## Ferramentas de Produtividade Informática aplicada a WEB

# Blockchain

# C:\Users\Tehio\Desktop\download.jpg& Criptomoeda

### Brian Luca Dias da Cunha 33º

### 10º 1C



Índice

[Como o blockchain funciona? 7](#_Toc11099553)

[Blocos 7](#_Toc11099554)

[Mineiros 7](#_Toc11099555)

[Vantagens do blockchain 9](#_Toc11099557)

[Aplicações do blockchain 10](#_Toc11099558)

[Serviços financeiros 10](#_Toc11099559)

[Transparência pública 10](#_Toc11099560)

[Gestão de identidade 10](#_Toc11099561)

[Propriedade intelectual 10](#_Toc11099562)

[Base de conhecimento 11](#_Toc11099563)

[Contratos inteligentes (smart contracts) 11](#_Toc11099564)

[Finalizando 11](#_Toc11099565)

[Webgrafia 13](#_Toc11099566)

[Glossário 14](#_Toc11099567)

Introdução

Em 2009, um sistema de criptomoeda ou moeda virtual chamado Bitcoin foi lançado e, desde então, vem representando uma grande revolução nos meios de pagamentos digitais. O principal ingrediente do êxito do Bitcoin é um sistema de registro que ficou um bom tempo sem ser notado: o **blockchain**.

Então o que é blockchain?

O blockchain é um banco de dados e o que o faz tão importante é o fato de esse não ser um banco de dados convencional: o seu sistema funciona como um livro de registros, mas inviolável, "inderrubável" e extremamente eficiente.

O blockchain também pode ser usado em outros sistemas, dos mais diversos tipos: financeiros, comerciais, governamentais, eleitorais e por aí vai. Não é por menos que bancos, seguradoras, corretoras de ações, empresas de segurança, governos e tantas outras instituições estão sendo atraídas pelo assunto.

Mas como o blockchain funciona?

Por que o blockchain tem tantas vantagens?

Por qual razão o blockchain é tão revolucionário?

Antes de entrar no universo do blockchain, vale a pena entender o que é **Bitcoin**. Assim fica mais fácil compreender a importância e o funcionamento do blockchain.

Pois bem, o Bitcoin surgiu oficialmente no começo de 2009 em 3 de janeiro, para ser exato. Meses antes, em 2008, um artigo em PDF assinado por Satoshi Nakamoto foi divulgado em grupos de discussões descrevendo o conceito do Bitcoin.

"Satoshi Nakamoto" é um pseudônimo que representa uma pessoa ou um grupo, que até hoje não ficou claro quem realmente é.

Enfim o que a gente precisa entender aqui é que o Bitcoin é uma moeda totalmente digital, de alcance global e que não é controlada por governos ou instituições. Não há banco central, casa da moeda ou fundos monetários privados, enfim, não há nenhuma entidade por trás da plataforma do Bitcoin.

Estamos falando de uma moeda de um sistema, com modo de operação distribuído sem um elemento central e autorregulado. Tudo se baseia em transações digitais criptografadas, razão pela qual o Bitcoin é considerado um tipo de criptomoeda.

E quanto vale um Bitcoin? Olha, depende da demanda da oferta e da via de regra, quanto mais transações existirem em dado momento, mais caro um Bitcoin será. No momento em que fiz a pesquisa um único Bitcoin custava entorno de EU: 3.133,68. Os preços podem variar muito de uma hora para outra.

E como obter?

Há, basicamente, três formas:

- Você pode ir em um mercado on-line de Bitcoins (há vários), que funciona como uma espécie de casa de câmbio, só que digital. Você pode comprar Bitcoin com dólares, euros, reais, etc.;

- Você pode receber Bitcoins como forma de pagamento por alguma venda ou serviço prestado;

- Você pode "minerar Bitcoins", ou seja, recorrer a um sistema que usa a capacidade de processamento de um ou mais computadores para resolver problemas matemáticos complexos para ser recompensado com Bitcoins. Porém, não é fácil ganhar Bitcoins dessa forma.

Os Bitcoins podem ser usados para transações da mesma forma como se usa o "dinheiro de verdade", inclusive podendo utilizar frações da moeda. Os Bitcoins devem ficar guardados em uma carteira Bitcoin chamada de wallets, que é um sistema que permite que você faça transações e controle seus ganhos.

Há vários tipos de carteiras. Cada uma está associada a uma chave criptográfica privada e uma chave pública para que você pode realizar as operações. Aliás, é graças ao sistema de criptografia que o Bitcoin não pode ser falsificado ou fraudado: qualquer alteração, por menor que seja, invalida as chaves.

Mas como uma moeda digital pode ter e gerar valor se não há nenhum tipo de comando central?

Acontece que o Bitcoin é uma rede Peer-to-Peer (P2P), ou seja, ponto a ponto, o que significa que as transações são gerenciadas por cada um dos usuários que fazem parte do sistema.

Quando você realiza transações com Bitcoin, o computador ou tele móvel que você utiliza passa a participar da rede por meio da sua carteira Bitcoin. Se um nó sai dessa rede, os demais continuam mantendo o sistema funcionando. Se houvesse um controle central, bastaria que este fosse derrubado para o sistema cair para todo mundo.

Não havendo um sistema centralizado, como a distribuição dos Bitcoins é feita? E como as transações são realizadas e validadas?

É aqui que entra em cena a figura do blockchain, um registro público que reúne todas as informações necessárias para o processamento e a proteção das transações.

Imagine que você faz parte de um grupo de 100 pessoas que, por conta de um bizarro acidente de avião, vai parar em uma ilha que não aparece no mapa. Vocês estão incomunicáveis com o resto do mundo e não existe nenhum meio de transporte para tirá-los dali. Vocês vão ficar ali por muito tempo, provavelmente, por isso, decidem montar uma sociedade nessa ilha.

Mas vocês sabem, por experiência própria que uma sociedade precisa de líderes. Mas uma estrutura de governo gera disputas de poder que podem se transformar em conflitos sérios. Por isso, vocês decidem elaborar um modelo de sociedade diferente: tudo o que acontece ali precisa ter aprovação de todo o grupo, de forma que o que é verdade para um terá que ser verdade para os outros.

E como isso é feito?

A partir de um livro de registros que alguém trazia no avião. Essa mesma pessoa explicou que esse livro é mágico: é possível criar infinitas cópias deles, mas tudo o que for registrado nele será automaticamente registrado nos demais.

Assim, as cópias serão iguais para sempre. Devido a essa característica, vocês decidem criar uma cópia do livro para cada pessoa.  Como esse livro também não pode ser apagado e nem adulterado, ele se torna parte essencial de um sistema que distribui de maneira justa e eficiente os recursos na ilha. Tudo o que é registrado no livro é válido para todo mundo, pois os registros aparecem em todas as unidades.

E então esse livro foi chamado de blockchain.

Ok voltando ao "mundo real". Entenda a tal sociedade na ilha como a plataforma do Bitcoin, e o livro mágico como, o blockchain. A diferença é que o blockchain é um sofisticado sistema computacional.

Como estamos falando de um sistema de banco de dados distribuído e sem intermediários, precisamos de um mecanismo confiável para permitir transações diretas ponto a ponto. Esse é papel do blockchain.

O blockchain é um sistema de registro que contém todas as transações processadas no sistema. Traduzindo o nome significa *cadeia de blocos*. E uma cadeia de blocos é um conjunto de informações registradas que é ligada a blocos de informações anteriores e sucessores.

Esses blocos de informações também são públicos e todos os participantes da rede têm acesso. Porém, quando processados, os blocos não podem ser apagados ou alterados. Além disso, novos registros só podem ser feitos diante um processo de validação.

Esse sistema, por ser distribuído, está em milhares de computadores. Quando uma atualização legítima é feita, todos as cópias são sincronizadas em questão de segundos. Pode até ser que um ou outro computador desapareça da rede, mas isso não afetará o sistema, pois todos os outros nós ainda estão lá.

Para certificar uma informação em uma cadeia de blocos e evitar fraudes, o blockchain conta com um mecanismo chamado *prova de trabalho*. Trata-se de um protocolo criptográfico que valida uma transação em um dispositivo por meio da resolução de um problema matemático.

Adulterações nas cadeias de blocos, por menores que sejam, gerarão resultados diferentes do esperado para esse problema matemático. Isso impede o processamento da transação e, consequentemente, o seu registro.

Como o blockchain funciona?

Esse esquema de cadeia de blocos com estrutura distribuída é o que torna o Bitcoin tão confiável. Parar entendermos melhor como o blockchain funciona, convém olharmos um pouco os elementos que formam o sistema, começando pelos blocos.

Blocos

os *blocos* contêm os registros em si. Todas as transações confirmadas devem ser registradas neles. Novas transações geram novos registros que, como tal, devem ser inseridos em novos blocos.

No Bitcoin, por padrão, a cada dez minutos um bloco é fechado contendo toda as transações nesse período. Mas esse intervalo de tempo pode ser diferente em outros momentos e em outros sistemas que utilizam blockchain.

Além do conjunto de transações, um bloco precisa ter um código que o liga ao bloco anterior, além de um código próprio que serve para conectá-lo ao bloco seguinte.

Mas como gerar esses blocos de modo seguro, sem que as conexões sejam alteradas para direcionar para um bloco ilegítimo, por exemplo?

Aqui, a principal arma do sistema é a figura do mineiro ou minerador.

Mineiros

Pois bem, os problemas complexos que os *mineiros* têm que resolver dizem respeito à criação de novos blocos e, com efeito, à validação das transações.

Um mineiro nada mais é do que um computador ou um conjunto de máquinas atuando como uma que utiliza um software específico para a realização dos cálculos. Sempre que o processo é concluído, o mineiro é recompensado nesse caso, com Bitcoins.

Funciona assim: o software analisa todas as informações referentes ao bloco e aplica uma fórmula matemática específica sobre esse conjunto de dados. O resultado do cálculo feito com essa fórmula é um código chamado *hash*. Normalmente, esse código usa base hexadecimal.

Cada conjunto de dados é único, portanto, toda vez que essa fórmula matemática for aplicada no bloco, o código hash gerado será o mesmo. Mas, se o conjunto de dados sofrer alguma modificação, por menor que ela seja, o código hash será totalmente diferente. Aí não dá para ir adiante.

Além do seu próprio hash, o bloco contém o hash do bloco anterior. Dessa forma, um processo de verificação conseguirá perceber quando um bloco não é legítimo, pois o código hash deste será diferente dos registrados.

Nós

O Bitcoin é uma rede e cada integrante da rede é um *nó*. Assim, se você tem um computador com um software para realizar transações com Bitcoins, essa máquina acaba sendo um nó.

Esse software mantém e ajuda a distribuir cópias atualizadas em tempo real da cadeia de blocos em uso. Cada vez que transações são realizadas blocos são adicionados e todos os nós são comunicados para que possam atualizar os registros com as novas informações.

O mecanismo de comunicação criptografada impede que essa rede seja invadida ou que os nós sejam adicionados inadequadamente.

Então levando em conta que os nós participam da validação das transações. Uma série de procedimentos é aplicada para verificar se há consenso sobre a realização de determinada transação. Assim, se você está recebendo Bitcoins de alguém como forma de pagamento, um processo de verificação junto aos nós confirmará a operação.

Essa transação será então registrada no blockchain. Como esse registro supostamente não pode ser apagado, ninguém consegue tomar esses Bitcoins de você fazendo alterações nos blocos.

Vantagens do blockchain

Podemos começar com a segurança.

A estrutura em forma de cadeias de blocos torna o blockchain praticamente inviolável. Para conseguir adulterar algo, o invasor teria que controlar mais da metade dos nós para realizar mudanças por consenso.

No universo do Bitcoin, pelo menos, esse controle massivo dos nós exigiria um poder computacional extremamente grande e a alteração de um registro exigiria a reescrita de praticamente toda a base de dados. O que é inviável, para não dizer impossível.

A disponibilidade é outra grande vantagem. A estrutura distribuída faz o sistema continuar funcionando mesmo que um ou vários nós caiam. Quando os nós faltantes voltam à rede, eles são imediatamente atualizados.

Um ponto muito importante também é a confiabilidade. Como os dados no blockchain não podem ser apagados ou alterados, temos a certeza de que as transações registradas ali são legítimas e íntegras.

Outro aspecto é a transparência. As transações são públicas, o que significa que todos os nós podem checá-las. Os mecanismos de criptografia fazem com que os usuários do sistema não precisem ser identificados, no entanto, é perfeitamente possível vincular identidades, se necessário, esse aspecto ajuda a assegurar que somente usuários legítimos estejam participando da transação.

Os custos operacionais também podem ser mais baixos na comparação com sistemas computacionais centralizados. Esse aspecto varia conforme a aplicação, mas, de modo geral, o modelo distribuído implica em compartilhamento de recursos de processamento e armazenamento.

Aplicações do blockchain exemplos

Já sabemos que o blockchain é parte fundamental do Bitcoin, mas também já sabemos que o conceito pode ser empregado em outras aplicações. Ok, mas quais? Vamos a alguns exemplos.

Serviços financeiros

Há um número crescente de bancos e financeiras se interessando pelo blockchain. O setor já percebeu, por exemplo, que a tecnologia pode ser usada para transações de pagamento e transferências de dinheiro. Pelo menos no âmbito internacional, transações desse tipo podem levar várias horas para serem concluídas. O blockchain pode tornar o processo mais rápido e, simultaneamente, prover mais segurança.

Transparência pública

Como os dados não podem ser apagados, tampouco adulterados, sistemas governamentais podem utilizar o blockchain para combater desvio de recursos públicos, facilitar processo de auditorias e evitar fraudes em eleições, por exemplo.

Gestão de identidade

O registro de usuários ou clientes em um sistema de blockchain pode combater falsificação de identidades, o que seria útil, por exemplo, para fechamento de contratos eletrônicos ou transferência de propriedade.

Propriedade intelectual

O uso do blockchain também vem sendo considerado para gestão de patentes e direitos autorais. Com a associação de uma obra a uma pessoa, o sistema poderia, por exemplo, ajudar uma empresa a conferir se determinado indivíduo é mesmo autor do conteúdo que ele está oferecendo.

Base de conhecimento

Como o blockchain é, basicamente, um banco de dados distribuído, é possível também o uso da tecnologia para distribuição de documentação de sistemas, manuais de uso, artigos acadêmicos, livros digitais e afins.  Na verdade, o blockchain pode ser usado para compartilhamento de praticamente qualquer tipo de informação.

Contratos inteligentes (smart contracts)

O blockchain tem se mostrado particularmente relevante para um tipo de aplicação que está ganhando força, que são os *contratos inteligentes*. Nessa modalidade, um software elabora contratos com termos e condições específicas conforme as circunstâncias.

Por exemplo, em uma loja virtual que recorre a diferentes serviços de entrega para atender a clientes de todo o país. Para um cliente mais próximo, o sistema pode considerar a distância menor para elaborar um contrato com prazo de entrega curto. Para clientes que estão mais longe, esse mesmo sistema pode incluir no contrato prazo mais longo e a cobrança de um eventual imposto local, tudo automaticamente.

O blockchain pode ajudar esse tipo de software a fazer verificações e registrar operações que, entre outros benefícios, evitarão que a empresa cometa deslizes em uma ou mais cláusulas e sofra prejuízos por conta disso

Finalizando

As aplicações mencionadas são só exemplos. Há uma gama enorme de possibilidades que o blockchain pode proporcionar para usuários individuais, empresas de todos os portes, governos e outras instituições.

O assunto é relativamente novo, por isso, as ideias em torno do conceito estão apenas começando a surgir. Mas, a proposta da cadeia de blocos tem enorme potencial e pode beneficiar os mais diferentes ramos de atividade.

É verdade que as características do blockchain podem ser desvantajosas para determinadas aplicações, por exemplo, serviços que, em respeito às leis de privacidade, precisam permitir que os usuários apaguem seus dados a imutabilidade da cadeia de blocos é uma barreira para essa necessidade.

Além disso, em um sistema privado como por exemplo a rede interna de uma empresa, todos os nós podem ser controlados de uma vez só porque a administração dessas máquinas costuma ser centralizada. Se não houver um meio eficiente de proteção, um invasor poderá assumir o controle dos nós para modificar permanentemente o blockchain.

As vantagens e desvantagens do blockchain precisam ser avaliadas em cada caso.

Antes de encerrar queria deixar uma curiosidade aqui se você pesquisar mais sobre o assunto, talvez chegue ao endereço *blockchain.info*. Esse site não é a mesma coisa que blockchain, mas sim um serviço para acompanhamento do mercado de Bitcoins.

## Webgrafia

<https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml>;

<https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/>;

<https://www.ibm.com/blockchain/what-is-blockchain>;

<https://pt.wikipedia.org/wiki/Blockchain>;

<https://www.sap.com/brazil/products/leonardo/blockchain/what-is-blockchain.html>;

<https://foxbit.com.br/o-que-e-blockchain/>;

<https://computerworld.com.br/2016/06/22/blockchain-o-que-e-e-como-funciona/>.

## Glossário

## Bitcoin: um sistema de criptomoeda ou moeda virtual.

## ***Blockchain:*** O blockchain é um banco de dados.

## *Inderrubável:* Algo que não pode ser derrubado

## Peer-to-Peer:é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede que funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

## *Hash:* é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo.