**Capítulo 1: Blockchain 101**

**Parte 1**

É muito provável que, se você está lendo este livro, já tenha ouvido falar sobre blockchain e tenha alguma apreciação fundamental de seu enorme potencial. Caso contrário, deixe-me dizer que esta é uma tecnologia que promete alterar positivamente os paradigmas existentes de quase todas as indústrias — incluindo, mas não se limitando aos setores de TI, finanças, governo, mídia, medicina e direito — tornando-os mais eficientes, confiáveis e transparentes.

Este capítulo introduz a tecnologia blockchain, seus fundamentos técnicos, a teoria por trás dela e várias tecnologias que contribuíram para a construção do que hoje é conhecido como blockchain. As fundações teóricas dos sistemas distribuídos são descritas primeiro. Em seguida, são apresentados os precursores do Bitcoin. Por fim, a tecnologia blockchain é introduzida. Essa abordagem é uma forma lógica de compreender a tecnologia blockchain, pois suas raízes estão em sistemas distribuídos e criptografia. Cobriremos muitos tópicos rapidamente aqui, mas não se preocupe — veremos grande parte desse material em muito mais detalhe ao longo do livro.

Neste capítulo, focaremos em:

* O crescimento da tecnologia blockchain
* Sistemas distribuídos
* A história do blockchain
* Introdução ao blockchain
* Tipos de blockchain

**O crescimento da tecnologia blockchain**

Com a invenção do Bitcoin em 2008, o mundo foi apresentado a um novo conceito que revolucionou toda a sociedade. Era algo que prometia impactar todas as indústrias. Esse novo conceito era o blockchain, a tecnologia subjacente que sustenta o Bitcoin.

Alguns descrevem o blockchain como uma revolução, enquanto outra corrente de pensamento acredita que será mais uma evolução e levará muitos anos até que quaisquer benefícios práticos do blockchain se concretizem. Esse pensamento está correto em certa medida, mas, na minha opinião, a revolução já começou.

**Progresso rumo à maturidade**

Por volta de 2013, surgiram algumas ideias sobre o uso da tecnologia blockchain para outras aplicações além de apenas criptomoedas. Em 2014, começaram algumas pesquisas e experimentações, o que levou a provas de conceito, pesquisas adicionais e projetos-piloto em escala total entre 2015 e 2017. Em 2015, o Ethereum foi lançado como o primeiro blockchain programável com contratos inteligentes, o que abriu muitas possibilidades. O interesse por blockchains de nível empresarial surgiu por volta da mesma época. Nesse período, também vimos vários projetos como Everledger, Quorum e Corda.

Além disso, o desenvolvimento de arquiteturas monolíticas e multichain evoluiu rapidamente após 2018. Alguns exemplos importantes de protocolos inovadores incluem Solana, Avalanche e Polkadot, que discutiremos mais adiante neste livro.

Atualmente, no segundo trimestre de 2023, as finanças descentralizadas (DeFi), os tokens não fungíveis (NFTs) e a tokenização em geral são aplicações muito populares do blockchain. Elas já estão em uso convencional por milhões de usuários em todo o mundo que utilizam serviços DeFi. Espera-se que, em cerca de três anos, o DeFi se estabilize como uma tecnologia madura e amplamente adotada. Com toda a atividade e adoção no DeFi e no comércio de NFTs, podemos dizer que, em certa medida, o blockchain já faz parte de nossas vidas diárias. Claro que uma maturidade adicional ainda é necessária, especialmente do ponto de vista regulatório e de segurança, mas milhões de usuários já usam o blockchain regularmente, seja para fazer pagamentos, negociar NFTs, obter empréstimos ou jogar.

Essa tendência só tende a crescer e, durante 2022 em diante, mais e mais pesquisas e desenvolvimentos estão sendo realizados. Haverá mais foco na regulamentação e padronização da tecnologia blockchain. Inúmeros projetos já estão prontos para produção, e mais adoção é esperada nos próximos anos.

A pesquisa sobre escalabilidade dos blockchains — em que os blockchains possam lidar com muitas transações como as redes financeiras tradicionais — levou ao desenvolvimento de arquiteturas de camada 2 e de múltiplas cadeias. O avanço na viabilização prática de provas de conhecimento zero ajudou enormemente na realização de soluções de camada 2. Essas soluções estão sob intenso desenvolvimento e pesquisa atualmente, e muitos mecanismos já foram introduzidos, como Plasma, rollups, sidechains, Lightning Network e outros.

Veja o seguinte artigo para detalhes sobre quais plataformas estão sendo utilizadas por esses milhões de usuários:  
<https://beincrypto.com/ethereum-defi-users-reach-new-highs-over-4m-growing-roughly-8x-in-a-year/>

O progresso na tecnologia blockchain quase dá a sensação do boom das ponto-com na internet no final da década de 1990.

**Interesse crescente**

O interesse pela tecnologia blockchain aumentou significativamente nos últimos anos. Antes descartada por alguns apenas como “dinheiro de nerds” sob a ótica das criptomoedas, ou como algo que simplesmente não valia a pena perseguir, a blockchain agora está sendo pesquisada pelas maiores empresas e organizações do mundo. Milhões de dólares estão sendo gastos para adotar e experimentar essa tecnologia.

Além disso, o interesse acadêmico pela blockchain é impressionante, e muitas instituições de ensino — incluindo universidades prestigiadas ao redor do mundo — estão conduzindo pesquisa e desenvolvimento em tecnologia blockchain. Não apenas cursos educacionais estão sendo oferecidos por muitas instituições, como também os acadêmicos estão realizando pesquisas de alta qualidade e produzindo artigos científicos perspicazes sobre o tema. Há também vários grupos de pesquisa e conferências ao redor do mundo que se concentram especificamente em pesquisa de blockchain. Essa comunidade de pesquisa é benéfica para o crescimento de todo o ecossistema blockchain. Uma simples busca online por “grupos de pesquisa sobre blockchain” revelaria centenas, senão milhares, desses grupos.

Muitas startups já estão fornecendo soluções baseadas em blockchain. Uma simples busca por tendências no Google revela a imensa escala de interesse na tecnologia blockchain nos últimos anos. Tópicos em alta incluem organizações autônomas descentralizadas (DAOs), entidades totalmente autônomas e transparentes, governadas por membros, desenvolvidas com contratos inteligentes e sem autoridade central. Enquanto isso, NFTs — por meio dos quais arte digital é rotineiramente comprada e vendida por milhões de dólares — e Metaversos vêm ganhando destaque nas notícias.

Também existem diversos consórcios, como o Enterprise Ethereum Alliance (EEA) em <https://entethalliance.org> e o Hyperledger em <https://www.hyperledger.org>, que foram estabelecidos para a pesquisa, desenvolvimento e padronização da tecnologia blockchain. Além disso, o Instituto de Engenheiros Elétricos e Eletrônicos (IEEE) e a Organização Internacional para Padronização (ISO) também começaram suas tentativas de padronizar vários aspectos da tecnologia blockchain.

**Metaverso**

Um Metaverso é um ambiente tridimensional simulado por computador. Uma convergência da nossa vida digital com o mundo real, ele fornece um mundo virtual para os usuários realizarem atividades como interações sociais, engajamento em negócios e compras. Esse mundo virtual é geralmente acessado por meio de hardware especializado chamado headsets de realidade virtual (VR), que aprimoram a experiência do mundo virtual.

Esse não é um conceito novo; na era da Web 2.0 (a internet comum que usamos diariamente), Second Life, World of Warcraft e várias outras plataformas semelhantes ganharam destaque, como entidades centralmente controladas por acionistas. Na era da Web 3.0 (pós-blockchain), Decentraland e The Sandbox, entre muitos outros, estão se tornando populares, com base em fundamentos descentralizados e governança comunitária.

**Sistemas distribuídos**

Compreender sistemas distribuídos é essencial para compreendermos o blockchain, pois o blockchain é, em sua essência, um sistema distribuído. Ele é um livro-razão distribuído que pode ser centralizado ou descentralizado. Originalmente, o blockchain foi concebido para ser — e geralmente é usado como — uma plataforma descentralizada. Pode-se pensar nele como um sistema que possui propriedades tanto dos paradigmas descentralizados quanto distribuídos. É um sistema descentralizado-distribuído.

Um sistema distribuído é um paradigma computacional no qual dois ou mais nós trabalham entre si de forma coordenada para alcançar um resultado comum. Ele é modelado de tal maneira que os usuários finais o percebem como uma única plataforma lógica. Por exemplo, o mecanismo de busca do Google é baseado em um grande sistema distribuído; no entanto, para o usuário, parece uma única plataforma coerente. Ele é composto de processos (nós) e canais (canais de comunicação), onde os nós se comunicam passando mensagens. Um blockchain é um sistema distribuído baseado na troca de mensagens.

Um **nó** é um participante individual (um computador) em um sistema distribuído. Todos os nós podem enviar e receber mensagens uns dos outros. Os nós podem ser honestos, defeituosos ou maliciosos, e possuem memória e processador. Um nó que apresenta comportamento arbitrário é conhecido como um **nó bizantino**, em referência ao problema dos generais bizantinos.

Esse tipo de comportamento inconsistente dos nós bizantinos pode ser intencionalmente malicioso, o que é prejudicial para a operação da rede. Qualquer comportamento inesperado de um nó na rede, seja malicioso ou não, pode ser categorizado como bizantino.

Um exemplo em pequena escala de um sistema distribuído é mostrado no diagrama a seguir. Esse sistema distribuído possui seis nós, dos quais um (N4) é um nó bizantino, levando à possível inconsistência de dados. L2 é um link que está quebrado ou lento, e isso pode levar a uma partição na rede:

**Figura 1.1: Projeto de um sistema distribuído: N4 é um nó bizantino e L2 é um link de rede quebrado ou lento**

**O Problema dos Generais Bizantinos**

Em 1982, um experimento mental foi proposto por Lamport et al. em seu artigo de pesquisa *The Byzantine Generals Problem*, disponível em:  
<https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/>

Nesse problema, um grupo de generais do exército bizantino, que lideram diferentes partes do exército, está planejando atacar ou recuar de uma cidade. A única forma de comunicação entre eles é por meio de mensageiros. Eles precisam concordar em atacar ao mesmo tempo para vencer. O problema é que um ou mais generais podem ser traidores que poderiam enviar mensagens enganosas. Além disso, o mensageiro pode ser capturado pela cidade, resultando na não entrega da mensagem. Portanto, é necessário um mecanismo viável que permita o acordo entre os generais, mesmo na presença de traidores e da perda de mensagens, de forma que o ataque possa ocorrer ao mesmo tempo.

Como uma analogia para sistemas distribuídos, os generais podem ser considerados como nós honestos, os traidores como nós bizantinos (ou seja, nós com comportamento arbitrário), o mensageiro como o canal de comunicação entre os generais, e um mensageiro capturado como uma mensagem atrasada ou perdida. Diversas soluções foram apresentadas para esse problema no artigo de Lamport et al. de 1982.

Dois desafios principais no projeto de sistemas distribuídos são a **coordenação entre os nós** e a **tolerância a falhas**. Mesmo que alguns (acima de um determinado limite ditado pelo protocolo de consenso) dos nós apresentem falhas ou os links de rede se quebrem, o sistema distribuído deve ser capaz de tolerar isso e continuar a funcionar para alcançar o resultado desejado. Esse problema tem sido uma área ativa de pesquisa no design de sistemas distribuídos por muitos anos, e diversos algoritmos e mecanismos foram propostos para superá-los.

Projetar sistemas distribuídos é um desafio. Foi provado que um sistema distribuído **não pode ter simultaneamente** as três propriedades desejadas de **consistência**, **disponibilidade** e **tolerância a partições**. Esse princípio é conhecido como **Teorema CAP**.

**Teorema CAP**

O Teorema CAP, também conhecido como Teorema de Brewer, foi introduzido por Eric Brewer em 1998 como uma conjectura. Em 2002, foi provado como um teorema por Seth Gilbert e Nancy Lynch. O teorema afirma que qualquer sistema distribuído **não pode ter simultaneamente** consistência, disponibilidade e tolerância a partições:

* **Consistência** é uma propriedade que garante que todos os nós em um sistema distribuído tenham uma única cópia atual e idêntica dos dados. A consistência é alcançada utilizando algoritmos de consenso para assegurar que todos os nós tenham a mesma cópia dos dados. Isso também é chamado de **replicação de máquina de estados** (*state machine replication*, SMR). O blockchain é um meio de alcançar a replicação de máquina de estados.
* **Disponibilidade** significa que os nós no sistema estão ativos, acessíveis e aceitando requisições, e respondendo com dados sem falhas sempre que necessário. Em outras palavras, os dados estão disponíveis em cada nó, e os nós estão respondendo a requisições.
* **Tolerância a partições** garante que, se um grupo de nós não puder se comunicar com outros nós devido a falhas de rede, o sistema distribuído continue a operar corretamente. Isso pode ocorrer por falhas de rede e de nós.

Um diagrama de Venn é comumente utilizado para visualizar o Teorema CAP, como mostrado abaixo:

**Figura 1.2: Teorema CAP**

O diagrama anterior mostra que **apenas duas propriedades por vez podem ser alcançadas**: ou AP, CA ou CP.

**Em resumo:**

* Se optarmos por **CP** (consistência e tolerância a partições), sacrificamos a disponibilidade.
* Se optarmos por **AP** (disponibilidade e tolerância a partições), sacrificamos a consistência.
* Se optarmos por **AC** (disponibilidade e consistência), sacrificamos a tolerância a partições.

Observe que **AC não existe de fato**. O Teorema CAP, na prática, significa que, no caso de uma partição de rede, um sistema distribuído será ou **disponível** ou **consistente**. Como as partições de rede não podem ser ignoradas, a escolha, quando elas ocorrem, é entre consistência ou disponibilidade.

Podemos explicar esse conceito com o seguinte exemplo:

Vamos imaginar que existe um sistema distribuído com dois nós. Agora, apliquemos as três propriedades do teorema a esse sistema distribuído mínimo, com apenas dois nós:

* **Consistência** é alcançada se ambos os nós tiverem o mesmo estado compartilhado; ou seja, possuem a mesma cópia atualizada dos dados.
* **Disponibilidade** é alcançada se ambos os nós estiverem ativos e operando, e respondendo com a cópia mais recente dos dados.
* **Tolerância a partições** é alcançada se, apesar de falhas ou atrasos de comunicação entre os nós, a rede (sistema distribuído) continuar a operar.

Agora, pense em um cenário onde ocorre uma partição e os nós não conseguem mais se comunicar entre si. Se novos dados forem atualizados nesse momento, eles só poderão ser atualizados em um dos nós. Se o nó aceitar a atualização, então apenas um nó da rede estará atualizado, e a consistência será perdida. Se o nó rejeitar a atualização, isso resultará na perda de disponibilidade. Isso significa que ou a disponibilidade ou a consistência será inatingível devido à partição da rede.

Isso é curioso, pois de alguma forma, o blockchain parece alcançar todas essas propriedades, **violando o teorema** (especialmente em sua implementação mais bem-sucedida, o Bitcoin) — ou será que não?

Nos blockchains, **a consistência é sacrificada em favor da disponibilidade e da tolerância a partições**. Nesse cenário, a **consistência (C)** no blockchain **não é alcançada simultaneamente** com a **tolerância a partições (P)** e a **disponibilidade (A)**, mas sim **ao longo do tempo**. Isso é chamado de **consistência eventual**, onde a consistência é obtida devido à validação por múltiplos nós ao longo do tempo. Pode haver um desacordo temporário entre os nós sobre o estado final, mas eventualmente chega-se a um consenso.

Por exemplo, no Bitcoin, são necessárias múltiplas confirmações de transações para alcançar um bom nível de confiança de que as transações não serão revertidas no futuro. Eventualmente, uma visão consistente do histórico de transações estará disponível em todos os nós. Múltiplas confirmações de uma transação ao longo do tempo proporcionam **consistência eventual** no Bitcoin.

Para esse fim, o processo de mineração foi introduzido no Bitcoin. **Mineração** é um processo que facilita a obtenção de consenso usando o algoritmo de **Prova de Trabalho (PoW)**. Em um nível mais alto, a mineração pode ser definida como o processo usado para adicionar novos blocos ao blockchain.

**Teorema PACELC**

Uma extensão do Teorema CAP chamada **PACELC** foi proposta pela primeira vez por Daniel J. Abadi, da Universidade de Yale. Ela afirma que, além das três propriedades propostas pelo CAP, também existem **compensações entre latência e consistência**. Em outras palavras, há compensações entre consistência e latência **mesmo quando não ocorrem partições de rede**.

Isso significa que mesmo sem partições, durante a operação normal, o sistema deve escolher entre consistência e latência. Por exemplo, alguns bancos de dados podem optar por sacrificar a consistência para alcançar uma menor latência, enquanto outros podem pagar o preço na disponibilidade e latência para obter maior consistência. Isso é verdade para sistemas replicados e oferece uma visão mais abrangente sobre as compensações de consistência em sistemas distribuídos.

O Teorema PACELC foi formalmente comprovado em um artigo disponível aqui:  
<https://dl.acm.org/doi/10.1145/3197406.3197420>

**A história do blockchain**

O blockchain foi introduzido com a invenção do Bitcoin em 2008. Sua implementação prática ocorreu então em 2009. O Bitcoin será explorado com grande profundidade no Capítulo 6, *Arquitetura do Bitcoin*. No entanto, é essencial mencioná-lo aqui, pois sem ele, a história do blockchain não estaria completa.

Agora, vamos olhar para a história inicial da computação e das redes de computadores e discutir como essas tecnologias evoluíram e contribuíram para o desenvolvimento do Bitcoin em 2008:

* **1976** – Diffie–Hellman trabalham no intercâmbio seguro de chaves criptográficas.
* **1978** – Invenção da criptografia de chave pública.
* **1979** – Invenção das Árvores de Merkle (hashes em estrutura de árvore) por Ralph C. Merkle.
* **Década de 1980** – Desenvolvimento do TCP/IP.
* **1980** – Protocolos para sistemas criptográficos de chave pública, Ralph C. Merkle.
* **1982** – Assinaturas cegas propostas por David Chaum.
* **1982** – O problema dos Generais Bizantinos.
* **1985** – Trabalhos em criptografia de curvas elípticas por Neal Koblitz e Victor Miller.
* **1991** – Haber e Stornetta trabalham na proteção contra adulteração de registros de data e hora de documentos. Isso pode ser considerado a ideia mais antiga de uma cadeia de blocos ou *hash chains*.
* **1992** – Cynthia Dwork e Moni Naor publicam *Pricing via Processing or Combatting Junk Mail*. Este é considerado o primeiro uso da Prova de Trabalho (PoW).
* **1993** – Haber, Bayer e Stornetta aprimoram o sistema de marcação de tempo com Árvores de Merkle.
* **1995** – O sistema Digicash de David Chaum (um sistema de dinheiro eletrônico anônimo) começa a ser utilizado em alguns bancos.
* **1998** – Bit Gold, um mecanismo para moeda digital descentralizada, inventado por Nick Szabo. Ele usava encadeamento de hashes e quóruns bizantinos.
* **1999** – Emergência do aplicativo de compartilhamento de arquivos Napster, usado principalmente para compartilhamento de música, uma rede P2P, mas centralizada com uso de servidores de indexação.
* **1999** – Desenvolvimento de um serviço seguro de marcação de tempo para o projeto belga TIMESEC.
* **2000** – Rede de compartilhamento de arquivos Gnutella, que introduziu descentralização.
* **2001** – Surgimento do BitTorrent e das Tabelas Hash Distribuídas (DHTs).
* **2002** – Hashcash por Adam Back.
* **2004** – Desenvolvimento do B-Money por Wei Dai usando Hashcash.
* **2004** – Hal Finney, invenção do sistema de PoW reutilizável.
* **2005** – Prevenção de ataques Sybil usando quebra-cabeças computacionais, por James Aspnes et al.
* **2009** – Bitcoin (primeiro blockchain).

Essas tecnologias contribuíram de alguma forma para o desenvolvimento do Bitcoin, mesmo que não diretamente; os trabalhos são relevantes para o problema que o Bitcoin resolveu.

**Bitcoin**

Todas as tentativas anteriores de criar uma moeda digital anônima e descentralizada tiveram sucesso até certo ponto, mas não conseguiram resolver o problema de prevenir o **gasto duplo** em um ambiente completamente sem confiança (trustless) ou sem permissão (permissionless). Esse problema foi finalmente resolvido pela blockchain do Bitcoin, que introduziu a criptomoeda Bitcoin.

O Bitcoin também resolve o problema da **replicação de máquina de estados** (*state machine replication* – SMR), introduzido em 1978 por Leslie Lamport e formalizado em 1980 por Fred Schneider. SMR é um esquema usado para implementar um serviço tolerante a falhas, replicando dados (estado) entre nós em um sistema distribuído. O Bitcoin resolve esse problema permitindo a replicação de blocos em todos os nós corretos e assegurando a consistência por meio de seu mecanismo de Prova de Trabalho (PoW). Aqui, o consenso é alcançado entre os nós (ou réplicas) repetidamente para adicionar novos blocos à blockchain.

**Dinheiro eletrônico**

O conceito de dinheiro eletrônico (e-cash), ou moeda digital, não é novo. Desde a década de 1980, existem protocolos de e-cash baseados em um modelo proposto por David Chaum.

Assim como compreender os conceitos de sistemas distribuídos é necessário para entender a tecnologia blockchain, a ideia de e-cash também é essencial para apreciar a primeira — e surpreendentemente bem-sucedida — aplicação da blockchain: o Bitcoin, e mais amplamente, as criptomoedas em geral. Para criar um sistema de e-cash eficaz, dois requisitos fundamentais precisam ser atendidos: **responsabilização** e **anonimato**.

A **responsabilização** é necessária para garantir que o dinheiro seja gasto apenas uma vez (resolvendo o problema do gasto duplo) e que possa ser gasto apenas por seu legítimo proprietário. O problema do gasto duplo surge quando o mesmo dinheiro é gasto duas vezes. Como é bastante fácil fazer cópias de dados digitais, isso se torna um grande problema nas moedas digitais, já que se pode fazer muitas cópias do mesmo dinheiro eletrônico. Gastar o mesmo dinheiro duas vezes é conhecido como o problema do **gasto duplo**.

O **anonimato** é necessário para proteger a privacidade dos usuários. Com dinheiro físico, é quase impossível rastrear um pagamento até o indivíduo que de fato pagou, o que fornece privacidade adequada, caso o consumidor deseje ocultar sua identidade. No mundo digital, entretanto, fornecer esse nível de privacidade é difícil devido à personalização inerente, mecanismos de rastreamento e registros de log em sistemas de pagamento digital como cartões de crédito. Isso é considerado um requisito para assegurar a segurança da rede financeira, mas também é frequentemente visto como uma violação da privacidade.

Isso ocorre porque os usuários finais não têm controle sobre com quem seus dados podem ser compartilhados, mesmo sem seu consentimento. No entanto, esse é um problema solucionável, e a criptografia é usada para tratar dessas questões. Especialmente em redes blockchain, a privacidade e o anonimato dos participantes são características altamente desejadas. David Chaum resolveu ambos os problemas durante seus trabalhos nos anos 1980 usando duas operações criptográficas: **assinaturas cegas** e **compartilhamento secreto**. Esses termos e conceitos relacionados serão discutidos em detalhes no Capítulo 4, *Criptografia Assimétrica*. Por ora, basta dizer que assinaturas cegas permitem a assinatura de um documento sem realmente vê-lo, e um esquema de compartilhamento secreto possibilita a detecção de gastos duplos.

Em 2009, surgiu a primeira implementação prática de um sistema de dinheiro eletrônico chamado **Bitcoin**. O termo **criptomoeda** surgiu posteriormente. Pela primeira vez, ele resolveu o problema do consenso distribuído em uma rede sem confiança. Usou a criptografia de chave pública com o mecanismo de Prova de Trabalho para fornecer um método seguro e descentralizado de emissão de moeda digital. A principal inovação é a ideia de uma **lista ordenada de blocos** composta por transações que são **criptograficamente protegidas** por meio do mecanismo de PoW para **prevenir o gasto duplo** em um ambiente sem confiança. Esse conceito será explicado em maior detalhe no Capítulo 6, *Arquitetura do Bitcoin*.

Observando todas as tecnologias mencionadas anteriormente e sua história, é fácil ver como conceitos de esquemas de dinheiro eletrônico e de sistemas distribuídos foram combinados para criar o Bitcoin e o que agora é conhecido como blockchain. Esse conceito também pode ser visualizado com a ajuda do seguinte diagrama:

**Figura 1.3: As diversas ideias que sustentaram a invenção do Bitcoin e do blockchain**

**Introduzindo o blockchain**

Em 2008, um artigo inovador, intitulado *Bitcoin: A Peer-to-Peer Electronic Cash System*, foi escrito sobre o tema do dinheiro eletrônico ponto a ponto sob o pseudônimo de **Satoshi Nakamoto**.

O artigo introduziu o termo **cadeia de blocos** (*chain of blocks*), que mais tarde evoluiu para “blockchain”, onde uma sequência cronologicamente ordenada de blocos contendo transações é produzida pelo protocolo. O artigo está disponível em:  
<https://bitcoin.org/bitcoin.pdf>

Existem algumas maneiras diferentes de se definir blockchain; as duas definições a seguir estão entre as mais amplamente aceitas:

* **Definição leiga**: Blockchain é um sistema de registro compartilhado, seguro e em constante crescimento, no qual cada usuário dos dados mantém uma cópia dos registros, que só pode ser atualizada se a maioria das partes envolvidas em uma transação concordar com a atualização.
* **Definição técnica**: Blockchain é um livro-razão distribuído ponto a ponto que é criptograficamente seguro, somente de acréscimo (*append-only*), imutável (extremamente difícil de alterar) e atualizável apenas por meio de consenso entre os pares.

Agora, vamos examinar esses termos com mais detalhe. Analisaremos os elementos da definição técnica um por um:

* **Ponto a ponto (peer-to-peer)**: O primeiro termo da definição técnica é **ponto a ponto**, ou **P2P**. Isso significa que não há um controlador central na rede, e todos os participantes (nós) se comunicam diretamente uns com os outros. Essa propriedade permite que transações sejam realizadas diretamente entre os pares, sem envolvimento de terceiros, como um banco.
* **Livro-razão distribuído**: Ao aprofundarmos a definição técnica, vemos que blockchain é um “livro-razão distribuído”, o que significa que um livro-razão é distribuído por toda a rede entre todos os pares, e cada par mantém uma cópia completa desse livro-razão.
* **Criptograficamente seguro**: A seguir, vemos que esse livro-razão é “criptograficamente seguro”, o que significa que a criptografia foi utilizada para fornecer serviços de segurança que protegem o livro-razão contra adulterações e uso indevido. Esses serviços incluem **não repúdio**, **integridade dos dados** e **autenticação da origem dos dados**.
* **Somente de acréscimo (append-only)**: Outra propriedade importante é que o blockchain é **somente de acréscimo**, o que significa que os dados só podem ser adicionados ao blockchain em ordem cronológica. Essa propriedade implica que, uma vez que os dados são adicionados ao blockchain, é quase impossível alterá-los, podendo-se considerá-los praticamente **imutáveis**. Em outras palavras, blocos adicionados ao blockchain **não podem ser modificados**, o que permite que o blockchain se torne um livro-razão **imutável e à prova de adulterações**.

Ninguém conhece a verdadeira identidade de **Satoshi Nakamoto**. Após introduzir o Bitcoin em 2009, Nakamoto permaneceu ativo na comunidade de desenvolvedores do Bitcoin até 2011, quando entregou o desenvolvimento do Bitcoin aos desenvolvedores principais e simplesmente desapareceu.

* **Atualizável via consenso**:  
  O atributo mais crítico de um blockchain é que ele só pode ser atualizado **via consenso**. É isso que lhe confere o poder da **descentralização**. Neste cenário, nenhuma autoridade central está no controle da atualização do livro-razão. Em vez disso, qualquer atualização feita ao blockchain é validada contra critérios rigorosos definidos pelo protocolo da blockchain e adicionada ao blockchain somente após **consenso** ser alcançado entre a maioria dos pares/nós participantes da rede. Para atingir o consenso, existem diversos **algoritmos de consenso** que garantem que todas as partes concordem com o estado final dos dados na rede blockchain e o aceitem como verdadeiro.

**Arquitetura do blockchain**

Começaremos observando como o blockchain atua como uma camada dentro de uma rede ponto a ponto distribuída.

**Blockchain em camadas**

O blockchain pode ser visto como uma **camada** de uma rede distribuída ponto a ponto executando sobre a internet, como pode ser visto no diagrama a seguir. É análogo ao SMTP, HTTP ou FTP executando sobre o TCP/IP:

Um blockchain pode ser alterado em cenários raros, nos quais uma **colusão contra a rede blockchain** por atores maliciosos consiga obter mais de 51% da autoridade.  
Também pode haver algumas razões legítimas para alterar dados no blockchain depois que eles foram adicionados, como o “**direito ao esquecimento**” ou o “**direito de exclusão**” (também definidos na legislação GDPR: <https://gdpr-info.eu/art-17-gdpr/>).  
O direito ao esquecimento é o direito que exige que dados pessoais de uma pessoa sejam removidos de registros na internet, registros organizacionais e outros serviços associados. No entanto, esses são casos individuais que precisam ser tratados separadamente e exigem uma solução técnica elegante.

**Figura 1.4: Visão arquitetural em camadas de uma blockchain genérica**

Agora discutiremos todos esses elementos, um por um:

* A **camada mais baixa** é a **Camada de Rede**, que geralmente é a própria internet e fornece uma camada base de comunicação para qualquer blockchain.
* Uma rede **P2P (ponto a ponto)** é executada sobre a Camada de Rede, composta por protocolos de propagação de informações, como protocolos de gossip (sussurro) ou de inundação.
* Após isso, vem a **Camada de Criptografia**, que contém protocolos criptográficos cruciais que garantem a segurança do blockchain. Esses protocolos desempenham um papel vital na integridade dos processos do blockchain, na disseminação segura de informações e nos mecanismos de consenso do blockchain. Essa camada consiste em criptografia de chave pública e componentes relacionados, como **assinaturas digitais** e **funções hash criptográficas**. Às vezes, essa camada é abstraída, mas foi incluída no diagrama porque desempenha um papel fundamental nas operações da blockchain.

Dando sequência à explicação das camadas da arquitetura de blockchain:

* Em seguida vem a **Camada de Consenso**, que se refere ao uso de diversos mecanismos de consenso para garantir **acordo entre os diferentes participantes** do blockchain. Essa é outra parte essencial da arquitetura do blockchain, composta por diversas técnicas, como **replicação de máquina de estados (SMR)**, mecanismos de consenso baseados em prova (como PoW, PoS), ou protocolos de consenso tolerantes a falhas bizantinas oriundos da pesquisa tradicional de sistemas distribuídos.
* Depois temos a **Camada de Execução**, que pode consistir em **máquinas virtuais**, **blocos**, **transações** e **contratos inteligentes**. Esta camada, como o nome sugere, fornece serviços de execução no blockchain, realizando operações como **transferência de valor**, **execução de contratos inteligentes** e **geração de blocos**. Máquinas virtuais como a Ethereum Virtual Machine (**EVM**), Ethereum WebAssembly (**ewasm**) e Zinc VM fornecem um ambiente de execução para que contratos inteligentes sejam executados.
* Finalmente, temos a **Camada de Aplicações**, composta por **contratos inteligentes**, **aplicações descentralizadas (dApps)**, **organizações autônomas descentralizadas (DAOs)** e **agentes autônomos**. Essa camada pode conter efetivamente todos os tipos de programas e agentes em nível de usuário que operam sobre o blockchain. Os usuários interagem com o blockchain por meio de dApps.

Todos esses conceitos serão discutidos em mais detalhes nos próximos capítulos deste livro.

**Blockchain nos negócios**

O modelo tradicional atual de negócios é **centralizado**. Por exemplo, para transferências em dinheiro, **bancos** atuam como uma terceira parte confiável central. Em negociações financeiras, uma **câmara de compensação central** atua como uma terceira parte confiável entre duas ou mais partes envolvidas na negociação.

Do ponto de vista dos negócios, uma blockchain pode ser definida como uma plataforma onde os pares podem **trocar valor usando transações sem a necessidade de um árbitro confiável central (terceira parte)**. Esse conceito é poderoso e, uma vez absorvido, você perceberá o enorme potencial da tecnologia blockchain.

Essa desintermediação permite que a blockchain seja um mecanismo **descentralizado**, no qual nenhuma autoridade única controla a rede. Imediatamente, já podemos ver um benefício significativo da descentralização aqui: se não são necessários bancos ou câmaras de compensação central, isso leva naturalmente a **economia de custos**, **transações mais rápidas**, **transparência** e **maior confiança**.

Além disso, no setor de pagamentos, a blockchain pode ser utilizada para facilitar **pagamentos locais e internacionais de forma descentralizada e segura**.

**Elementos genéricos de um blockchain**

Agora, vamos percorrer os elementos genéricos de uma blockchain. Você pode usar esta seção como uma referência prática caso precise se lembrar das diferentes partes de um blockchain. Elementos mais específicos serão discutidos no contexto de suas respectivas blockchains nos capítulos posteriores, por exemplo, a blockchain do Ethereum.

A estrutura de uma blockchain genérica pode ser visualizada com o auxílio do seguinte diagrama:

**Figura 1.5: Estrutura genérica de uma blockchain**

Os elementos de uma blockchain genérica são descritos a seguir, um por um. Estes são os elementos com os quais você se deparará ao lidar com blockchain:

* **Endereço**: Endereços são identificadores únicos usados em uma transação na blockchain para denotar remetentes e destinatários. Um endereço geralmente é uma chave pública ou derivado de uma chave pública.
* **Transação**: Uma transação é a unidade fundamental de uma blockchain. Representa uma **transferência de valor** de um endereço para outro.
* **Bloco**: Um bloco é composto por **múltiplas transações** e outros elementos, como o **hash do bloco anterior** (ponteiro hash), **carimbo de tempo (timestamp)** e **nonce**. Um bloco é composto por um **cabeçalho de bloco** e uma seleção de transações agrupadas logicamente.

Um bloco contém diversos elementos, que apresentamos a seguir:

* + **Uma referência ao bloco anterior** também é incluída no bloco, a menos que seja um bloco gênese (*genesis block*). Essa referência é o hash do cabeçalho do bloco anterior. Um bloco gênese é o primeiro bloco na blockchain, codificado quando a blockchain é iniciada.
  + **Nonce** é um número gerado e usado apenas uma vez. O nonce é amplamente utilizado em muitas operações criptográficas para prover proteção contra repetição (*replay protection*), autenticação e criptografia. No blockchain, é usado em algoritmos de consenso por PoW e para proteção contra repetição de transações. Um bloco inclui esse valor de nonce.
  + **Timestamp** é o momento de criação do bloco.
  + **Merkle Root** é um hash de todos os nós de uma **árvore de Merkle**. Em um bloco da blockchain, é o hash combinado de todas as transações do bloco. Árvores de Merkle são amplamente utilizadas para validar grandes estruturas de dados de forma segura e eficiente. No mundo do blockchain, são usadas para permitir a verificação eficiente das transações.

O Merkle Root em um bloco está presente na seção de cabeçalho e representa o hash de todas as transações em um bloco. Isso significa que basta verificar o Merkle Root para validar todas as transações presentes na árvore, sem a necessidade de verificá-las uma a uma.

Além do **cabeçalho do bloco**, o bloco contém **transações**, que compõem o **corpo do bloco**. Uma **transação** é um registro de um evento — por exemplo, o evento de transferir dinheiro da conta de um remetente para a conta de um beneficiário. Um bloco contém transações, e seu tamanho varia dependendo do tipo e design da blockchain. Por exemplo, o tamanho do bloco do Bitcoin é limitado a **um megabyte**, o qual inclui o cabeçalho do bloco com 80 bytes e as transações.

A seguinte estrutura é um diagrama simples que mostra a estrutura genérica de um bloco:

**Figura 1.6: Estrutura genérica de um bloco**

Em geral, há apenas alguns atributos que são essenciais para o funcionamento de um bloco: o **cabeçalho do bloco**, que é composto pelo hash do cabeçalho do bloco anterior, timestamp, nonce, Merkle root; e o **corpo do bloco**, que contém as transações.

Há também outros atributos em um bloco, mas, geralmente, os componentes introduzidos nesta seção estão sempre presentes em um bloco:

* **Rede ponto a ponto (P2P)**: Como o nome indica, é uma topologia de rede na qual todos os pares podem se comunicar diretamente entre si, enviando e recebendo mensagens.
* **Linguagem de script ou programação**: Scripts ou programas realizam diversas operações em uma transação para viabilizar certas funções. Por exemplo, no Bitcoin, os scripts de transações são pré-definidos em uma linguagem chamada **Script**, que consiste em conjuntos de comandos que permitem aos nós transferir bitcoins de um endereço para outro. Script é uma linguagem limitada no sentido de que permite apenas operações essenciais necessárias para executar transações, mas **não permite o desenvolvimento de programas arbitrários**.

Pense na linguagem Script como uma calculadora que só suporta operações aritméticas pré-programadas padrão.  
Como tal, a linguagem Script do Bitcoin **não pode ser considerada Turing completa**.  
Em termos simples, uma linguagem Turing completa significa que pode realizar qualquer computação.  
É assim chamada em homenagem a **Alan Turing**, que desenvolveu a ideia de uma máquina de Turing — capaz de executar qualquer algoritmo, por mais complexo que seja.  
Linguagens Turing completas precisam de laços (loops) e ramificações (branching) para executar computações complexas.  
Portanto, a linguagem Script do Bitcoin **não é Turing completa**, enquanto a linguagem **Solidity do Ethereum é**.

* **Máquina virtual**:  
  Essa é uma extensão do script de transação mencionado anteriormente. Uma **máquina virtual** permite a execução de código **Turing completo** em uma blockchain (como contratos inteligentes), enquanto um script de transação é limitado em suas operações. No entanto, **máquinas virtuais não estão disponíveis em todas as blockchains**. Diversas blockchains usam máquinas virtuais para executar programas, como a **EVM (Ethereum Virtual Machine)** e a **CVM (Chain Virtual Machine)**. A EVM é usada na blockchain do Ethereum, enquanto a CVM é uma máquina virtual desenvolvida para e usada na blockchain corporativa “Chain Core”.
* **Máquina de estados**:  
  Uma blockchain pode ser vista como um **mecanismo de transição de estados**, em que um estado é modificado de sua forma inicial para o estado seguinte pelos nós na rede blockchain como resultado da execução de transações.
* **Contratos inteligentes**:  
  São programas que rodam sobre a blockchain e encapsulam a **lógica de negócios** que deve ser executada quando certas condições são atendidas. Esses programas são **executáveis automaticamente e aplicáveis**. A funcionalidade de contratos inteligentes não está disponível em todas as plataformas blockchain, mas está se tornando uma característica muito desejada devido à flexibilidade e poder que proporciona às aplicações em blockchain.

Os contratos inteligentes têm muitos casos de uso, incluindo, mas não se limitando a:

* + gerenciamento de identidade,
  + mercados de capitais,
  + financiamento de comércio,
  + gerenciamento de registros,
  + seguros,
  + e-governança.

Contratos inteligentes serão discutidos com mais detalhes no Capítulo 8, *Smart Contracts*.

* **Nó**:  
  Um nó em uma rede blockchain desempenha várias funções, dependendo do papel que assume. Um nó pode:
  + propor e validar transações,
  + realizar mineração para facilitar o consenso e proteger a blockchain.

Esse objetivo é alcançado ao seguir um protocolo de consenso (mais comumente **Proof of Work – PoW**).

Os nós também podem executar outras funções, como:

* + verificação de pagamentos simples (*lightweight nodes*),
  + validação,
  + e muitas outras, dependendo do tipo de blockchain utilizada e do papel atribuído ao nó.

Os nós também realizam a função de **assinatura de transações**.  
As transações são criadas pelos nós e **assinadas digitalmente** por eles usando **chaves privadas** como prova de que são os legítimos proprietários do ativo que desejam transferir para outra pessoa na rede blockchain. Esse ativo geralmente é um **token** ou **moeda virtual**, como o Bitcoin, mas também pode ser qualquer ativo do mundo real representado na blockchain usando tokens.

Existem agora **padrões relacionados a tokens**; por exemplo, no Ethereum, temos:

* + ERC20
  + ERC721
  + ERC777
  + entre outros

Esses padrões definem as interfaces e a semântica da tokenização.

Um diagrama de alto nível da arquitetura de blockchain destacando os principais elementos mencionados anteriormente é mostrado a seguir:

**Figura 1.7: Estrutura genérica de uma rede blockchain**

O diagrama acima mostra uma rede blockchain com quatro nós (na parte superior), cada um mantendo uma cadeia de blocos, máquina virtual, máquina de estados e endereço. A blockchain é então ampliada (meio) para mostrar a estrutura da cadeia de blocos, que é novamente ampliada (parte inferior) para mostrar a estrutura de uma transação.

Observe que esta é uma **estrutura genérica** de uma blockchain; veremos estruturas específicas em detalhes no contexto das blockchains Ethereum e Bitcoin nos capítulos posteriores deste livro.

**Funcionalidade do blockchain**

Agora que já definimos e descrevemos o blockchain, vejamos **como ele funciona**.

Os nós são ou **mineradores**, que criam novos blocos e cunham criptomoeda (moedas), ou **assinadores de blocos**, que validam e assinam digitalmente as transações.

Uma decisão crítica que toda rede blockchain precisa tomar é **determinar qual nó irá adicionar o próximo bloco** à blockchain. Essa decisão é tomada por meio de um **mecanismo de consenso**.

**Consenso** é o processo de alcançar acordo entre **nós desconfiados** quanto ao estado final dos dados. Para atingir consenso, são utilizados diferentes algoritmos. É fácil alcançar consenso em uma rede centralizada (por exemplo, sistemas cliente-servidor), mas quando múltiplos nós participam de um sistema distribuído e precisam concordar sobre um único valor, **tornar-se um desafio alcançar o consenso**. Esse processo de alcançar acordo sobre um estado comum ou valor entre múltiplos nós é conhecido como **consenso distribuído**.

Se falhas forem permitidas, então chamamos esse mecanismo de **consenso distribuído tolerante a falhas**, em que, mesmo com falhas em alguns nós, o consenso é alcançado entre os participantes.

Agora, vejamos como uma blockchain **valida transações**, **cria** e **adiciona blocos** para expandir a cadeia de blocos, usando um esquema geral de criação de blocos:

1. **Transação é iniciada**:  
   Um nó inicia uma transação ao **criá-la** e **assiná-la digitalmente** com sua chave privada.  
   Uma transação pode representar várias ações em uma blockchain.  
   Mais comumente, é uma estrutura de dados que representa a **transferência de valor** entre usuários na rede blockchain.

A estrutura da transação geralmente contém:

* + a lógica da transferência de valor,
  + regras relevantes,
  + endereços de origem e destino,
  + e outras informações de validação.

As transações normalmente são uma **transferência de criptomoeda** (transferência de valor) ou uma **invocação de contrato inteligente** que pode realizar qualquer operação desejada.  
Uma transação ocorre entre duas ou mais partes. Isso será tratado com mais detalhes em capítulos específicos sobre Bitcoin e Ethereum mais adiante.

1. **Transação é validada e propagada**:  
   Uma transação é **propagada (broadcast)**, geralmente utilizando protocolos de disseminação de dados, como o **protocolo Gossip**, para outros pares que validam a transação com base em critérios de validade predefinidos.  
   Antes de a transação ser propagada, ela também é **verificada para assegurar sua validade**.
2. **Encontrar novo bloco**:  
   Quando a transação é recebida e validada por participantes especiais chamados **mineradores** na rede blockchain, ela é incluída em um **bloco**, e o processo de **mineração** começa.  
   Esse processo também é chamado de “**encontrar um novo bloco**”.  
   Aqui, os nós chamados mineradores **competem entre si** para finalizar o bloco que criaram, através de um processo chamado mineração.
3. **Novo bloco é encontrado**:  
   Uma vez que um minerador resolve um **quebra-cabeça matemático** (ou cumpre os requisitos do mecanismo de consenso implementado no blockchain), o bloco é considerado “**encontrado**” e **finalizado**.  
   Nesse ponto, a transação é considerada **confirmada**.  
   Normalmente, em blockchains de criptomoedas como o Bitcoin, o minerador que resolve o problema é **recompensado com moedas** como incentivo pelo esforço e recursos gastos no processo de mineração.
4. **Adicionar novo bloco à blockchain**:  
   O bloco recém-criado é **validado**, as transações ou contratos inteligentes dentro dele são **executados**, e o bloco é **propagado para outros pares**.  
   Esses pares também validam e executam o bloco.  
   Ele agora se torna **parte da blockchain (livro-razão)**, e o próximo bloco **se conecta criptograficamente** a este.  
   Essa ligação é chamada de **ponteiro hash**.

Esse processo pode ser visualizado no diagrama a seguir:

**Figura 1.8: Como um bloco é gerado**

**Benefícios e características do blockchain**

Numeras vantagens da tecnologia blockchain têm sido discutidas em muitos setores e propostas por líderes de pensamento ao redor do mundo que participam do espaço blockchain. Os benefícios notáveis são os seguintes:

* **Simplificação dos paradigmas atuais**:  
  O modelo atual de blockchain em muitos setores, como finanças ou saúde, é algo desorganizado. Nesse modelo, múltiplas entidades mantêm seus próprios bancos de dados, e o compartilhamento de dados pode se tornar muito difícil devido à natureza **dispar** dos sistemas.  
  No entanto, como uma blockchain pode servir como um **livro-razão único e compartilhado** entre muitas partes interessadas, isso pode **simplificar o modelo** ao reduzir a complexidade de manter sistemas separados por cada entidade.
* **Transações mais rápidas**:  
  Na indústria financeira, especialmente em funções de liquidação pós-negociação, a blockchain pode desempenhar um papel vital ao permitir a **liquidação rápida de negociações**.  
  A blockchain não requer um processo longo de verificação, reconciliação e compensação, pois **uma versão única de dados acordados já está disponível** em um livro-razão compartilhado entre as organizações financeiras.
* **Redução de custos**:  
  Como nenhuma terceira parte confiável ou câmara de compensação é necessária no modelo de blockchain, isso pode **reduzir massivamente os custos indiretos** na forma de taxas pagas a essas partes.
* **Propriedade inteligente** (*smart property*):  
  É possível vincular um ativo digital ou físico à blockchain de forma **segura e precisa**, de modo que **não possa ser reivindicado por mais ninguém**.  
  Você tem **controle total sobre seu ativo**, e ele **não pode ser gasto ou possuído duas vezes**.  
  Compare isso com um arquivo de música digital, por exemplo, que pode ser copiado várias vezes sem controle algum.
* **Descentralização**:  
  Este é um conceito e benefício central da blockchain.  
  Não há necessidade de uma **terceira parte confiável** para validar transações; em vez disso, um **mecanismo de consenso** é usado para concordar sobre a validade das transações.
* **Transparência e confiança**:  
  Como as blockchains são compartilhadas e todos podem ver o que está na blockchain, isso permite que o sistema seja **transparente**.  
  Como resultado, estabelece-se **confiança**. Isso é especialmente relevante em cenários como a **distribuição de fundos ou benefícios**, nos quais a discricionariedade pessoal na escolha de beneficiários precisa ser restrita.

Embora seja verdade que muitos esquemas de Gerenciamento de Direitos Digitais (DRM) estejam sendo usados atualmente juntamente com leis de direitos autorais, **nenhum deles é aplicável de forma tão eficaz** quanto um DRM baseado em blockchain.  
A blockchain pode fornecer **funcionalidade de gerenciamento de direitos digitais** de maneira que possa ser **totalmente aplicada**: se você possui um ativo, **ninguém mais pode reivindicá-lo** a menos que você decida transferi-lo.  
Essa característica tem implicações de longo alcance, especialmente em DRM e sistemas de dinheiro eletrônico, nos quais a detecção de gastos duplos é um requisito crucial.

* **Imutabilidade**:  
  Uma vez que os dados foram escritos na blockchain, é extremamente difícil alterá-los.  
  Eles não são **verdadeiramente imutáveis**, mas como modificar os dados é tão desafiador e quase impossível, isso é visto como um **benefício importante** para manter um livro-razão de transações imutável, especialmente útil em **cenários de auditoria e conformidade**.
* **Alta disponibilidade**:  
  Como o sistema é baseado em **milhares de nós** em uma rede ponto a ponto, e os dados são replicados e atualizados em todos os nós, o sistema se torna **altamente disponível**.  
  Mesmo que alguns nós saiam da rede ou fiquem inacessíveis, a rede continua a funcionar, tornando-a altamente disponível.  
  Essa **redundância** resulta em alta disponibilidade.
* **Alta segurança**:  
  Todas as transações em uma blockchain são **criptograficamente protegidas**, o que fornece **integridade de rede**.  
  Qualquer transação postada pelos nós na blockchain é **verificada com base em um conjunto predefinido de regras**.  
  Somente transações válidas são selecionadas para inclusão em um bloco.  
  A blockchain se baseia em **tecnologia criptográfica comprovada**, que assegura a integridade e a disponibilidade dos dados.

Geralmente, **confidencialidade** não é fornecida devido às exigências de **transparência**.  
Essa limitação é o principal **obstáculo à sua adoção por instituições financeiras** e outras indústrias que requerem privacidade e confidencialidade nas transações.

No entanto, pode-se argumentar que, em muitas situações, **a confidencialidade não é necessária**, e a transparência é preferível.  
Por exemplo, com o Bitcoin, a confidencialidade não é um requisito absoluto; embora seja **desejável em certos cenários**.

Um exemplo mais recente é o **Zcash** (<https://z.cash>), que utiliza **provas de conhecimento zero (zero-knowledge proofs)** para fornecer uma plataforma de **transações anônimas**.

Outros serviços de segurança, como **não repúdio** e **autenticação**, também são fornecidos pela blockchain, já que todas as ações são protegidas com **chaves privadas e assinaturas digitais**.

* **Plataforma para contratos inteligentes**:  
  Contratos inteligentes são programas automatizados e autônomos que residem na rede blockchain e encapsulam a **lógica de negócios e o código necessários** para executar uma função quando certas condições são atendidas.  
  Essa é, de fato, uma característica **revolucionária** da blockchain, pois proporciona **flexibilidade, velocidade, segurança e automação** para cenários do mundo real, podendo levar a um sistema totalmente confiável com **reduções significativas de custo**.  
  Contratos inteligentes podem ser programados para realizar qualquer ação em nível de aplicação de que os usuários da blockchain precisem, de acordo com seus requisitos específicos de negócio.

**Limitações da tecnologia blockchain**

Assim como qualquer tecnologia, há desafios que precisam ser superados para tornar o sistema mais robusto, útil e acessível. A tecnologia blockchain **não é exceção**.  
De fato, **muito esforço** está sendo feito tanto na academia quanto na indústria para superar os desafios enfrentados.

Nem todas as blockchains têm um mecanismo para executar contratos inteligentes; no entanto, essa é uma funcionalidade muito desejável.  
Ainda assim, algumas blockchains **optam por não incluir contratos inteligentes** de propósito, com o argumento de que **execuções codificadas são mais rápidas** sem as complexidades de contratos inteligentes de uso geral.

A seguir, estão as limitações principais da tecnologia blockchain:

* **Escalabilidade**:  
  A escalabilidade é uma das **maiores questões enfrentadas** pela blockchain.  
  O tempo necessário para registrar transações e a limitação no número de transações por segundo são **problemas sérios** que impedem a adoção em larga escala da blockchain para casos de uso com alto volume de transações.  
  Como exemplo, o Bitcoin só pode processar entre **7 e 10 transações por segundo**, e o Ethereum, cerca de **15 a 30 transações por segundo**.  
  Por outro lado, **sistemas tradicionais** como Visa podem processar **milhares de transações por segundo**.

A comunidade tem buscado diversas **soluções de escalabilidade**, como:

* + **Aumento do tamanho dos blocos**,
  + **Segmentação de estados (state sharding)**,
  + **Soluções de camada 2**, como **Lightning Network** e **rollups**,
  + **Sidechains** e **off-chain computation**.

Cada uma dessas abordagens tem seus prós e contras e está em constante desenvolvimento.

* **Regulação**:  
  A regulação do blockchain e de suas aplicações, especialmente criptomoedas, **ainda é incerta**.  
  Devido à natureza **transfronteiriça, descentralizada e pseudônima** da blockchain, muitos governos ainda não definiram claramente como essa tecnologia será tratada.  
  A ausência de regulamentação ou a implementação de regulamentações rígidas **pode afetar a adoção** da blockchain, especialmente no setor financeiro.
* **Privacidade**:  
  Em muitos blockchains públicos, como o Bitcoin, as transações são **totalmente visíveis** a todos na rede.  
  Isso pode ser problemático para empresas ou indivíduos que **precisam manter a confidencialidade de suas transações**.  
  Algumas soluções vêm sendo desenvolvidas com o objetivo de equilibrar **transparência e privacidade**, como:
  + **ZK-SNARKs** e **ZK-STARKs** (provas de conhecimento zero),
  + **MimbleWimble**,
  + **Transações confidenciais** (Confidential Transactions – CT).
* **Imaturidade**:  
  A tecnologia blockchain ainda é considerada **emergente e em desenvolvimento**.  
  Embora existam muitas implementações de blockchain em uso atualmente, os padrões ainda estão evoluindo, e muitas ferramentas e plataformas estão em estágios experimentais ou beta.  
  Isso implica que **desenvolvedores e empresas enfrentam incertezas** e riscos ao adotar soluções baseadas em blockchain.
* **Interoperabilidade**:  
  Existem **várias plataformas blockchain**, e muitas delas **não são compatíveis entre si**.  
  Isso cria silos de dados e redes, limitando a comunicação e a transferência de ativos entre diferentes blockchains.  
  Iniciativas como:
  + **Polkadot**,
  + **Cosmos**,
  + **Interledger Protocol (ILP)**  
    tentam resolver esse problema e proporcionar **interoperabilidade entre blockchains**.
* **Adoção**:  
  Embora o entusiasmo com o blockchain seja grande, a **adoção em massa ainda não foi alcançada**.  
  Isso se deve, em parte, às limitações acima, mas também à **falta de compreensão**, ao **ceticismo**, e à **complexidade técnica** envolvida na implementação de soluções baseadas em blockchain.

**Revisão**

Neste capítulo, aprendemos sobre os **conceitos fundamentais** da tecnologia blockchain.  
O blockchain é um **livro-razão distribuído imutável** de transações, **mantido por uma rede ponto a ponto**, que **alcança consenso distribuído** por meio de **algoritmos de consenso**.

Estudamos os seguintes conceitos principais:

* Uma introdução à tecnologia blockchain e à sua evolução,
* Como o blockchain resolve problemas de confiança e descentralização,
* A história e os antecedentes técnicos que levaram ao surgimento do Bitcoin,
* A arquitetura em camadas do blockchain,
* Elementos genéricos de uma blockchain (blocos, transações, nós, contratos inteligentes),
* O funcionamento de uma transação desde sua criação até ser incluída em um bloco,
* Benefícios, características e limitações da tecnologia blockchain.

**Resumo**

O blockchain é um **livro-razão distribuído** baseado em uma rede **ponto a ponto (P2P)**.  
Cada nó na rede mantém uma cópia do livro-razão.  
Todos os nós participam no processo de verificação e validação de transações, que são então **inseridas em blocos**.  
Esses blocos são **criptograficamente conectados** entre si para formar a cadeia de blocos — a **blockchain**.

A blockchain **elimina a necessidade de uma terceira parte confiável**, utilizando **criptografia** e **consenso distribuído**.  
Ela tem aplicações em **finanças, saúde, cadeia de suprimentos, governo, identidade digital**, entre outros setores.

Apesar das suas **limitações atuais** — como escalabilidade, regulação, privacidade, interoperabilidade — a blockchain representa uma **mudança de paradigma** com potencial de transformar significativamente a maneira como interagimos, conduzimos negócios e trocamos valor.