**INTRODUÇÃO**

A blockchain (também conhecido como “o protocolo da confiança”) é uma tecnologia de [registro distribuído](https://pt.wikipedia.org/wiki/Registro_distribu%C3%ADdo) que visa a descentralização como medida de segurança. São bases de registros e dados distribuídos e compartilhados que têm a função de criar um índice global para todas as transações que ocorrem em um determinado mercado. Funciona como um [livro-razão](https://pt.wikipedia.org/wiki/Raz%C3%A3o_(contabilidade)), só que de forma pública, compartilhada e universal, que cria consenso e confiança na comunicação direta entre duas partes, ou seja, sem o intermédio de terceiros.

**DEFINIÇÃO**

Blockchain é um tipo de Base de Dados Distribuída que guarda um registro de [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) permanente e à prova de violação. A [base de dados](https://pt.wikipedia.org/wiki/Base_de_dados) blockchain consiste em dois tipos de registros: [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) individuais e blocos.

Um bloco é a parte atual da blockchain onde são registrados algumas ou todas as [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) mais recentes e uma vez concluído é guardado na blockchain como [base de dados](https://pt.wikipedia.org/wiki/Banco_de_dados) permanente. Toda vez que um bloco é concluído um novo é gerado. Existe um número incontável de blocos na blockchain que são linkados uns aos outros - como uma cadeia - onde cada bloco contém uma referência para o bloco anterior.

**HISTÓRIA**

A blockchain foi primeiramente definida no [código fonte](https://pt.wikipedia.org/wiki/C%C3%B3digo-fonte) original do [bitcoin](https://pt.wikipedia.org/wiki/Bitcoin" \o "Bitcoin). Portanto, estão intimamente ligados no que diz respeito ao surgimento de ambos.

A definição original foi criada em 2008 com a publicação do artigo "Bitcoin: A Peer-to-Peer Electronic Cash System" publicado por [Satoshi Nakamoto](https://pt.wikipedia.org/wiki/Satoshi_Nakamoto" \o "Satoshi Nakamoto) (cuja real identidade permanece em aberto apesar de haver algumas especulações e pronunciamentos a respeito). Em 2009 o código foi lançado como código aberto.

Assim, em 2009 começa a rede do [bitcoin](https://pt.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) quando Satoshi Nakamoto [minerou](https://pt.wikipedia.org/wiki/Minera%C3%A7%C3%A3o_de_Bitcoin) os primeiros [bitcoins](https://pt.wikipedia.org/wiki/Bitcoin" \o "Bitcoin). Satoshi Nakamoto desaparece então em 2011 do público - isto é, dos fóruns, artigos e contribuições de código acerca do [bitcoin](https://pt.wikipedia.org/wiki/Bitcoin" \o "Bitcoin). Mas mesmo com a ausência de Satoshi Nakamoto, o [bitcoin](https://pt.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) continuou a ser desenvolvido e mercantilizado, com o esforço da comunidade em geral trabalhando para resolver diversos problemas no código - incluindo, por exemplo, uma bifurcação na rede que originou o Bitcoin Cash.

Sendo a base tecnológica das [criptomoedas](https://pt.wikipedia.org/wiki/Criptomoeda" \o "Criptomoeda), a blockchain tem recebido o interesse de bancos, empresas e organizações governamentais. Desde então, modificações tem sido feitas a partir da versão original e novas aplicações tem sido atreladas à blockchain.

Em 2014, surge o termo "Blockchain 2.0" usado para descrever um novo projeto no campo de [banco de dados distribuído](https://pt.wikipedia.org/wiki/Banco_de_dados_distribu%C3%ADdos) da blockchain.

Em 2015, o jornal [*The Economist*](http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable) descreveu uma das implementações da segunda geração da blockchain, o [Ethereum](https://pt.wikipedia.org/wiki/Ethereum" \o "Ethereum), como "uma linguagem de programação que permite usuários escreverem contratos inteligentes mais sofisticados [...]". Tal sacada permitiria a formação de "organizações autônomas descentralizadas" ([DAO](https://pt.wikipedia.org/wiki/The_DAO_(organiza%C3%A7%C3%A3o))), companhias virtuais baseadas apenas em um conjunto de regras provenientes desta nova geração da blockchain.

Em 2016, foi previsto o montante de 1 bilhão de dólares em investimento em tecnologia ligada à blockchain, pelo mercado financeiro, segundo pesquisa do jornal [*CCN*](https://www.cryptocoinsnews.com/blockchain-news/).

A evolução da blockchain tornou possível também o surgimento de conceitos distribuídos de blockchain, tal como a [sidechain](https://pt.wikipedia.org/wiki/Sidechain" \o "Sidechain), que permitiria uma maior diversidade de blockchains sem comprometer a comunicação entre elas. Este é um conceito importante já que prepararia a rede para uma iminente tendência de diversificação já que diferentes empresas têm trabalhado na implementação de sua própria blockchain

**REDE PEER-TO-PEER**

De um modo geral e simples, uma rede [P2P](https://pt.wikipedia.org/wiki/Peer-to-peer) é uma [arquitetura de computadores](https://pt.wikipedia.org/wiki/Arquitetura_de_computadores) ou redes que compartilha tarefas, trabalho, ou arquivos entre pares (peers). Pares são parceiros na rede com iguais privilégios e influência no ambiente. Em uma rede [P2P](https://pt.wikipedia.org/wiki/Peer-to-peer) cada computador ou usuário é chamado de nó e coletivamente eles compõem uma rede [P2P](https://pt.wikipedia.org/wiki/Peer-to-peer) de nós.

A rede [P2P](https://pt.wikipedia.org/wiki/Peer-to-peer) na blockchain consiste de uma série de computadores e servidores onde cada um atua como um nó na rede. Quando uma nova mensagem entra na rede, a informação nesta mensagem é propagada entre todos os nós da rede [P2P](https://pt.wikipedia.org/wiki/Peer-to-peer). A informação é normalmente encriptada e privada e não há como rastrear quem adicionou a informação na rede apenas verificar sua validade.

**VANTAGENS**

Eliminação de troca por intermediário e falta de confiança:

Duas partes são capazes de fazer uma troca sem a supervisão ou intermediação de uma terceira parte, reduzindo fortemente ou até eliminando o risco de contraparte.

Empoderamento dos usuários:

Usuários estão no controle de todas as suas informações e [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados).

Alta qualidade de dados:

Os dados da blockchain são completos, consistentes, datados, precisos e amplamente disponíveis.

Durabilidade, confiabilidade e longevidade:

Devido as redes serem descentralizadas, a blockchain não tem um ponto central de falha e é mais resistente a ataques maliciosos.

Integridade de processo:

Usuários podem confiar que suas [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) serão executadas exatamente como o protocolo determina, removendo a necessidade de uma terceira parte.

Transparência e imutabilidade:

Mudanças na blockchain são visíveis publicamente por todas as partes, criando transparência, e todas as [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) são imutáveis, isto é, elas não podem ser alteradas ou deletadas.

Simplificação de ecossistema:

Com todas a [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) sendo adicionadas a um único [livro-razão](https://pt.wikipedia.org/wiki/Raz%C3%A3o_(contabilidade)) público, isso reduz a desordem e complicações geradas por múltiplos [livros-razões](https://pt.wikipedia.org/wiki/Raz%C3%A3o_(contabilidade)).

Transações mais rápidas:

[Transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) interbancárias podem potencialmente levar dias para serem compensadas e terem acordo final, especialmente fora do horário de trabalho. [Transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) com blockchain podem reduzir o tempo de [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados) para minutos e são processadas 24 horas por dia e 7 dias por semana.

Menor custo por transação:

Eliminando o intermédio de terceiros e despesas gerais para troca de bens, blockchains têm o potencial de reduzir significativamente taxas de [transações](https://pt.wikipedia.org/wiki/Transa%C3%A7%C3%A3o_em_base_de_dados).

Digital:

Praticamente qualquer documento ou bem pode ser expressado em forma de código e encapsulado ou referenciado por uma entrada do [livro-razão](https://pt.wikipedia.org/wiki/Raz%C3%A3o_(contabilidade)), o que significa que a tecnologia blockchain tem aplicações muito amplas, a maioria ainda não pensada, muito menos implementada.

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

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