**Capítulo 2**

**Descentralização**

Descentralização não é um conceito novo. Ele tem sido usado em estratégia, gestão e no setor governamental há muito tempo. A ideia básica da descentralização é distribuir o controle e a autoridade para as periferias de uma organização, em vez de concentrá-los em um único corpo central. Essa estrutura produz diversos benefícios para as organizações, como aumento da eficiência, tomada de decisões acelerada, melhor motivação e uma carga reduzida sobre a alta administração.

Neste capítulo, discutiremos o conceito de descentralização no contexto do blockchain, cuja base fundamental é que nenhuma autoridade central única controla a rede. Este capítulo apresentará exemplos de vários métodos de descentralização e maneiras de alcançá-la. Além disso, discutiremos aplicações descentralizadas e plataformas para alcançar a descentralização.

Neste capítulo, cobriremos o seguinte:

* Introdução à descentralização
* Descentralização de ecossistema completo
* Descentralização na prática
* Tendências inovadoras

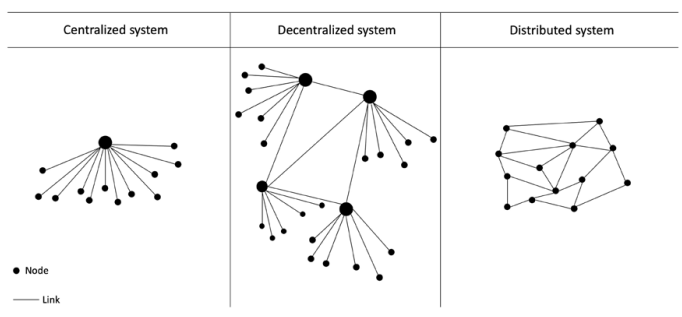
**Introdução à descentralização**

A descentralização é um benefício central da tecnologia blockchain. Por design, o blockchain é um veículo perfeito para fornecer uma plataforma que não necessita de intermediários e que pode funcionar com líderes escolhidos ao longo do tempo por meio de mecanismos de consenso. Esse modelo permite que qualquer pessoa dispute a posição de autoridade decisória. Essa competição é governada por um mecanismo de consenso, que discutiremos no Capítulo 5, *Algoritmos de Consenso*.

A descentralização é aplicada em graus variados, desde um modelo semidescentralizado até um totalmente descentralizado, dependendo dos requisitos e circunstâncias. A descentralização pode ser vista, a partir da perspectiva do blockchain, como um mecanismo que fornece uma maneira de remodelar aplicações e paradigmas existentes, ou de construir novas aplicações, dando controle total aos usuários.

A infraestrutura de TI foi, convencionalmente, baseada em um paradigma centralizado, no qual os servidores de banco de dados ou de aplicação estão sob o controle de uma autoridade central, como um administrador de sistemas. Com o Bitcoin e o advento da tecnologia blockchain, esse modelo mudou, e agora existe tecnologia que permite a qualquer pessoa iniciar um sistema descentralizado e operá-lo sem um ponto único de falha ou uma autoridade confiável única. Ele pode ser executado de forma autônoma ou exigir alguma intervenção humana, dependendo do tipo e modelo de governança utilizado na aplicação descentralizada que roda no blockchain.

O diagrama a seguir mostra os diferentes tipos de sistemas que existem atualmente: central, distribuído e descentralizado. Este conceito foi publicado pela primeira vez por Paul Baran em *On Distributed Communications: Introduction to Distributed Communications Networks* (Rand Corporation, 1964):



**Figura 2.1: Diferentes tipos de redes/sistemas**

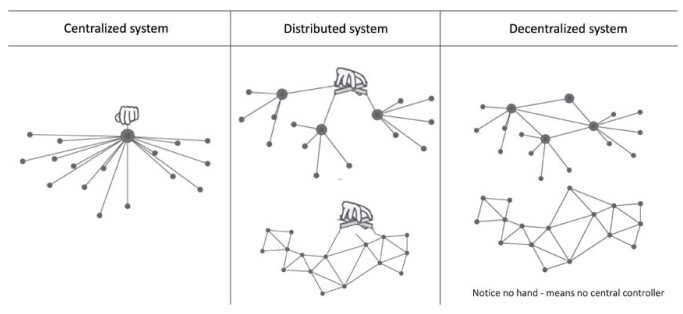
Sistemas centralizados são sistemas convencionais de TI (cliente-servidor) nos quais há uma única autoridade que controla e é exclusivamente responsável por todas as operações no sistema. Todos os usuários de um sistema centralizado dependem de uma única fonte de serviço. A maioria dos provedores de serviços online, incluindo Google, Amazon, eBay, Yahoo! e a App Store da Apple, usam esse modelo convencional para fornecer serviços.

Em um sistema distribuído, dados e computação são replicados entre múltiplos nós em uma rede no que os usuários veem como um único sistema coerente.

Um sistema descentralizado é um tipo de rede em que os nós não dependem de um único nó mestre; em vez disso, o controle é distribuído entre muitos nós. Isso é análogo a um modelo no qual cada departamento de uma organização é responsável pelo seu próprio servidor de banco de dados, retirando, assim, o poder do servidor central e distribuindo-o para os subdepartamentos, que gerenciam seus próprios bancos de dados.

Uma inovação significativa no paradigma descentralizado é o **consenso descentralizado**. Esse mecanismo surgiu com o Bitcoin, e ele permite que usuários concordem sobre algo por meio de um algoritmo de consenso sem a necessidade de uma terceira parte confiável central, intermediário ou provedor de serviços.

Também podemos agora visualizar os diferentes tipos de redes a partir de uma perspectiva diferente, destacando a autoridade controladora dessas redes como uma mão simbólica, conforme mostrado no diagrama a seguir:

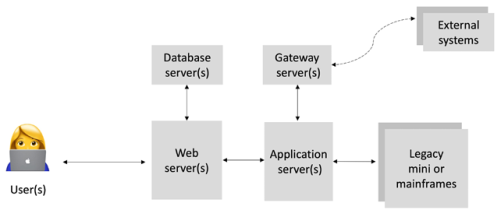


**Figura 2.2: Diferentes tipos de redes/sistemas representando a descentralização sob uma perspectiva moderna**

Às vezes, esse termo é confundido com **computação paralela**. Variações de ambos os modelos são usadas para alcançar tolerância a falhas e velocidade. Embora haja alguma sobreposição na definição, a principal diferença entre esses sistemas é que, em um sistema de computação paralela, a computação é realizada por todos os nós simultaneamente para atingir um único resultado; por exemplo, plataformas de computação paralela são usadas em pesquisa e previsão meteorológica, simulação e modelagem financeira. No modelo de sistema paralelo, ainda há uma autoridade central que controla todos os nós e governa o processamento. Isso significa que o sistema ainda é centralizado por natureza.

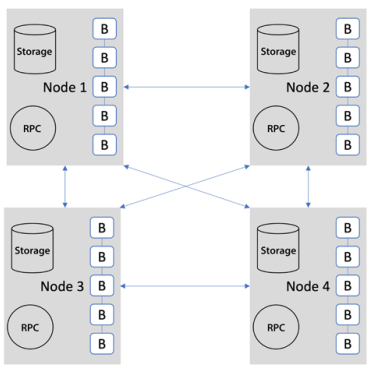
O diagrama anterior mostra o modelo centralizado tradicional com um controlador central, que representa o modelo usual cliente/servidor. No meio, temos sistemas distribuídos, nos quais ainda temos um controlador central, mas o sistema é composto por muitos nós dispersos. No lado direito, observe que não há nenhuma mão/controlador controlando as redes. Essa é a principal diferença entre redes descentralizadas e distribuídas. Um sistema descentralizado pode parecer, do ponto de vista topológico, com um sistema distribuído, mas não possui uma autoridade central que controle a rede.

As diferenças entre sistemas distribuídos e descentralizados também podem ser observadas em um nível prático no seguinte diagrama:



**Figura 2.3: Um sistema distribuído tradicional compreende muitos servidores desempenhando diferentes papéis**

O diagrama a seguir mostra um sistema descentralizado (baseado em blockchain) no qual uma réplica exata das aplicações e dos dados é mantida em toda a rede, em cada nó participante:



**Figura 2.4: Um sistema descentralizado baseado em blockchain (observe as conexões diretas P2P e as réplicas exatas de blocos (dados))**

Uma comparação entre sistemas centralizados e descentralizados é mostrada na tabela a seguir:

| **Característica** | **Centralizado** | **Descentralizado** |
| --- | --- | --- |
| Propriedade | Provedor de serviço | Todos os usuários |
| Arquitetura | Cliente/servidor | Distribuída, diferentes topologias |
| Segurança | Básica | Mais segura |
| Alta disponibilidade | Não | Sim |
| Tolerância a falhas | Limitada, ponto único de falha | Altamente tolerante, pois o serviço é replicado |
| Resistência à colusão | Básica, pois está sob controle de um grupo ou até mesmo de um único indivíduo | Altamente resistente, pois algoritmos de consenso garantem defesa contra adversários |
| Arquitetura de aplicação | Aplicação única | Aplicação replicada em todos os nós da rede |
| Confiança | Consumidores devem confiar no provedor de serviço, ou seja, uma terceira parte confiável | Não é necessário confiança mútua |
| Custo para o consumidor | Alto | Baixo |

A comparação na tabela cobre apenas algumas características principais e não é uma lista exaustiva, mas deve fornecer um bom nível de comparação.

Note que a tolerância a falhas (a capacidade de um sistema continuar operando mesmo que alguns de seus componentes falhem) em sistemas centralizados também é melhorada pela replicação de dados. Contudo, no caso de um sistema descentralizado, a tolerância a falhas é maior porque, primeiro, ele é um sistema distribuído, e segundo, é descentralizado, de modo que nenhum participante único poderia manipular o sistema sozinho e obter uma vantagem desproporcional. Se a arquitetura for cliente/servidor básica, com apenas um servidor central ou talvez apenas um servidor primário e um servidor de backup fornecendo serviços, ela será consideravelmente menos tolerante a falhas do que um sistema blockchain descentralizado distribuído, já que blockchains geralmente são replicados em centenas ou milhares de réplicas (participantes) ao redor do mundo, em diferentes localizações geográficas.

Agora discutiremos quais métodos podem ser usados para alcançar a descentralização.

**Métodos de descentralização**

Dois métodos podem ser usados para alcançar a descentralização: **desintermediação** e **competição**. Esses métodos serão discutidos em detalhes nas seções a seguir.

**Desintermediação**

O conceito de desintermediação pode ser explicado com um exemplo. Imagine que você queira enviar dinheiro a um amigo em outro país. Você vai a um banco que, mediante uma taxa, transferirá seu dinheiro para o banco nesse país. Nesse caso, o banco mantém um banco de dados central que é atualizado, confirmando que você enviou o dinheiro.

Com a tecnologia blockchain, é possível enviar esse dinheiro diretamente, sem a necessidade de um banco. Tudo o que você precisa é de um endereço no blockchain. Dessa forma, o intermediário (ou seja, o banco) não é mais necessário, e a descentralização é alcançada pela desintermediação. É discutível, no entanto, o quão prática é a descentralização por meio da desintermediação no setor financeiro, devido aos imensos requisitos regulatórios e de conformidade.

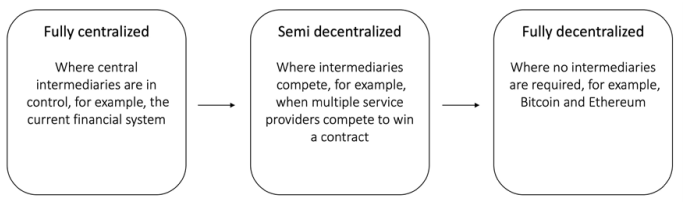
No entanto, esse modelo pode ser usado não apenas nas finanças, mas também em muitos outros setores, como saúde, direito e setor público. Na área da saúde, em vez de depender de uma terceira parte confiável (como um sistema de prontuários de hospital), os pacientes podem ter controle total de sua própria identidade e dos seus dados, que podem compartilhar diretamente apenas com as entidades em que confiam. Como solução geral, o blockchain pode servir como um sistema descentralizado de gestão de registros de saúde, no qual os registros podem ser trocados de forma segura e direta entre diferentes entidades (hospitais, empresas farmacêuticas, pacientes) globalmente, sem qualquer autoridade central. Embora a interoperabilidade entre diferentes padrões de registro e categorização de dados de saúde não seja fácil, o blockchain pode ao menos fornecer uma plataforma para compartilhar dados entre diferentes prestadores de serviços de saúde.

**Descentralização impulsionada por competição**

Em um método baseado em competição, diferentes prestadores de serviço competem para serem selecionados para fornecer serviços ao sistema. Esse paradigma não alcança descentralização completa. No entanto, até certo ponto, garante que um intermediário ou provedor de serviços não monopolize o serviço. No contexto da tecnologia blockchain, pode-se imaginar um sistema no qual contratos inteligentes escolhem um provedor de dados externo dentre vários disponíveis com base em sua reputação, pontuação anterior, avaliações e qualidade de serviço. Esse método não resultará em descentralização total, mas permite que contratos inteligentes façam escolhas livres com base em diversos critérios. Dessa forma, cultiva-se um ambiente de competição entre provedores de serviço, que competem para se tornar o prestador de serviço preferido.

**Quantificando a descentralização**

No diagrama a seguir, são mostrados níveis variados de descentralização. No lado esquerdo, está representada a abordagem convencional, onde um sistema central está no controle; no lado direito, a desintermediação completa é alcançada, pois os intermediários são completamente removidos. Intermediários ou provedores de serviço concorrentes são mostrados no centro.



**Figura 2.5: Escala de descentralização**

Os bancos centrais e as autoridades monetárias reconheceram que podem usar blockchain para emitir uma moeda digital regulada chamada moeda digital de banco central (CBDC), o que pode simplificar a implementação e execução de políticas monetárias e fiscais. Embora esse seja um insight significativo e possa resultar em um ecossistema financeiro mais seguro, eficiente e inclusivo, espera-se que seja centralizado, com um banco central ou autoridade monetária nacional regulando e emitindo a moeda.

Nesse nível, intermediários ou provedores de serviço são selecionados com base na reputação ou votação, alcançando assim uma descentralização parcial:

**Figura 2.5: Escala de descentralização**

Também podemos pensar sobre o espectro de descentralização a partir de outro ângulo, onde a descentralização atingível varia do mínimo de descentralização alcançável (MAD – *Minimum Achievable Decentralization*) até o máximo de descentralização viável (MFD – *Maximum Feasible Decentralization*). Além disso, podemos focar em encontrar um ponto ótimo de descentralização (ODP – *Optimal Decentralization Point*) no espectro para um determinado caso de uso, ou seja, onde se atinge a máxima descentralização juntamente com o mínimo possível de centralização, o que é mais favorável para o caso de uso específico em consideração.

Uma pergunta surge aqui: como podemos medir o nível de descentralização? Uma resposta para essa pergunta é o **coeficiente de Nakamoto**. Essa métrica é calculada usando diversos fatores. Ela representa o número de entidades que precisam ser controladas para comprometer uma rede blockchain. Quanto maior o valor do coeficiente de Nakamoto, mais descentralizada é a rede.

Qualquer sistema descentralizado é composto de diversos subsistemas descentralizados. Se qualquer subsistema for centralizado, o sistema como um todo é considerado centralizado. Por exemplo, uma blockchain pode ser composta de diversos subsistemas, incluindo mineradores, clientes, desenvolvedores, corretoras (*exchanges*), nós e propriedade. Podemos dizer que, devido ao monopólio dos pools de mineração no processo de mineração do Bitcoin, o Bitcoin pode ser considerado centralizado. A ideia-chave por trás dessa métrica é, primeiro, enumerar os subsistemas de um sistema descentralizado, depois descobrir quantas entidades precisam ser comprometidas para obter controle de cada subsistema e, então, usar o menor desses valores para obter o grau efetivo de descentralização do sistema. Por exemplo, o Ethereum poderia ser considerado centralizado porque apenas um punhado de desenvolvedores realiza a maior parte dos *commits*, resultando assim em centralização do desenvolvimento.

Você pode acompanhar o coeficiente de Nakamoto aqui: <https://nakaflow.io>

O coeficiente de Nakamoto foi introduzido por Balaji S. Srinivasan e Leland Lee em seu artigo disponível aqui:  
<https://news.earn.com/quantifying-decentralization-e39db233c28e>

**Benefícios da descentralização**

Existem muitos benefícios da descentralização, incluindo transparência, eficiência, economia de custos, desenvolvimento de ecossistemas confiáveis e, em alguns casos, privacidade e anonimato. Alguns desafios, como exigências de segurança, falhas de software e erro humano, precisam ser examinados cuidadosamente.

Por exemplo, em um sistema descentralizado como o Bitcoin ou o Ethereum, onde a segurança é normalmente fornecida por chaves privadas, como podemos garantir que um ativo ou token associado a essas chaves privadas não possa se tornar inútil devido à negligência ou a bugs no código? E se as chaves privadas forem perdidas por negligência do usuário? E se, devido a um erro no código do contrato inteligente, a aplicação descentralizada se tornar vulnerável a ataques?

Antes de embarcar em uma jornada para descentralizar tudo usando blockchain e aplicações descentralizadas, é essencial compreendermos que **nem tudo pode ou precisa ser descentralizado**.

Essa visão levanta algumas perguntas fundamentais. Um blockchain é realmente necessário? Quando um blockchain é exigido? Em quais circunstâncias o blockchain é preferível aos bancos de dados tradicionais? Para responder a essas perguntas, observe o simples conjunto de questões apresentado abaixo:

| **Pergunta** | **Sim/Não** | **Solução recomendada** |
| --- | --- | --- |
| É necessário alto rendimento de dados? | Sim | Use um banco de dados tradicional. |
|  | Não | Um banco de dados central ainda pode ser útil se outros requisitos forem atendidos. Por exemplo, se os usuários confiarem uns nos outros, talvez não haja necessidade de um blockchain. No entanto, se eles não confiarem ou a confiança não puder ser estabelecida por qualquer razão, o blockchain pode ser útil. |
| As atualizações são controladas centralmente? | Sim | Use um banco de dados tradicional. |
|  | Não | Você pode investigar como um blockchain público/privado pode ajudar. |
| Os usuários confiam uns nos outros? | Sim | Use um banco de dados tradicional. |
|  | Não | Use um blockchain público. |
| Os usuários são anônimos? | Sim | Use um blockchain público. |
|  | Não | Use um blockchain privado. |
| É necessário manter consenso dentro de um consórcio? | Sim | Use um blockchain privado. |
|  | Não | Use um blockchain público. |
| É necessária imutabilidade estrita dos dados? | Sim | Use um blockchain. |
|  | Não | Use um banco de dados central/tradicional. |

Responder a todas essas perguntas pode ajudá-lo a decidir se um blockchain é necessário ou adequado para resolver um problema. Além das perguntas colocadas neste modelo, há muitas outras questões a considerar, como latência, escolha dos mecanismos de consenso, se o consenso é necessário ou não, e onde o consenso será alcançado.

Se o consenso for mantido internamente por um consórcio, então um blockchain privado deve ser usado; caso contrário, se o consenso for necessário publicamente entre múltiplas entidades, então uma solução de blockchain público deve ser considerada. Outros aspectos, como a imutabilidade, também devem ser considerados ao decidir se deve-se usar um blockchain ou um banco de dados tradicional. Se for necessária imutabilidade estrita dos dados, então um blockchain público deve ser usado; caso contrário, um banco de dados central pode ser uma opção.

À medida que a tecnologia blockchain amadurece, mais perguntas surgirão com relação a este modelo de seleção. Por ora, no entanto, este conjunto de perguntas é suficiente para decidir se uma solução baseada em blockchain é adequada ou não.

Agora entendemos diferentes métodos de descentralização e vimos como decidir se um blockchain é necessário ou não em um cenário particular. Vamos agora observar o processo de descentralização, ou seja, como podemos pegar um sistema existente e descentralizá-lo.

**Avaliando os requisitos**

Existem sistemas que precedem o blockchain e o Bitcoin, incluindo o BitTorrent e o sistema de compartilhamento de arquivos Gnutella, que, até certo ponto, poderiam ser classificados como descentralizados. No entanto, devido à falta de qualquer mecanismo de incentivo, a participação da comunidade diminuiu gradualmente. Com o advento da tecnologia blockchain, muitas iniciativas estão sendo tomadas para aproveitar essa nova tecnologia com o intuito de alcançar a descentralização.

A blockchain do Bitcoin tem sido tipicamente a primeira escolha para muitos, pois provou ser a mais resiliente e segura. No entanto, o Ethereum tornou-se uma escolha mais proeminente devido à flexibilidade que oferece para programar qualquer lógica de negócios na blockchain por meio da criação de contratos inteligentes. Além disso, novas cadeias como Polkadot, Solana e Cardano também estão sendo usadas como plataformas para descentralização por muitos desenvolvedores.

O coeficiente de Nakamoto varia de cadeia para cadeia e deve ser um fator decisivo durante a avaliação de plataformas de blockchain para um caso de uso. Embora seja ideal ser o mais descentralizado possível, em alguns casos, dependendo do uso, pode-se abrir mão de parte da descentralização. O Bitcoin possui o maior coeficiente de Nakamoto, enquanto algumas cadeias têm coeficientes bastante baixos. A escolha da plataforma de blockchain é governada pelo caso de uso e pelos requisitos dos usuários e, em alguns casos, até mesmo abrir mão de algum nível de descentralização é aceitável.

Arvind Narayanan et al. propuseram uma estrutura em seu livro *Bitcoin and Cryptocurrency Technologies* que pode ser usada para avaliar os requisitos de descentralização de uma variedade de questões no contexto da tecnologia blockchain. A estrutura levanta quatro perguntas cujas respostas fornecem uma compreensão clara de como um sistema pode ser descentralizado:

* **O que está sendo descentralizado?**: Pode ser qualquer sistema, como um sistema de identidade ou um sistema de negociação.
* **Qual o nível de descentralização necessário?**: Pode ser desintermediação total ou parcial.
* **Qual blockchain está sendo usada?**: Pode ser a blockchain do Bitcoin, a do Ethereum ou qualquer outra que se julgue adequada para a aplicação específica.
* **Qual mecanismo de segurança é usado?**: Por exemplo, o mecanismo de segurança pode ser baseado em atomicidade, onde a transação é executada totalmente ou não é executada. Essa abordagem determinística garante a integridade do sistema. Outros mecanismos incluem aqueles baseados em reputação, o que permite diferentes graus de confiança em um sistema.

A seguir, vamos avaliar um sistema de transferência de dinheiro como exemplo de uma aplicação selecionada para ser descentralizada. As quatro perguntas discutidas anteriormente são usadas para avaliar os requisitos de descentralização dessa aplicação. As respostas para essas perguntas são as seguintes:

* **O que está sendo descentralizado?**: Um sistema de transferência de dinheiro.
* **Qual o nível de descentralização necessário?**: Desintermediação.
* **Qual blockchain está sendo usada?**: Bitcoin.
* **Qual mecanismo de segurança é usado?**: Atomicidade.

As respostas indicam que o sistema de transferência de dinheiro pode ser descentralizado removendo-se o intermediário, implementado na blockchain do Bitcoin, e que uma garantia de segurança pode ser fornecida via atomicidade. A atomicidade garantirá que as transações sejam executadas com sucesso por completo ou não sejam executadas de forma alguma. Escolhemos a blockchain do Bitcoin porque ela é a blockchain estabelecida há mais tempo e resistiu ao teste do tempo.

De forma semelhante, essa estrutura pode ser usada para qualquer outro sistema que precise ser avaliado em termos de descentralização. As respostas a essas quatro perguntas simples ajudam a esclarecer qual abordagem tomar para descentralizar o sistema.

Para alcançar a descentralização completa, é necessário que o ambiente ao redor da blockchain também seja descentralizado. Vamos observar a descentralização do ecossistema completo a seguir.

**Descentralização de ecossistema completo**

O blockchain é um livro-razão distribuído que roda sobre sistemas convencionais. Esses elementos incluem armazenamento, comunicação e computação.

Há outros fatores, como identidade e riqueza, que são tradicionalmente baseados em paradigmas centralizados, e há uma necessidade de descentralizar esses aspectos também para alcançar um ecossistema suficientemente descentralizado.

**Armazenamento**

Os dados podem ser armazenados diretamente em uma blockchain e, com esse fato, alcança-se a descentralização. No entanto, uma desvantagem significativa dessa abordagem é que a blockchain não é adequada para armazenar grandes quantidades de dados por design. Ela pode armazenar transações simples e alguns dados arbitrários, mas certamente não é adequada para armazenar imagens ou grandes blocos de dados, como acontece com sistemas tradicionais de banco de dados.

Uma alternativa melhor para armazenar dados é usar **tabelas hash distribuídas (DHTs)**. As DHTs foram usadas inicialmente em softwares de compartilhamento de arquivos ponto a ponto, como BitTorrent, Napster, Kazaa e Gnutella. A pesquisa em DHTs foi popularizada pelos projetos CAN, Chord, Pastry e Tapestry. O BitTorrent é a rede mais escalável e rápida, mas o problema com o BitTorrent e os demais é que **não há incentivo** para que os usuários mantenham os arquivos indefinidamente.

Os usuários geralmente não mantêm os arquivos permanentemente, e se os nós que possuem os dados ainda necessários por alguém saírem da rede, não há como recuperar esses dados, exceto fazendo com que os nós necessários retornem à rede para que os arquivos se tornem novamente disponíveis.

Duas exigências principais aqui são:

* **Alta disponibilidade**, o que significa que os dados devem estar disponíveis quando necessários;
* **Estabilidade de link**, o que significa que os links da rede também devem estar sempre acessíveis.

O **InterPlanetary File System (IPFS)** possui ambas as propriedades, e sua visão é fornecer uma Web descentralizada, substituindo o protocolo HTTP. O IPFS usa a DHT Kademlia e **Grafos Acíclicos Dirigidos de Merkle (DAGs)** para fornecer suas funcionalidades de armazenamento e busca, respectivamente. O conceito de DHTs e DAGs será introduzido em detalhes no Capítulo 4 (*Criptografia Assimétrica*) e no Capítulo 17 (*Escalabilidade*), respectivamente.

O mecanismo de incentivo para armazenar dados é baseado em um protocolo conhecido como **Filecoin**, que paga incentivos aos nós que armazenam dados usando o mecanismo **Bitswap**. O Bitswap permite que os nós mantenham um livro-razão simples de bytes enviados ou recebidos em uma relação um-para-um. Além disso, um mecanismo de controle de versão baseado no Git é usado no IPFS para fornecer estrutura e controle sobre o versionamento dos dados.

Existem outras alternativas para armazenamento de dados, como **Ethereum Swarm**, **Storj** e **MaidSafe**. O Ethereum possui seu próprio ecossistema descentralizado e distribuído que usa o Swarm para armazenamento e o protocolo Whisper para comunicação. O MaidSafe busca fornecer uma Web descentralizada. Todos esses projetos são discutidos mais adiante neste livro com maior profundidade.

O **BigChainDB** é outro projeto de descentralização da camada de armazenamento, com o objetivo de fornecer um banco de dados descentralizado escalável, rápido e linearmente escalável, como alternativa a um sistema de arquivos tradicional. O BigChainDB complementa plataformas de processamento descentralizado e sistemas de arquivos como o Ethereum e o IPFS.

**Comunicação**

A Internet (a camada de comunicação no blockchain) parece ser descentralizada. Essa crença é correta até certo ponto, já que a visão original da Internet era desenvolver um sistema de comunicações descentralizado. Serviços como e-mail e armazenamento online são agora todos baseados em um paradigma em que o **provedor de serviço está no controle**, e os usuários confiam nesses provedores para lhes conceder acesso ao serviço conforme solicitado. Esse modelo é baseado na **confiança incondicional em uma autoridade central** (o provedor de serviços), onde os usuários **não estão no controle de seus dados**. Até mesmo as senhas dos usuários são armazenadas em sistemas de terceiros confiáveis.

Assim, existe a necessidade de fornecer **controle aos usuários individuais** de forma que o acesso a seus dados seja garantido e **não dependa de um único terceiro**. O acesso à Internet é baseado em Provedores de Serviços de Internet (ISPs), que atuam como um hub central para os usuários da Internet. Se o ISP for desligado por qualquer motivo, então nenhuma comunicação é possível com esse modelo.

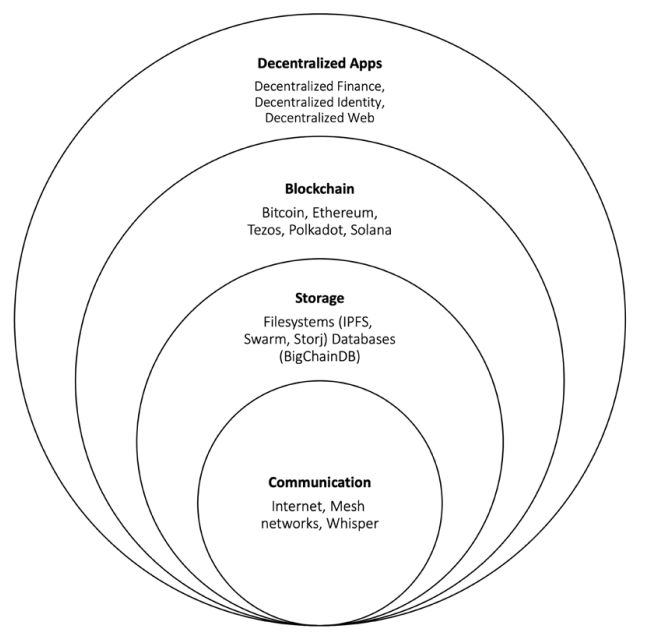
Uma alternativa é usar **redes mesh** (*mesh networks*). As redes mesh usam tecnologias sem fio como o **Bluetooth Low Energy (BLE)** para formar redes de comunicação que não precisam de conectividade com a Internet. Embora sejam limitadas em funcionalidade em comparação com a Internet, ainda fornecem uma **alternativa descentralizada**, onde nós em proximidade relativa podem se comunicar diretamente entre si, sem necessidade de Internet ou de um hub central como um ISP. Agora imagine uma rede que permita aos usuários **controlar sua comunicação**; ninguém pode desligá-la por qualquer razão. Esse tipo de rede é muito vantajoso em situações como **desastres naturais ou zonas de guerra**. Outro uso pode ser a organização de **protestos contra regimes opressores** que possam ter bloqueado a Internet. Um exemplo de tal aplicativo de mensagens offline é o **Bridgefy**. Esse pode ser o próximo passo para descentralizar as redes de comunicação no ecossistema blockchain.

Como mencionado anteriormente, a visão original da Internet era construir uma rede descentralizada; no entanto, ao longo dos anos, com o surgimento de provedores de serviços em larga escala como Google, Amazon e eBay, o controle foi transferido para esses grandes atores. Por exemplo, o e-mail é um sistema descentralizado em sua essência; isto é, qualquer pessoa pode executar um servidor de e-mail com esforço mínimo e começar a enviar e receber e-mails. No entanto, existem alternativas melhores disponíveis. Por exemplo, Gmail e Outlook já fornecem serviços gerenciados para usuários finais, então há uma inclinação natural para selecionar um desses grandes serviços centralizados, pois são mais convenientes, seguros e, acima de tudo, gratuitos. Este é um exemplo que mostra como a Internet caminhou em direção à **centralização**.

Serviços gratuitos, no entanto, são oferecidos **ao custo de exposição de dados pessoais valiosos**, e muitos usuários não estão cientes desse fato. O blockchain **reviveu a visão da descentralização** ao redor do mundo, e agora esforços coordenados estão sendo feitos para aproveitar essa tecnologia e tirar vantagem dos benefícios que ela pode fornecer.

**Poder de computação**

A descentralização da computação ou do poder de processamento é alcançada por uma tecnologia blockchain como o **Ethereum**, onde contratos inteligentes com lógica de negócios incorporada podem ser executados na rede blockchain. Outras tecnologias blockchain também fornecem plataformas de camada de processamento semelhantes, onde a lógica de negócios pode ser executada na rede de maneira descentralizada.



**Figura 2.6: Ecossistema descentralizado**

Na camada inferior, a Internet ou redes mesh fornecem uma camada de comunicação descentralizada. Na camada seguinte, uma **camada de armazenamento** usa tecnologias como o IPFS e o BigChainDB para possibilitar a descentralização. Finalmente, na próxima camada acima, podemos ver que o blockchain serve como uma **camada de processamento (computação) descentralizada**. O blockchain pode, de forma limitada, fornecer uma camada de armazenamento também, mas isso prejudica severamente a velocidade e a capacidade do sistema. Portanto, outras soluções como IPFS e BigChainDB são mais adequadas para armazenar grandes quantidades de dados de forma descentralizada. As camadas de **identidade, finanças e web** são mostradas no nível superior.

O blockchain pode fornecer soluções para várias questões relacionadas à descentralização. Um conceito relevante à identidade, conhecido como **triângulo de Zooko**, exige que o sistema de nomes em um protocolo de rede seja **seguro**, **descentralizado** e **capaz de fornecer nomes significativos e memoráveis para seres humanos**. A conjectura é que um sistema pode possuir **apenas duas dessas propriedades simultaneamente**.

No entanto, esse problema foi resolvido com o surgimento do **Namecoin**, que torna possível alcançar segurança, descentralização e nomes compreensíveis por humanos. Contudo, isso **não é uma solução perfeita**, e vem acompanhado de muitos desafios, como a **dependência dos usuários para armazenar e manter suas chaves privadas com segurança**. Isso levanta outras **questões gerais sobre a adequação da descentralização a um problema específico**.

A descentralização pode **não ser apropriada para todos os cenários**. Sistemas centralizados com reputações bem estabelecidas tendem a funcionar melhor em muitos casos. Por exemplo, plataformas de e-mail de empresas confiáveis como Google ou Microsoft oferecem **um serviço melhor** do que um cenário onde **servidores de e-mail individuais fossem hospedados de forma privada por usuários na Internet**.

Existem muitos projetos em andamento que estão desenvolvendo soluções para um sistema blockchain distribuído mais abrangente. Por exemplo, **Swarm** e **Whisper** estão sendo desenvolvidos para fornecer **armazenamento descentralizado** e **comunicação descentralizada** para o Ethereum.

Com o advento da tecnologia blockchain, agora é possível construir **versões em software de organizações físicas tradicionais**, na forma de **Organizações Descentralizadas (DOs)** e outras estruturas similares, que examinaremos em detalhes em breve.

Além disso, com o surgimento do paradigma da descentralização, diferentes **termos e palavras da moda** estão agora aparecendo na mídia e na literatura acadêmica, os quais exploraremos na próxima seção.

**Descentralização na prática**

Os conceitos a seguir merecem destaque no contexto da descentralização. A terminologia introduzida aqui é frequentemente usada na literatura sobre descentralização e suas aplicações.

**Contratos inteligentes**

Um **contrato inteligente** é um programa de software que normalmente roda em uma blockchain. Contratos inteligentes **não precisam necessariamente de uma blockchain** para rodar; no entanto, devido aos benefícios de segurança que a tecnologia blockchain oferece, ela se tornou a **plataforma descentralizada padrão de execução para contratos inteligentes**.

Um contrato inteligente geralmente contém alguma lógica de negócios e uma quantidade limitada de dados. A lógica de negócios é executada se certos critérios forem atendidos. Atores ou participantes da blockchain usam esses contratos inteligentes, ou eles rodam autonomamente em nome dos participantes da rede.

Mais informações sobre contratos inteligentes serão fornecidas no **Capítulo 8, Contratos Inteligentes**.

**Agentes autônomos**

Um **Agente Autônomo (AA)** é uma entidade de software (programada de forma tradicional ou com inteligência artificial) que **atua em nome de seu proprietário** para atingir objetivos desejáveis, sem exigir nenhuma ou com mínima intervenção desse proprietário.

**Organizações descentralizadas**

**DOs** (Organizações Descentralizadas) são programas de software que rodam em uma blockchain e são baseados no modelo de organizações da vida real, com pessoas e protocolos. Uma vez que uma DO é adicionada à blockchain na forma de um contrato inteligente ou de um conjunto de contratos inteligentes, ela se torna descentralizada, e as partes interagem entre si com base no código definido dentro do software da DO.

**Organizações autônomas descentralizadas**

Assim como as DOs, uma **Organização Autônoma Descentralizada (DAO)** também é um programa de computador que roda sobre uma blockchain, e dentro dele estão embutidas regras de governança e lógica de negócios. As DAOs e DOs são **fundamentalmente a mesma coisa**. A principal diferença, entretanto, é que as DAOs são **autônomas**, o que significa que elas são **totalmente automatizadas** e contêm lógica com inteligência artificial. As DOs, por outro lado, não têm esse recurso e **dependem da entrada humana** para executar a lógica de negócios.

A blockchain do Ethereum foi pioneira na introdução das DAOs. Em uma DAO, o código é considerado a **entidade governante**, em vez de pessoas ou contratos em papel. No entanto, um **curador humano mantém esse código** e atua como avaliador de propostas para a comunidade. DAOs podem contratar prestadores de serviços externos se receberem entrada suficiente dos detentores de tokens (participantes).

O projeto DAO mais famoso é **The DAO**, que arrecadou **168 milhões de dólares** em sua fase de financiamento coletivo (*crowdfunding*). O projeto The DAO foi projetado para ser um fundo de capital de risco com o objetivo de fornecer um modelo de negócios descentralizado **sem uma única entidade como proprietária**. Infelizmente, esse projeto foi hackeado devido a um bug no código da DAO, e milhões de dólares em ether (ETH) foram desviados do projeto para uma DAO filha criada pelos hackers. Uma **mudança importante na rede (hard fork)** foi necessária na blockchain do Ethereum para reverter o impacto do ataque e iniciar a recuperação dos fundos. Esse incidente abriu o debate sobre a **segurança, qualidade e necessidade de testes rigorosos do código em contratos inteligentes** para garantir sua integridade e controle adequado. Há outros projetos em andamento, especialmente na academia, que buscam **formalizar a codificação e testes de contratos inteligentes**.

Atualmente, **DAOs não possuem status legal**, embora possam conter algum código inteligente que imponha certos protocolos e condições. No entanto, essas regras **não têm valor no sistema jurídico do mundo real**, no momento. Talvez um dia, um **Agente Autônomo** (isto é, um pedaço de código que roda sem intervenção humana), comissionado por uma agência reguladora ou de aplicação da lei, contenha regras e regulamentos que possam ser incorporados em uma DAO **com o objetivo de garantir sua integridade do ponto de vista jurídico e de conformidade**. O fato de que as DAOs são **entidades puramente descentralizadas** lhes permite operar em qualquer jurisdição. Assim, elas levantam uma **grande questão sobre como o sistema legal atual pode ser aplicado a tal mistura variada de jurisdições e geografias**.

**Corporações autônomas descentralizadas**

Uma **Corporação Autônoma Descentralizada (DAC)** é semelhante a uma DAO em conceito, embora seja considerada um **subconjunto** delas. As definições de DACs e DAOs às vezes se sobrepõem, mas a distinção geral é que **DAOs são geralmente consideradas sem fins lucrativos**, enquanto **DACs podem gerar lucro** por meio de ações oferecidas aos participantes, aos quais podem pagar dividendos. As DACs podem **operar um negócio automaticamente, sem intervenção humana**, com base na lógica programada nelas.

**Sociedades autônomas descentralizadas**

Uma **Sociedade Autônoma Descentralizada (DAS)** é **uma sociedade inteira** que pode funcionar sobre uma blockchain com a ajuda de múltiplos contratos inteligentes complexos e uma combinação de **DAOs** e **aplicações descentralizadas (DApps)** operando de forma autônoma. Esse modelo **não necessariamente se traduz em uma abordagem libertária radical**, nem é baseado inteiramente em uma ideologia libertária; em vez disso, **muitos serviços que normalmente são oferecidos por um governo** podem ser entregues por meio de blockchains, como sistemas de identidade governamental, passaportes e registros de escrituras, casamentos e nascimentos. Outra teoria é que, **se um governo é corrupto** e **sistemas centrais não oferecem os níveis de confiança que uma sociedade precisa**, então essa sociedade pode iniciar sua **própria versão virtual** sobre uma blockchain, conduzida por **consenso descentralizado** e **transparência**. Esse conceito pode parecer um sonho libertário ou de um **cypherpunk**, mas é totalmente possível em uma blockchain.

Esse conceito também entra no **reino da algocracia**, uma forma alternativa de governança e sistema social onde **algoritmos computacionais mantêm, controlam e automatizam serviços públicos**, como leis, sistema jurídico, regulação, governança, economia, políticas e tomada de decisões públicas. Blockchain e DApps são meios muito adequados para **viabilizar a algocracia**, especialmente quando combinados com **inteligência artificial**. Inicialmente, a IA (ou até mesmo software tradicionalmente programado) era vista como forma de permitir a governança algorítmica; agora, **blockchain combinado com IA** pode oferecer uma abordagem mais elegante.

Entretanto, há **tanto oportunidades quanto ameaças** associadas à algocracia. O aumento da dependência da governança por algoritmos é visto como uma **ameaça à participação humana ativa** e à **tomada de decisões na vida real**. Isso é verdade na algocracia tradicional, sem blockchain. No entanto, quando combinada com blockchain, a situação melhora. Devido ao modelo descentralizado e governado pela comunidade do blockchain, **os algoritmos de governança também estão sujeitos à aprovação e escrutínio da comunidade (sociedade)** que opera na blockchain. Portanto, o blockchain pode ser visto como uma **solução para essa ameaça de perda de controle do processo decisório**. Podemos chamar essa variação da algocracia de **"blockcracia"**, ou seja, **governo por blockchain**, seguindo a visão de uma blockchain executando contratos inteligentes com inteligência artificial (algoritmos) responsáveis pela governança.

**Aplicações descentralizadas**

Todas as ideias mencionadas até este ponto estão sob o guarda-chuva mais amplo das **aplicações descentralizadas**, abreviadas como **DApps** (pronunciado *Di-Épi*, ou mais comumente rimando com *app*). DAOs, DACs e DOs são **DApps** que rodam sobre uma blockchain em uma rede ponto a ponto (*peer-to-peer*). Elas representam o mais recente avanço na tecnologia de descentralização.

As DApps, em um nível fundamental, são programas de software que são executados utilizando um dos seguintes métodos. Elas são categorizadas como **DApps do Tipo 1, Tipo 2 ou Tipo 3**:

* **Tipo 1**: Essas rodam em sua própria blockchain dedicada, por exemplo, DApps padrão baseadas em contratos inteligentes rodando no Ethereum. Se necessário, elas fazem uso de um token nativo, como o **ETH** na blockchain Ethereum. Um exemplo é o **Ethlance**, que usa ETH para fornecer um mercado de trabalho.
* **Tipo 2**: Essas usam uma blockchain estabelecida existente. Isto é, elas fazem uso de uma blockchain do Tipo 1 e têm protocolos e tokens personalizados. Por exemplo, **DAI**, que é construído sobre a blockchain Ethereum, mas contém suas **próprias stablecoins** e mecanismos de distribuição e controle. Outro exemplo é o **Golem**, que tem seu próprio token **GNT** e uma estrutura de transações construída sobre a blockchain Ethereum para fornecer um mercado descentralizado de **poder computacional**, onde os usuários compartilham poder computacional entre si em uma rede ponto a ponto. Um exemplo de DApp do Tipo 2 é a **rede OMNI**, que é uma camada de software construída sobre o Bitcoin para suportar a negociação de ativos digitais personalizados e moedas digitais.
* **Tipo 3**: Usam os protocolos das DApps do Tipo 2; por exemplo, a **SAFE Network** usa o protocolo da rede OMNI.

Outro exemplo para entender a diferença entre os diferentes tipos de DApps é o token **USDT (Tether)**. O USDT original usa a **camada OMNI** (uma DApp do Tipo 2) sobre a rede Bitcoin. O USDT também está disponível no Ethereum usando **tokens ERC-20**. Esse exemplo mostra que o USDT pode ser considerado uma **DApp do Tipo 3**, onde é usado o protocolo da camada OMNI (uma DApp do Tipo 2), que por sua vez é construída sobre o Bitcoin (uma DApp do Tipo 1). Além disso, sob a perspectiva do Ethereum, o USDT também pode ser considerado uma DApp do Tipo 3, pois utiliza a blockchain Ethereum do Tipo 1 por meio do padrão ERC-20.

Mais informações sobre o **Ethlance** podem ser encontradas em: <https://ethlance.com>

Mais informações sobre a **rede OMNI** podem ser encontradas em: <https://www.omnilayer.org>  
Mais informações sobre a **rede Golem** estão disponíveis em: <https://golem.network>  
Mais informações sobre o **DAI** estão disponíveis em: <https://makerdao.com/en>  
Mais informações sobre a **SAFE Network** podem ser encontradas em: <https://safenetwork.tech>  
Mais informações sobre o **Tether (USDT)** podem ser encontradas em: <https://tether.to>

Nos últimos anos, o termo **DApp** tem sido usado cada vez mais para se referir a qualquer aplicação blockchain descentralizada ponta a ponta, incluindo uma interface de usuário (geralmente uma interface web), contratos inteligentes e a blockchain hospedeira. A distinção clara entre os diferentes tipos de DApps agora não é comumente referida, mas ela **ainda existe**. Frequentemente, **nenhuma referência ao tipo é feita**, e todas são simplesmente chamadas de **DApps**.

Existem milhares de DApps diferentes rodando em várias plataformas (blockchains) atualmente. Há diversas categorias dessas DApps, abrangendo **mídia, redes sociais, finanças, jogos, seguros e saúde**. Existem diversas plataformas descentralizadas (ou blockchains), como **Ethereum, Solana, Avalanche, Polkadot e EOS**. Algumas estatísticas sobre DApps estão disponíveis em:  
<https://thedapplist.com>

**Critérios para uma DApp**

Para que uma aplicação seja considerada descentralizada, ela deve atender aos seguintes critérios:

* **Descentralizada**: A DApp deve ser **totalmente descentralizada**. Em outras palavras, nenhuma entidade única deve estar no controle de suas operações. Todas as mudanças na aplicação devem ser guiadas por consenso, com base na visão da comunidade.
* **Código aberto (open source)**: Ela deve ser de código aberto, para **escrutínio público e transparência**.
* **Segura criptograficamente**: A transição de estado e os dados da aplicação devem ser **criptograficamente protegidos** e armazenados em uma blockchain, para evitar qualquer ponto central de falha. Note que os dados **não precisam necessariamente ser criptografados** para prover confidencialidade, mas devem ser protegidos contra manipulação não autorizada. Devem ser fornecidos serviços de **integridade de dados, autenticação e não repúdio**.
* **Disponibilidade de incentivo**: Um **token criptográfico** deve ser usado pela aplicação para fornecer **acesso e incentivos àqueles que contribuem com valor** para as aplicações — por exemplo, os mineradores no Bitcoin. Esse requisito pode ser flexibilizado em uma cadeia de consórcio, onde um token ainda pode ser usado para **transferência de valor**, mas **não como uma criptomoeda**.
* **Prova de valor**: Os tokens (se aplicável) devem ser **gerados pela aplicação descentralizada** usando consenso e um algoritmo criptográfico aplicável. Essa geração de tokens atua como **prova de valor para os contribuidores** (por exemplo, mineradores).

Em geral, DApps atualmente fornecem todos os tipos de serviços diferentes, incluindo, mas não se limitando a, aplicações financeiras, jogos, redes sociais e gestão da cadeia de suprimentos.

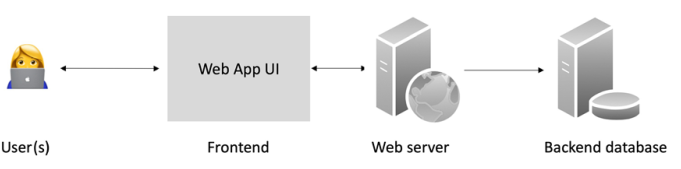
**Operações de uma DApp**

O estabelecimento de consenso por uma DApp pode ser alcançado usando **algoritmos de consenso**, como **Proof of Work (PoW)** e **Proof of Stake (PoS)**. Até agora, apenas o PoW se mostrou incrivelmente resistente a ataques, como é evidente pela confiança que as pessoas depositaram na rede Bitcoin, juntamente com seu sucesso. Além disso, uma DApp pode **distribuir tokens (moedas)** por meio de **mineração**, **financiamento coletivo (fundraising)** e **desenvolvimento**.

**Design de uma DApp**

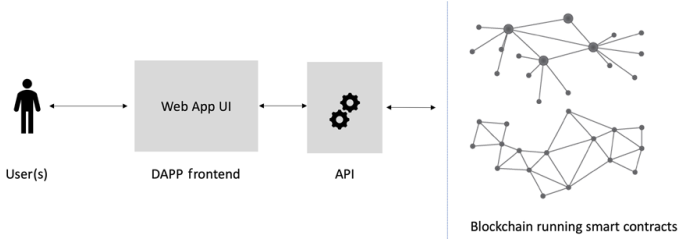
Uma DApp é uma **aplicação de software que roda sobre uma rede descentralizada**, como um livro-razão distribuído. Elas se tornaram recentemente muito populares devido ao desenvolvimento de várias **plataformas descentralizadas**, como **Ethereum, Solana, EOS e Tezos**.

As aplicações tradicionais geralmente consistem em uma interface de usuário e, normalmente, um servidor web ou um servidor de aplicações e um banco de dados de backend. Esta é uma **arquitetura cliente/servidor comum**. Isso é visualizado no seguinte diagrama:



**Figura 2.7: Arquitetura de aplicação tradicional (cliente/servidor genérica)**

Uma DApp, por outro lado, tem uma **blockchain como backend** e pode ser visualizada conforme mostrado no diagrama a seguir. O elemento-chave que desempenha um papel vital na criação de uma DApp é um **contrato inteligente que roda na blockchain** e que possui lógica de negócios incorporada:



**Figura 2.8: Arquitetura genérica de uma DApp**

Note que o frontend em uma DApp pode ser **um cliente pesado, um aplicativo móvel ou uma interface web**. Contudo, **geralmente é uma interface web**, escrita comumente usando um framework JavaScript como **React** ou **Angular**.

A tabela comparativa a seguir destaca as propriedades principais e as diferenças entre esses diferentes tipos de entidades descentralizadas:

| **Entidade** | **Autônoma?** | **Software?** | **Possui proprietário?** | **Capital?** | **Status legal?** | **Custo** |
| --- | --- | --- | --- | --- | --- | --- |
| DO | Não | Não | Sim | Sim | Sim | Alto |
| DAO | Sim | Sim | Não | Sim | Algum trabalho já começou | Baixo |
| DAC | Sim | Sim | Sim | Sim | Indefinido | Baixo |
| DAS | Sim | Sim | Não | Possível | Indefinido | Baixo |
| DApp | Sim | Sim | Sim | Tokens opcionais | Indefinido (dependente do caso de uso) | Variável |

Espera-se que **todas essas entidades sejam reguladas** e venham a possuir algum **reconhecimento legal** no futuro, **enquanto permanecem descentralizadas**.

Qualquer rede blockchain, como **Bitcoin, Ethereum, Solana, Hyperledger Fabric ou Quorum**, pode servir como uma **plataforma de descentralização sobre a qual DApps podem ser construídas e hospedadas**.

Devido à inovação acelerada e à evolução do blockchain, muitas tendências inovadoras surgiram, as quais exploraremos na próxima seção.

**Tendências inovadoras**

Com o crescimento do blockchain, surgiram várias ideias que fazem uso do aspecto de **descentralização** do blockchain para fornecer serviços mais centrados no usuário e totalmente descentralizados. Algumas das principais ideias nesse espaço são:

* **Web descentralizada**
* **Identidade descentralizada**
* **Finanças descentralizadas (DeFi)**

**Web descentralizada**

**Web descentralizada** é um termo usado para descrever uma visão da web onde **nenhuma autoridade central** ou **conjunto de autoridades** estará no controle. A intenção original da Internet era, de fato, ser descentralizada, e o desenvolvimento de protocolos abertos como **HTTP**, **SMTP** e **DNS** significava que qualquer indivíduo poderia usar esses protocolos livremente e, imediatamente, se tornar parte da Internet. Isso ainda é verdade; no entanto, com o surgimento de uma camada acima desses protocolos, chamada de **camada Web**, foi introduzida uma infraestrutura mais orientada a serviços, o que inevitavelmente levou a **grandes empresas com fins lucrativos assumirem o controle**. Isso é evidente com a ascensão de **Facebook, Google, Twitter e Amazon**, que, é claro, fornecem excelentes serviços ao usuário, mas ao **custo de um sistema mais controlado, centralizado e fechado**.

Protocolos originalmente concebidos como **descentralizados, abertos e gratuitos** estão agora sendo dominados por **poderosas entidades comerciais** ao redor do mundo, o que resultou em grandes preocupações em relação à **privacidade e proteção de dados**. Esses modelos de negócios funcionam bem e são bastante populares devido ao alto nível de padronização e aos serviços fornecidos, mas representam uma **ameaça à privacidade e à descentralização** devido à dominação de apenas um punhado de entidades sobre toda a Internet.

Com o blockchain, acredita-se que essa situação irá mudar, pois ele **permitirá o desenvolvimento da Internet descentralizada**, ou **web descentralizada**, ou ainda **Web 3**, que era a intenção original da Internet.

Podemos revisar a evolução da Web ao longo das últimas décadas dividindo os principais desenvolvimentos em três etapas principais: **Web 1, Web 2 e Web 3**.

**Web 1**

Esta é a **Web Mundial original**, que foi desenvolvida em 1989. Esta foi a era em que páginas web **estáticas** eram hospedadas em servidores e geralmente **permitiam apenas ações de leitura** do ponto de vista do usuário.

**Web 2**

Esta é a era em que **aplicações orientadas a serviços e hospedadas na web** começaram a surgir, por volta de 2003. Sites de **e-commerce**, **redes sociais**, **mídias sociais**, **blogs**, **compartilhamento de multimídia**, **mashups** e **aplicações web** são as principais características desse período. A web atual é a **Web 2**, e embora tenhamos uma Internet mais rica e interativa, **todos esses serviços ainda são centralizados**. A Web 2 gerou **enorme valor econômico** e fornece serviços que são essenciais para negócios diários, uso pessoal, interações sociais e praticamente todos os aspectos da vida. No entanto, preocupações com a **privacidade**, a **necessidade de terceiros confiáveis** e **vazamentos de dados** são questões reais que precisam ser abordadas. Exemplos comuns de serviços centralizados da Web 2 incluem **Twitter, Facebook, Google Docs** e serviços de e-mail como **Gmail e Hotmail**.

**Web 3**

Esta é a visão da **Internet descentralizada** ou **web** que irá revolucionar a maneira como usamos a Internet hoje. Esta é a era que será **totalmente centrada no usuário** e **descentralizada**, sem qualquer autoridade única, grande organização ou empresa de Internet no controle. Alguns exemplos da Web 3 são os seguintes:

* **Steemit**: Uma plataforma de mídia social baseada na blockchain **Steem** e na criptomoeda **STEEM**. Essa criptomoeda é concedida aos colaboradores pelo conteúdo que compartilham, e quanto mais votos recebem, mais tokens ganham. Mais informações em: <https://steemit.com>
* **Status**: Uma plataforma de comunicação descentralizada e multifuncional que fornece comunicação **segura e privada**. Mais informações em: <https://status.im>
* **IPFS**: Um protocolo de hipermídia/armazenamento ponto a ponto que permite **armazenar e compartilhar dados de forma descentralizada** em uma rede ponto a ponto. Mais informações em: <https://ipfs.io>

Outros exemplos incluem o **OpenSea**, um mercado para negociação de NFTs; **UniSwap**, uma exchange descentralizada de criptomoedas; e **Augur**, uma exchange descentralizada de previsões. Na Web 3, **mundos virtuais em 3D**, chamados de **metaversos**, provavelmente serão amplamente utilizados.

Outras aplicações empolgantes e de rápido crescimento incluem **identidade descentralizada** e **finanças descentralizadas (DeFi)**, que serão introduzidas em capítulos posteriores deste livro.

**Resumo**

Este capítulo introduziu o conceito de **descentralização**, que é o principal serviço oferecido pela tecnologia blockchain. Embora o conceito de descentralização não seja novo, ele ganhou um significado renovado no mundo do blockchain. Como tal, várias aplicações baseadas em uma arquitetura descentralizada foram recentemente introduzidas.

O capítulo começou com uma introdução ao conceito de descentralização. Em seguida, foi discutida a descentralização sob a **perspectiva do blockchain**. Além disso, foram apresentadas ideias relacionadas às diferentes **camadas de descentralização no ecossistema blockchain**. Vários novos conceitos e termos surgiram com o advento da tecnologia blockchain e da descentralização sob essa perspectiva, incluindo **DAOs**, **DACs** e **DApps**. Por fim, algumas **tendências inovadoras** relacionadas às DApps foram apresentadas. Também tocamos nos conceitos de **algocracia** e **blockcracia**.

**No próximo capítulo**

No próximo capítulo, serão apresentados **conceitos fundamentais necessários para entender a tecnologia blockchain** — principalmente a **criptografia**, que fornece uma base crucial para a tecnologia blockchain.

**Participe do nosso Discord!**

Para participar da comunidade do Discord deste livro — onde você pode compartilhar feedback, fazer perguntas ao autor e saber sobre novos lançamentos — siga o código QR abaixo:

<https://packt.link/ips2H>