado e armazenado na rede Blockchain, funcionando como um “livro-razão digital”, tornando-se um histórico para a próxima negociação.

# **COMO GERAR AS CHAVES**

A criptografia assimétrica é baseada em duas chaves: a chave privada e a chave pública. Imagine que você deseja transmitir um arquivo em uma rede, e busca garantir que apenas o destinatário possa ler seu conteúdo. Para isso, você pode fazer uso da chave pública desse destinatário para cifrar o documento, criptografando-o. Somente com a chave privada (que fica em posse do destinatário) será possível decifrar o texto. Observe a imagem abaixo:

A geração dessas chaves se dá a partir de números aleatórios, normalmente números primos. Podemos resumir esse processo como segue, simulando o algoritmo RSA, um dos mais aplicados:

Escolha dois números primos distintos, p e q;

Calcule n 𝑛=𝑝∙𝑞

Calcule z 𝑧=(𝑝−1)∙(𝑞−1)

Obtenha um número 𝑒 (𝑒 :𝑛ú𝑚𝑒𝑟𝑜 𝑝𝑟𝑖𝑚𝑜 𝑞𝑢𝑎𝑙𝑞𝑢𝑒𝑟, então, escolha um número)

Calcule 𝑒∙𝑑(𝑚𝑜𝑑 𝑧)=1

O par (e,n) é a chave pública, e o par (d,n) é a chave privada.

Acompanhe um exemplo prático:

Suponha dois números primos: p = 29 e q = 37

Resolvendo:

Adotando: 𝑒=71

Então, agora podemos montar o par de chaves:

Chave pública = (e,n) = (71,1073)

Chave privada = (d,n) = (1079,1073)

# **COMPONENTES DO BLOCO**



## **MÓDULO 2**

Neste módulo, você conheceu mais detalhes sobre como novos blocos são validados e adicionados na Blockchain.

Você viu que o trabalho de mineração é essencial para esse processo, pois o minerador que primeiro resolver o desafio (encontrar uma hash válida, composta por número de bloco, hash anterior, marcação de tempo, dados e nonce que transcreve os dados da transação), transmite a prova de seu trabalho (proof of work) para os demais nós mineradores validarem a solução encontrada. Somente após o consenso de 51% da rede, a transação é validada e o bloco incluído na cadeia.

Além disso, você viu que o trabalho de mineração requer alto investimento em energia e equipamentos com alto poder de processamento. Todos esses elementos (desafio, prova de trabalho, consenso, alto custo computacional) visam inviabilizar a alteração indevida de blocos e garantir mais segurança nas transações.

# **FUNCIONAMENTO DA BLOCKCHAIN**

## **Transações**

Quando uma transação é solicitada, os mineradores a recebem e competem para resolver a equação.

## **Mineradores**

Cada minerador terá um grupo de transações pendentes a serem incluídas. Eles selecionam o bloco e tentam resolver o desafio.

## **Bloco Candidato**

Para resolver o desafio, os mineradores realizam uma prova de trabalho. O desafio consiste em incrementar o valor de NONCE do bloco, até que a hash do bloco apresente um determinado número de zeros iniciais. Conforme a Blockchain aumenta, o número de zeros aumenta, aumentando, assim, a dificuldade.

## **Mineração**

O minerador que consegue resolver o desafio transmite a solução (prova de trabalho) para a rede, a fim de que os demais mineradores a validem.

## **Prova de trabalho concluída, Validação e Consenso**

Os demais mineradores verificam a prova de trabalho, validando ou não o bloco.

O processo se reinicia. As transações remanescentes entram em uma nova rodada de competição pelo novo bloco. Isso se faz dessa maneira porque a prova de trabalho foi criada para que o processo de mineração fique em torno de um bloco a cada 10 minutos.

Os mineradores vão buscar formar um novo bloco sempre que houver transações pendentes. Logo, a busca por um novo bloco se inicia quando transações são submetidas à rede.

O processo da transação, desde a sua solicitação até sua validação (identificação das partes envolvidas, análise das chaves públicas, dentre outros fatores) dura em torno de 10 minutos.

A transação requer que um bloco seja criado e, para isso, o minerador deverá resolver um enigma através da prova de trabalho (proof of work). Através da prova de trabalho é que se garante a validade da transação.

Uma vez recebidas, tais transações são inseridas através da estrutura de dados da merkle tree e armazenadas no bloco que será minerado para ser inserido na rede Blockchain. Tal bloco é denominado bloco candidato.

**NONCE**

No link http://www.blockchain-basics.com/HashPuzzle.html, você encontra um simulador para compreender o conceito de NONCE.

No campo Data, insira o texto: BlockChain – SENAI-SP

Em restrições, altere os Leading Zeros para 2 – dificuldade

Clique em Solve Hash Puzzle

Veja a quantidade de Nonce (tentativas) para criar a hash.

# **MÓDULO 3**

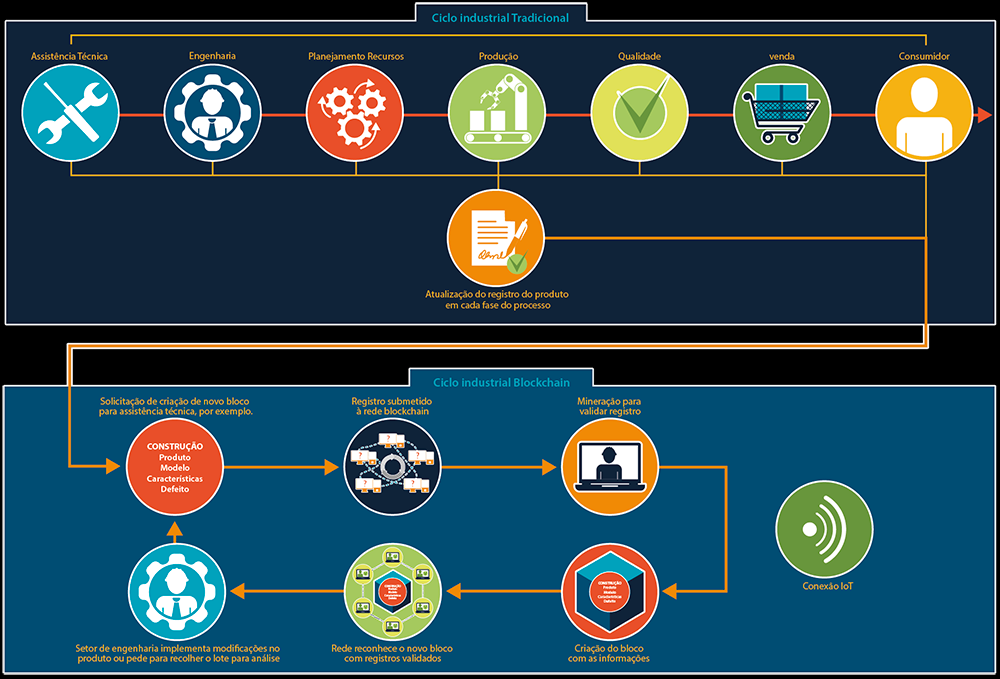
Neste módulo, você conheceu como a tecnologia Blockchain pode ser aplicada na formalização de contratos inteligentes para qualquer tipo de transação, na criação de um sistema unificado para identificação de pessoas, nos registros e atualizações de informações sobre qualquer negociação envolvendo imóveis, bem como nos processos da indústria.

Você viu que a rede distribuída de dados, por não haver a intervenção de terceiros (instituições privada e/ou públicas), traz autonomia, facilidade, rapidez, economia e transparência às transações. Por isso, tem atraído o interesse de várias áreas e segmentos, como jurídica, logística, governamental, energia, alimentícia, varejista, saúde, segurança e educação.

Além disso, em decorrência do crescimento e implantação da tecnologia Blockchain em diversos setores e do desenvolvimento da indústria 4.0, novas possibilidades profissionais têm surgido na área da Tecnologia da Informação.

**RASTREABILIDADE NA INDÚSTRIA**





**BLOCKCHAIN NA INDÚSTRIA**



**REFERÊNCIAS**

CROSBY, Michael et al. Blockchain technology: Beyond bitcoin. Applied Innovation, v. 2, p. 6-10, 2016.

EXAME.ABRIL. Entenda o que é bitcoin. Disponível em: https://exame.abril.com.br/mercados/entenda-o-que-e-bitcoin/. Acesso em: 02 ago. 2018.

FINANCEONE. O que é criptomoeda, para que serve e como investir. Disponível em: https://financeone.com.br/o-que-e-criptomoeda-e-como-investir/. Acesso em: 01 ago. 2018.

GLOBO.COM. Entenda o que é blockchain, a tecnologia por trás do bitcoin. Disponível em: https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml. Acesso em: 01 ago. 2018.

INFOMONEY. que o Bitcoin e o mercado de imóveis têm em comum?. Disponível em: https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/4153780/que-bitcoin-mercado-imoveis-tem-comum. Acesso em: 03 ago. 2018.

INSTITUTO DE REGISTRO IMOBILIáRIO DO BRASIL. Blockchain e o Futuro do Registro de Imóveis Eletrônico – Palestra I. Disponível em: http://www.irib.org.br/noticias/detalhes/blockchain-e-o-futuro-do-registro-de-imoveis-eletronico-undefined-palestra-i. Acesso em: 04 ago. 2018.

JUS. Blockchain e os Cartórios. Disponível em: https://jus.com.br/artigos/58855/blockchain-e-os-cartorios. Acesso em: 02 ago. 2018.

OFICINA DA NET. O que é P2P e como ela funciona?. Disponível em: https://www.oficinadanet.com.br/post/14046-o-que-e-p2p-e-como-ela-funciona. Acesso em: 02 ago. 2018.

SLATER, W. F. Introduction to Blockchain and Blockchain development. Forensecure 2018. Disponível em: http://billslater.com/forensecure/blockchain\_2018\_slater.pdf. Acesso em: 26 ago. 2018.

TECMUNDO. Tecmundo explica: como funcionam as bitcoins?. Disponível em: https://www.youtube.com/watch?v=T38mpPBBqv8. Acesso em: 02 ago. 2018.

TECHTUDO. O que é blockchain?. Disponível em: https://www.techtudo.com.br/noticias/2017/11/o-que-e-blockchain.ghtml. Acesso em: 03 ago. 2018.

YAGA, Dylan et al. Blockchain technology overview. Draft NISTIR, v. 8202, 2018. Disponível em: http://img1.wsimg.com/blobby/go/60231649-12ce-4835-96f0-945ea7f2116c/downloads/1cb8a20ea\_182905.pdf. Acesso em: 26 ago. 2018.