**Capítulo 22: Aplicações da Blockchain e O que Vem a Seguir**

A tecnologia blockchain está evoluindo rapidamente e continuará a afetar a maneira como conduzimos nossos negócios do dia a dia à medida que novos desenvolvimentos surgem. Ela desafiou os modelos de negócios existentes e prometeu grandes benefícios, como economia de custos, eficiência e transparência. Até agora, neste livro, exploramos os fundamentos técnicos da tecnologia blockchain, como criptografia, mecanismos de consenso e conceitos de sistemas distribuídos.

Este capítulo explorará alguns casos de uso e aplicações da tecnologia blockchain na Internet das Coisas (IoT) e nos setores financeiro, governamental e de mídia, e aprenderemos como a tecnologia blockchain pode enfrentar desafios nessas indústrias e em outras. Além disso, aprenderemos sobre os desenvolvimentos mais recentes, tendências emergentes, questões e previsões futuras relacionadas à tecnologia blockchain. Também apresentaremos alguns tópicos relacionados a problemas de pesquisa em aberto e melhorias para a tecnologia blockchain. Ao longo do caminho, abordaremos os seguintes tópicos principais:

* Casos de uso, incluindo IoT, governo, saúde e Inteligência Artificial (IA)
* Algumas tendências emergentes
* Alguns desafios

**Casos de uso**  
As moedas digitais foram a primeira aplicação da tecnologia blockchain, que, argumentavelmente, não realizou todo o potencial da tecnologia. Embora o Bitcoin, a primeira grande conceituação de blockchain, tenha sido introduzido em 2008, foi apenas anos depois que as possíveis aplicações da tecnologia blockchain além das criptomoedas foram percebidas. Em 2010, começou a discussão sobre o BitDNS, um sistema de nomes descentralizado para domínios na internet.

Depois, o Namecoin (<https://en.bitcoinwiki.org/wiki/Namecoin>) foi iniciado em abril de 2011 com uma visão diferente da do Bitcoin, cujo único propósito era fornecer dinheiro eletrônico. Isso pode ser considerado o primeiro exemplo de uso da blockchain além do uso puramente como uma criptomoeda.

<https://en.bitcoinwiki.org/wiki/Namecoin>

Em seguida, em 2013, surgiu a primeira Oferta Inicial de Moedas (ICO), o MasterCoin, que abriu caminho para mais ICOs. Depois disso, a ICO do Ethereum foi extremamente bem-sucedida. Com a disponibilidade do Ethereum em 2015, uma plataforma de contratos inteligentes de propósito geral, mais ideias começaram a surgir em torno de várias aplicações da tecnologia blockchain. Desde então, muitos casos de uso da tecnologia blockchain em várias indústrias foram propostos. Neste capítulo, cinco indústrias principais foram selecionadas devido à sua popularidade e promissores casos de uso da blockchain para discussão:

* IoT
* Governo
* Saúde
* Mídia

Vamos começar com um dos casos de uso mais empolgantes da tecnologia blockchain: a IoT.

**IoT**

A IoT ganhou recentemente muita atenção devido ao seu potencial de transformar aplicações comerciais e a vida cotidiana. A IoT pode ser definida como uma rede de objetos físicos computacionalmente inteligentes (quaisquer objetos, como carros, geladeiras e sensores industriais) que são capazes de se conectar à internet, detectar eventos ou ambientes do mundo real, reagir a esses eventos, coletar dados relevantes e comunicar isso pela internet.

Essa definição simples tem enormes implicações e levou a conceitos empolgantes, como dispositivos vestíveis (como rastreadores de saúde ou relógios), casas inteligentes, redes elétricas inteligentes, carros conectados inteligentes e cidades inteligentes, que são todos baseados nesse conceito básico de um dispositivo de IoT. Uma coisa a se notar é que todos esses componentes são acessíveis e controláveis pela internet, via IoT.

Após dissecar a definição de IoT, quatro funções surgem como sendo desempenhadas por um dispositivo de IoT: detecção, reação, coleta e comunicação. Todas essas funções são realizadas por meio de vários componentes no dispositivo de IoT. A detecção é realizada por sensores. A reação ou controle é realizada por atuadores; a coleta é a função de vários sensores; e a comunicação é realizada por chips que fornecem conectividade de rede.

Na próxima seção, apresentaremos a arquitetura típica de um ecossistema baseado em IoT.

**Arquitetura da IoT**

Uma arquitetura típica de IoT pode consistir em muitos objetos físicos conectados entre si e a um servidor centralizado na nuvem. Isso é mostrado na figura a seguir:

<IMAGEM>

**Figura 22.1: Uma rede típica de IoT**

Os elementos da IoT estão distribuídos em várias camadas, e várias arquiteturas de referência existentes podem ser usadas para desenvolver sistemas de IoT. Um modelo de cinco camadas pode ser usado para descrever a IoT, que contém uma camada de objetos físicos, uma camada de dispositivos, uma camada de rede, uma camada de serviços e uma camada de aplicação. Cada camada ou nível é responsável por várias funções e inclui vários componentes. Estes são mostrados na figura a seguir:

* Camada de Aplicação  
  Transporte, financeiro, seguros e muitos outros
* Camada de Gerenciamento  
  Processamento de dados, análises, gerenciamento de segurança
* Camada de Rede  
  LAN, WAN, PAN, roteadores
* Camada de Dispositivo  
  Sensores, atuadores, dispositivos inteligentes
* Objetos Físicos  
  Pessoas, carros, casas

<IMAGEM>

**Figura 22.2: Modelo em camadas da IoT**

Agora, vamos examinar cada camada em detalhe.

**A camada de objetos físicos**

Essa camada inclui quaisquer objetos físicos do mundo real. Inclui objetos como carros, geladeiras, trens e casas. De fato, qualquer coisa que precise ser monitorada e controlada pode ser conectada à IoT.

**A camada de dispositivos**

Essa camada contém os elementos que compõem a IoT, como sensores, transdutores, atuadores, smartphones, dispositivos inteligentes e etiquetas RFID (Identificação por Radiofrequência). Pode haver muitas categorias de sensores, como sensores corporais, sensores domésticos e sensores ambientais, com base no tipo de trabalho que realizam. Essa camada é o núcleo do ecossistema da IoT, onde vários sensores são usados para detectar ambientes do mundo real. Essa camada inclui sensores que podem monitorar temperatura, umidade, fluxo de líquidos, produtos químicos, ar, pressão e muito mais. Normalmente, é necessário um Conversor Analógico para Digital (ADC) para que um dispositivo converta o sinal analógico do mundo real em um sinal digital que um microprocessador possa entender.

Os atuadores nessa camada fornecem os meios para permitir o controle de ambientes externos; por exemplo, ligar um motor ou abrir uma porta. Esses componentes também requerem conversores digital-para-analógico para converter um sinal digital em analógico. Esse método é especialmente relevante quando o controle de um componente mecânico é necessário por meio do dispositivo de IoT.

**A camada de rede**

Essa camada é composta por vários dispositivos de rede que são usados para fornecer conectividade com a internet entre os dispositivos e a nuvem, ou servidores que fazem parte do ecossistema da IoT. Esses dispositivos podem incluir gateways, roteadores, hubs e switches. Essa camada pode incluir dois tipos de comunicação:

Primeiro, existem os meios horizontais de comunicação, que incluem rádio, Bluetooth, Wi-Fi, Ethernet, LANs, Zigbee e PANs, e podem ser usados para fornecer comunicação entre dispositivos de IoT. Essa camada pode ser opcionalmente incluída na camada de dispositivos, pois reside fisicamente na camada de dispositivos, onde os dispositivos podem se comunicar entre si.

Segundo, temos a comunicação com a próxima camada, que geralmente é feita pela internet e fornece comunicação entre máquinas e pessoas ou outras camadas superiores.

**A camada de gerenciamento**

Essa camada fornece o gerenciamento do ecossistema da IoT. Isso inclui plataformas que processam dados coletados de dispositivos de IoT e os transformam em percepções significativas. Gerenciamento de dispositivos, gerenciamento de segurança e gerenciamento de fluxo de dados estão incluídos nessa camada. Ela também gerencia a comunicação entre as camadas de dispositivos e de aplicação.

**A camada de aplicação**

Essa camada inclui as aplicações executadas sobre a rede de IoT. Essa camada pode consistir em muitas aplicações, dependendo dos requisitos, como tarefas de transporte, saúde, finanças, seguros ou gerenciamento da cadeia de suprimentos. Essa lista, é claro, não é exaustiva de forma alguma; há uma infinidade de aplicações de IoT que podem se encaixar nessa camada.

**Com a disponibilidade de sensores baratos, hardware e largura de banda, a IoT ganhou popularidade nos últimos anos e atualmente tem aplicações em muitas áreas diferentes, incluindo saúde, seguros, gerenciamento da cadeia de suprimentos, automação residencial, automação industrial e gerenciamento de infraestrutura. Além disso, avanços em tecnologias como a disponibilidade do IPv6, processadores menores e mais potentes e melhor acesso à internet também desempenharam um papel vital na popularidade da IoT.**

Na próxima seção, discutiremos algumas vantagens da convergência entre IoT e blockchain.

**Vantagens da convergência entre IoT e blockchain**

Os benefícios da IoT com tecnologia blockchain variam desde economia de custos até permitir que empresas tomem decisões vitais e, assim, melhorem o desempenho com base nos dados fornecidos pelos dispositivos de IoT. Mesmo no uso doméstico, aparelhos equipados com IoT podem fornecer dados valiosos para economia de custos. Por exemplo, medidores inteligentes para monitoramento de energia podem fornecer informações valiosas sobre como a energia está sendo usada e podem transmitir isso de volta ao provedor de serviços. Dados brutos de milhões de dispositivos IoT são analisados e fornecem percepções significativas que ajudam na tomada de decisões comerciais oportunas e eficientes.

O modelo usual da IoT é baseado em um paradigma centralizado, onde os dispositivos de IoT normalmente se conectam a uma infraestrutura de nuvem ou servidores centrais para relatar e processar os dados relevantes. Essa centralização é, de certa forma, vulnerável à exploração, incluindo invasões e roubo de dados. Além disso, não ter controle dos dados pessoais com um único provedor de serviços centralizado também aumenta a possibilidade de problemas de segurança e privacidade. Embora existam métodos e técnicas para construir um ecossistema de IoT altamente seguro com base no modelo normal de IoT, há benefícios muito mais específicos e desejáveis que um modelo baseado em blockchain pode trazer para a IoT.

A tecnologia blockchain para a IoT pode ajudar a construir confiança, reduzir custos e acelerar transações. Além disso, a descentralização, que está no cerne da tecnologia blockchain, pode eliminar pontos únicos de falha em uma rede de IoT. Por exemplo, um servidor central pode não conseguir lidar com a quantidade de dados que bilhões de dispositivos IoT (coisas) produzem em alta frequência, enquanto uma blockchain descentralizada atuando como camada de comunicação entre esses dispositivos permite que todos os dispositivos na blockchain mantenham uma cópia própria do armazenamento de dados, o que significa que essa arquitetura é inerentemente altamente disponível e resiliente.

Alguns dispositivos de IoT perderem seus bancos de dados não resulta na paralisação de toda a rede, como pode ser o caso de um servidor centralizado, mesmo com uma solução de recuperação de desastres. Além disso, o modelo de comunicação ponto-a-ponto (P2P) fornecido pela tecnologia blockchain pode ajudar a reduzir custos, pois não há necessidade de construir centros de dados centralizados de alto custo ou implementar uma infraestrutura de chave pública complexa para segurança. Os dispositivos podem se comunicar diretamente entre si ou via roteadores.

O IPv6 é a versão mais recente do protocolo da internet, que, com um tamanho de 128 bits, oferece mais espaço de endereçamento comparado aos 32 bits do IPv4.

De acordo com estimativas feitas por vários pesquisadores e empresas, até 2025, haverá aproximadamente 41 bilhões de dispositivos conectados à internet. Com essa explosão de bilhões de dispositivos conectando-se à internet, é difícil imaginar que infraestruturas centralizadas conseguirão lidar com as altas demandas de largura de banda, serviços e disponibilidade sem incorrer em gastos excessivos. Um modelo de IoT baseado em blockchain será capaz de resolver problemas de escalabilidade, disponibilidade, privacidade e confiabilidade no modelo atual de IoT.

A tecnologia blockchain permite que as coisas se comuniquem e realizem transações entre si diretamente e, com a disponibilidade de contratos inteligentes, negociações e transações financeiras também podem ocorrer diretamente entre dispositivos em vez de exigir um intermediário, uma autoridade ou intervenção humana. Por exemplo, se um quarto em um hotel estiver vago, ele pode se alugar sozinho, negociar o aluguel e abrir a fechadura da porta para um humano que tenha pago a taxa exigida. Outro exemplo poderia ser: se uma máquina de lavar ficar sem detergente, ela poderia fazer um pedido online após encontrar o melhor preço e valor com base na lógica programada em seu contrato inteligente.

O modelo de cinco camadas da IoT mencionado anteriormente pode ser adaptado a um modelo baseado em blockchain adicionando uma camada de blockchain sobre a camada de rede. Essa camada executará contratos inteligentes e fornecerá serviços de segurança, privacidade, integridade, autonomia, escalabilidade e descentralização para o ecossistema de IoT. A camada de gerenciamento, nesse caso, consistirá apenas em software relacionado a análises e processamento, e a segurança e o controle podem ser movidos para a camada de blockchain.

Esse novo modelo com seis camadas é visualizado na tabela a seguir:

* **Camada de Aplicação**  
  Transporte, finanças, seguros e muitos outros domínios
* **Camada de Gerenciamento**  
  Processamento de dados, análises, gerenciamento de segurança
* **Camada de Blockchain**  
  Segurança, consenso, transações autônomas ponto-a-ponto (máquina a máquina), descentralização, contratos inteligentes
* **Camada de Rede**  
  LAN, WAN, PAN, roteadores
* **Camada de Dispositivo**  
  Sensores, atuadores, dispositivos inteligentes
* **Objetos Físicos**  
  Pessoas, carros, casas

<IMAGEM>

**Figura 22.3: Modelo em camadas de IoT baseado em blockchain**

Nesse modelo, espera-se que as outras camadas permaneçam as mesmas, mas uma camada adicional de blockchain será introduzida como middleware entre todos os participantes da rede de IoT.

Também pode ser visualizado como uma rede de IoT ponto-a-ponto (P2P) após abstrair todas as camadas mencionadas anteriormente. Esse modelo é mostrado na figura a seguir, onde todos os dispositivos estão se comunicando e negociando entre si sem uma entidade central de comando e controle:

<IMAGEM>

**Figura 22.4: Modelo de comunicação direta baseada em blockchain (P2P ou máquina a máquina)**

Uma blockchain baseada em IoT também pode resultar em economia de custos devido ao gerenciamento mais fácil dos dispositivos oferecido por uma abordagem descentralizada baseada em blockchain. A rede IoT também pode ser otimizada para desempenho utilizando a tecnologia blockchain. Nesse caso, não haverá necessidade de armazenar dados de IoT centralmente para milhões de dispositivos. Isso ocorre porque os requisitos de armazenamento e processamento podem ser distribuídos entre todos os dispositivos de IoT na blockchain. Isso pode resultar na eliminação completa da necessidade de grandes centros de dados para processar e armazenar dados de IoT.

Uma IoT baseada em blockchain também pode frustrar ataques de negação de serviço (DoS): hackers podem atacar com mais eficiência um servidor centralizado ou centro de dados, mas com a natureza distribuída e descentralizada da blockchain, tais ataques deixam de ser possíveis. Além disso, se, conforme estimado, em breve houver bilhões de dispositivos conectados à internet, tornar-se-á quase impossível gerenciar a segurança e atualizações para todos esses dispositivos a partir de servidores tradicionais de propriedade centralizada. A tecnologia blockchain pode fornecer uma solução para esse problema ao permitir que os dispositivos se comuniquem diretamente entre si de forma segura, e até mesmo solicitem atualizações de firmware e segurança uns dos outros. Em uma rede blockchain, essas comunicações podem ser registradas de maneira imutável e segura, o que fornecerá auditabilidade, integridade e transparência ao sistema. Esse mecanismo não é possível em sistemas P2P tradicionais.

Em resumo, há benefícios claros que podem ser colhidos devido à convergência entre IoT e blockchain, e muitas pesquisas e trabalhos acadêmicos e industriais já estão em andamento. Casos de uso práticos e plataformas surgiram na forma de Plataforma como Serviço (PaaS) para IoT baseada em blockchain, como o IBM Watson IoT blockchain. Existem vários projetos que já foram propostos que fornecem soluções de IoT baseada em blockchain, como IBM Blue Horizon e IBM Bluemix, dois exemplos de plataformas de IoT que suportam IoT com blockchain. Diversas startups, como a Filament, já propuseram ideias inovadoras sobre como construir uma rede descentralizada que permite que os dispositivos da IoT transacionem entre si diretamente e de forma autônoma, impulsionados por contratos inteligentes. Na próxima seção, discutiremos a implementação de um sistema de IoT baseado em blockchain.

**Implementando IoT baseada em blockchain na prática**

Na seção seguinte, é fornecido um exemplo prático de como construir um dispositivo de IoT simples e conectá-lo à blockchain do Ethereum. O dispositivo de IoT neste exemplo será conectado à blockchain do Ethereum e usado para abrir uma porta (neste caso, a fechadura da porta é representada por um Diodo Emissor de Luz — LED) quando a quantidade apropriada de fundos for enviada por um usuário. Observe que este é um exemplo simples e requer uma versão mais rigorosamente testada para ser implementada em produção.

Os componentes de hardware pré-requisitos são listados a seguir:

* Um dispositivo Raspberry Pi, que é um Computador de Placa Única (SBC). O Raspberry Pi é um SBC desenvolvido como um computador de baixo custo para promover a educação em computação, mas também ganhou muito mais popularidade como a ferramenta de escolha para construção de plataformas de IoT. Você também pode usar modelos anteriores, mas eles não foram testados. Você pode explorar mais sobre o Raspberry Pi em:  
  <https://www.raspberrypi.com/products/>
* LED: Um LED pode ser usado como indicação visual para um evento.
* Resistor: É necessário um componente de 330 ohms, que fornece resistência à corrente com base em sua classificação. Não é necessário entender a teoria por trás disso para este experimento; qualquer texto padrão de engenharia eletrônica cobre todos esses tópicos em detalhe.
* Breadboard: Isso fornece um meio de construir um circuito eletrônico sem necessidade de solda.
* Conector T-cobbler: Isso é inserido na breadboard, conforme mostrado na figura a seguir, e fornece uma visualização rotulada de todos os pinos de I/O de uso geral (GPIO) do Raspberry Pi.
* Conector de cabo flat (ribbon cable): Isso é usado simplesmente para fornecer conectividade entre o Raspberry Pi e a breadboard via GPIO.

Todos esses componentes são mostrados na figura a seguir:

<IMAGEM>

**Figura 22.5: Componentes necessários**

<https://www.raspberrypi.com/products/>

**Configurando o Raspberry Pi**

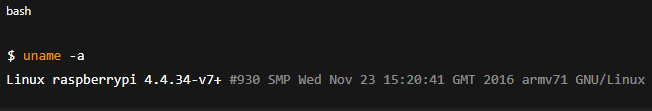
Primeiro, o Raspberry Pi precisa ser configurado. Isso pode ser feito utilizando o NOOBS (New Out Of Box Software), que fornece um método fácil de instalar o Raspbian ou qualquer outro sistema operacional.

NOOBS é um gerenciador de instalação de sistema operacional fácil de usar e amigável para o Raspberry Pi.

Para este exemplo, o NOOBS foi usado para instalar o Raspbian. Assim, o restante do exercício assume que o Raspbian está instalado no cartão de memória SD do Raspberry Pi. A saída do comando na captura de tela a seguir mostra em qual arquitetura o sistema operacional está sendo executado.

Neste caso, é o armv71; portanto, o binário compatível com ARM para o Geth será baixado.

A plataforma pode ser confirmada executando o comando uname -a em uma janela de terminal no sistema operacional Raspbian do Raspberry Pi:



Uma vez instalado o sistema operacional Raspbian, o próximo passo é baixar o binário apropriado do Geth para a plataforma ARM do Raspberry Pi.

Os passos para download e instalação são descritos detalhadamente a seguir:

1. Primeiro, baixe o binário do Geth no Raspberry Pi. Usamos wget para baixar as imagens do cliente Geth:

$ wget <https://gethstore.blob.core.windows.net/builds/geth-linux-arm7-1.5.6-2a609af5.tar.gz>

1. Descompacte e extraia isso em um diretório. O diretório chamado geth-linux-arm7-1.5.6-2a609af5 será criado automaticamente com o comando tar, como mostrado aqui:

$ tar -zxvf geth-linux-arm7-1.5.6-2a609af5.tar

O NOOBS pode ser baixado e instalado em <https://www.raspberrypi.org/downloads/noobs/>  
Alternativamente, você pode instalar apenas o Raspbian em <https://www.raspberrypi.org/downloads/raspbian/>  
Outra alternativa, disponível em <https://github.com/debian-pi/raspbian-ua-netinst>, também pode ser usada para instalar uma versão mínima (sem interface gráfica) do sistema operacional Raspbian.

Observe que, neste exemplo, uma versão específica do Geth está sendo baixada. Outras versões estão disponíveis e podem ser obtidas em <https://geth.ethereum.org/downloads/>. No entanto, recomenda-se baixar a versão utilizada nos exemplos deste capítulo.

1. Este comando criará um diretório chamado geth-linux-arm7-1.5.6-2a609af5 e extrairá o binário Geth e arquivos relacionados para esse diretório. O binário do Geth pode ser copiado para /usr/bin ou para o caminho apropriado no Raspbian para torná-lo disponível de qualquer lugar no sistema operacional. Após o término do download, o próximo passo é criar o bloco gênese.
2. O mesmo bloco gênese que foi criado anteriormente no Capítulo 10, *Ethereum na Prática*, deve ser usado. O arquivo gênese pode ser copiado de outro nó na rede. Isso é mostrado no trecho de código a seguir:



1. Uma vez que o arquivo genesis.json tenha sido copiado para o Raspberry Pi, o seguinte comando pode ser executado para gerar o bloco gênese. É importante que o mesmo bloco gênese usado anteriormente seja utilizado; caso contrário, os nós estarão efetivamente em redes separadas:

$ ./geth init genesis.json

Isso criará o bloco gênese e inicializará a cadeia.

Alternativamente, um bloco gênese inteiramente novo pode ser gerado. Os elementos do arquivo gênese foram explicados na seção “Redes privadas” do Capítulo 9, *Arquitetura do Ethereum*, ao qual você pode se referir como revisão.

1. Após a criação do bloco gênese, adicionamos pares à rede. Isso pode ser feito criando uma lista de nós na nossa rede privada. Para definir essa lista, criamos um arquivo chamado static-nodes.json usando qualquer editor de texto e adicionamos o enode do par ao qual o Geth, no Raspberry Pi, se conectará para sincronização.
2. A URL do enode pode ser obtida a partir do console JavaScript do Geth executando o seguinte comando, que deve ser executado no par ao qual o Raspberry Pi irá se conectar:

> admin.nodeInfo

1. Isso mostrará uma saída semelhante à exibida na captura de tela a seguir:

<IMAGEM>

**Figura 22.6: admin.nodeInfo do Geth**

1. O arquivo static-nodes.json deve conter o valor do enode, como mostrado na captura de tela a seguir. Podemos visualizar o conteúdo usando o comando cat:

$ cat static-nodes.json

1. Esse comando produzirá uma saída como esta:

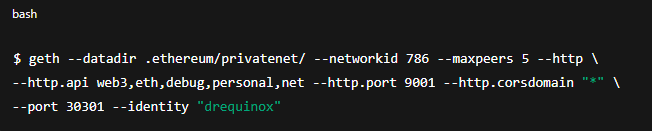
<IMAGEM>

**Figura 22.7: Configuração de nó estático**

Após esta etapa, as instruções apresentadas nas seções seguintes podem ser seguidas para conectar o Raspberry Pi ao outro nó na rede privada. Neste exemplo, o Raspberry Pi será conectado à rede com ID 786 que criamos no Capítulo 10, *Ethereum na Prática*. A chave é usar o mesmo arquivo gênese criado anteriormente e portas diferentes. Usar o mesmo arquivo gênese garantirá que os clientes se conectem à mesma rede da qual o arquivo gênese se originou. Portas diferentes não são um requisito estrito; no entanto, se os dois nós estiverem operando em uma rede privada e for necessário acesso a partir de um ambiente externo, então uma combinação de DMZ, roteador e redirecionamento de portas será utilizada. Portanto, recomenda-se o uso de diferentes portas TCP para permitir que o redirecionamento de portas funcione corretamente.

**Configurando o primeiro nó**

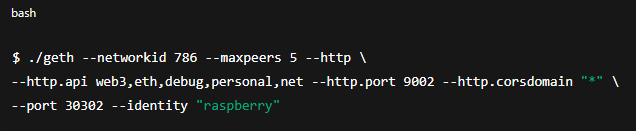
Primeiro, o cliente Geth precisa ser iniciado no primeiro nó usando o seguinte comando. O parâmetro --identity permite especificar um nome de identificação para o nó:



Isso iniciará o nó Geth. Uma vez que o nó tenha sido iniciado, ele deve ser mantido em execução, e outra instância do Geth deve ser iniciada a partir do nó Raspberry Pi.

**Configurando o nó do Raspberry Pi**

No Raspberry Pi, o seguinte comando deve ser executado para iniciar o Geth e sincronizá-lo com os outros nós (neste caso, apenas um outro nó). O comando é:



Isso deve iniciar o nó Geth no Raspberry Pi. Observe que, quando o log de saída contém uma linha exibindo *Block synchronisation started*, isso significa que o nó foi conectado com sucesso ao seu par iniciado anteriormente.

Essa conectividade pode ser verificada adicionalmente executando comandos no console Geth em ambos os nós, como mostrado na captura de tela a seguir. O cliente Geth pode ser conectado simplesmente executando o seguinte comando no Raspberry Pi:

$ geth attach

Isso abrirá o console JavaScript do Geth para interagir com o nó Geth. Podemos usar o comando admin.peers para ver os pares conectados:

<IMAGEM>

**Figura 22.8: Comando admin.peers do console Geth sendo executado no Raspberry Pi**

Da mesma forma, podemos conectar à instância Geth executando o seguinte comando no primeiro nó:

$ geth attach ipc:.ethereum/privatenet/geth.ipc

Uma vez no console, admin.peers pode ser executado para revelar os detalhes sobre os outros nós conectados, como mostrado na captura de tela a seguir:

<IMAGEM>

**Figura 22.9: Comando admin.peers do console Geth sendo executado no outro par**

**Instalando o Node.js**

As bibliotecas e dependências necessárias estão listadas aqui. Primeiro, o Node.js e o npm precisam ser atualizados no sistema operacional Raspbian do Raspberry Pi. Para isso, os seguintes passos podem ser seguidos:

1. Instale o Node.js no Raspberry Pi usando o seguinte comando:

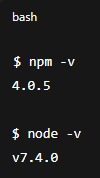
$ curl -sL https://deb.nodesource.com/setup\_7.x | sudo -E bash –

Isso deve instalar o Node.js.

1. Execute a atualização via apt-get:

$ sudo apt-get install nodejs

A verificação pode ser realizada executando o seguinte comando para garantir que as versões corretas do Node.js e do npm foram instaladas, como mostrado na captura de tela a seguir:



Observe que estamos usando a versão 7.x do Node para este exemplo, apenas para demonstração. Você pode usar uma versão mais recente, se desejar.

1. Instale o Ethereum Web3 usando o seguinte comando:

$ npm install [web3@0.18.0](mailto:web3@0.18.0)

Isso deve instalar o Web3. O Web3 é necessário para permitir que o código JavaScript acesse a blockchain do Ethereum.

Da mesma forma, o onoff pode ser instalado, que é necessário para comunicar-se com o Raspberry Pi e controlar os GPIO:

$ npm install onoff –save

1. Isso instalará o onoff.

Nesta seção, configuramos uma rede privada com nosso Raspberry Pi e outro nó com Geth, Node.js, Web3 e a biblioteca onoff para executar nosso exemplo.

Quando todos os pré-requisitos tiverem sido instalados, a configuração do hardware pode ser realizada. Para isso, um circuito simples será construído utilizando uma breadboard e alguns componentes eletrônicos.

**Construindo o circuito eletrônico**

Conforme mostrado na figura a seguir, a perna positiva (perna longa) do LED está conectada ao pino número 21 da breadboard, e a negativa (perna curta) está conectada ao resistor, que então é conectado ao pino de aterramento (GND) da breadboard. Uma vez que as conexões tenham sido feitas, o cabo flat (ribbon cable) pode ser usado para conectar ao conector GPIO no Raspberry Pi:

Deve-se observar que essas versões não são uma exigência; qualquer uma das versões mais recentes do npm e Node.js deve funcionar. No entanto, os exemplos neste capítulo utilizam o npm 4.0.5 e o node v7.4.0 apenas para demonstração, então recomenda-se que você use as mesmas versões para evitar possíveis problemas de compatibilidade.

Certifique-se de que a versão específica do Web3 mostrada no trecho, ou uma versão semelhante (por exemplo, 0.20.2), esteja instalada em vez da padrão, versão 1.2.11 (na época da escrita). Como este exemplo foi originalmente desenvolvido e testado usando a versão 0.18.0, recomenda-se que uma versão estável como 0.20.2 ou 0.18.0 do Web3 seja usada para este exemplo. O objetivo deste exemplo — demonstrar como redes de IoT baseadas em Ethereum podem ser criadas — não muda independentemente de se usar uma versão mais nova ou mais antiga do Web3. Você pode instalar a versão recomendada utilizando:

$ npm install [web3@0.20.2](mailto:web3@0.20.2)

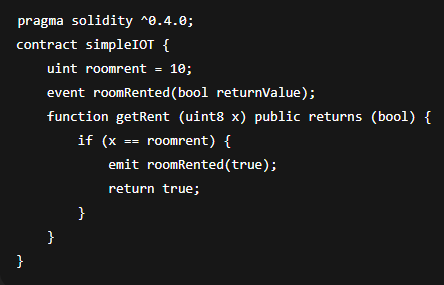
<IMAGEM>

**Figura 22.10: Conexões para os componentes na breadboard**

**Desenvolvendo e executando um contrato Solidity**

Claro, o contrato Solidity pode ser muito mais complexo e também pode lidar com o éter enviado a ele. Se a quantidade de éter for igual à quantia exigida, então o evento pode ser acionado. No entanto, neste exemplo, o objetivo é demonstrar o uso de contratos inteligentes para acionar eventos, que podem então ser lidos por um programa JavaScript em execução via Node.js, o qual, por sua vez, pode acionar ações em dispositivos IoT utilizando várias bibliotecas.

O código-fonte do contrato inteligente é mostrado a seguir:



O compilador Solidity online (o Remix IDE) pode ser usado para executar e testar este contrato. A Interface Binária de Aplicação (ABI) necessária para interagir com o contrato também está disponível na seção do compilador Solidity do Remix IDE.

A seguir está a ABI do contrato:



Existem dois métodos pelos quais o nó Raspberry Pi pode se conectar à blockchain privada via a interface web3. O primeiro é onde o dispositivo Raspberry Pi está executando seu próprio cliente Geth localmente e mantém seu próprio livro razão, conforme mostrado no diagrama a seguir:

<IMAGEM>

**Figura 22.11: Arquitetura da aplicação de IoT para aluguel de quarto  
(dispositivo IoT com livro razão local)**

Às vezes, com dispositivos com restrições de recursos, não é possível executar um nó Geth completo ou mesmo um nó leve. Nesse caso, o segundo método, que usa um provedor web3 (via um servidor HTTP-RPC), pode ser usado para se conectar ao canal RPC apropriado. O diagrama a seguir mostra a arquitetura de alto nível de uma aplicação IoT onde o Raspberry Pi não executa uma instância do Geth. Em vez disso, ele executa apenas o software mínimo necessário para fornecer funcionalidade de aplicação IoT ao dispositivo:

<IMAGEM>

**Figura 22.12: Arquitetura da aplicação de IoT para aluguel de quarto  
(dispositivo IoT sem livro razão local)**

Existem preocupações óbvias de segurança que surgem da exposição de interfaces RPC publicamente; portanto, recomenda-se que essa opção seja usada apenas em redes privadas. Caso seja necessário usá-la em redes públicas, medidas de segurança apropriadas precisam ser implementadas, como permitir apenas que endereços IP conhecidos se conectem à interface RPC do Geth. Isso pode ser alcançado por uma combinação de desativação dos mecanismos de descoberta de pares e das interfaces de escuta do servidor HTTP-RPC.

Mais informações sobre isso podem ser encontradas usando o comando geth help. Medidas de segurança tradicionais de rede, como firewalls, TLS (Transport Layer Security) e certificados, também podem ser utilizadas, mas não foram discutidas neste exemplo por brevidade. Agora, o Truffle pode ser usado para implantar o contrato na rede privada de ID 786 à qual, neste ponto, o Raspberry Pi está conectado.

O deploy via Truffle pode ser realizado simplesmente utilizando o seguinte comando; assume-se que o truffle init e outras preliminares discutidas no Capítulo 12, *Desenvolvimento Web3 usando Ethereum*, já tenham sido realizadas:

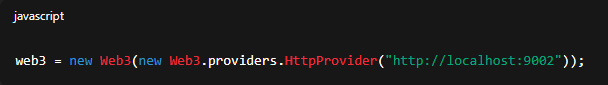
$ truffle migrate

Isso deve implantar o contrato.

Uma vez que o contrato tenha sido implantado corretamente, o código JavaScript pode ser desenvolvido para se conectar à blockchain via Web3, escutar os eventos do contrato inteligente na blockchain e acionar o LED via Raspberry Pi. O código JavaScript necessário para este exemplo está mostrado aqui. Basta escrever ou copiar e colar o código mostrado aqui em um arquivo chamado index.js:



Também observe a porta de escuta do servidor HTTP-RPC na qual o Geth foi iniciado no Raspberry Pi. Por padrão, é a porta TCP 8545. Lembre-se de alterar isso de acordo com a configuração do seu Raspberry Pi e Geth. Ela está definida como 9002 no exemplo de código acima porque o Geth em execução no Raspberry Pi está escutando na porta 9002 neste exemplo. Se estiver escutando em outra porta no seu Raspberry Pi, altere para essa porta:



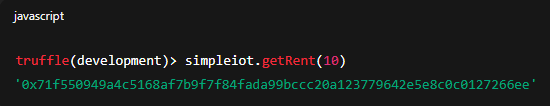
Quando o Geth for iniciado, ele mostrará em qual porta está escutando o endpoint HTTP. Isso também é configurável com a flag --http.port no Geth especificando o número da porta como parâmetro.

Este código JavaScript pode ser colocado em um arquivo no Raspberry Pi, por exemplo, index.js. Ele pode ser executado com o seguinte comando:

$ node index.js

Observe que, no exemplo de código acima, o endereço do contrato 0x975881c44fbef4573fef33cccec1777a8f76669c para a variável ContractAddress é específico do deploy; ele será diferente quando você executar este exemplo. Basta alterar o endereço no arquivo para aquele que você verá após implantar o contrato.

Isso iniciará o programa, que será executado no Node.js e escutará eventos do contrato inteligente. Uma vez que o programa esteja funcionando corretamente, o contrato inteligente pode ser invocado utilizando o console do Truffle. Neste caso, a função getRent é chamada com o parâmetro 10, que é o valor esperado:



Depois que o contrato for minerado, o evento roomRented será acionado, o que acenderá o LED.

Neste exemplo, trata-se de um LED simples, mas poderia ser qualquer dispositivo físico, como uma fechadura de porta, que pode ser controlado via atuador. Se tudo correr bem, o LED será aceso como resultado da invocação da função do contrato inteligente, como mostrado na figura a seguir:

<IMAGEM>

**Figura 22.13: Raspberry Pi com controle de LED**

Além disso, no lado do nó, será exibida uma saída semelhante à seguinte:

$ node index.js

LED On

Como demonstrado no exemplo anterior, uma rede privada de dispositivos IoT pode ser construída executando um cliente Geth em cada um dos nós, escutando eventos de contratos inteligentes e acionando uma ação de acordo. O exemplo mostrado é simples em design, mas demonstra os princípios subjacentes de uma rede Ethereum que pode ser construída utilizando dispositivos IoT, junto com controle baseado em contratos inteligentes de dispositivos físicos.

**Governo**

Há várias aplicações da tecnologia blockchain sendo pesquisadas atualmente que podem apoiar funções governamentais e levar o modelo atual de governo eletrônico (e-government) a um novo patamar. Primeiro, nesta seção, será fornecido um contexto sobre o governo eletrônico, e depois discutiremos alguns casos de uso, como votação eletrônica, segurança nacional (controle de fronteiras) e identidades eletrônicas (carteiras de identidade dos cidadãos).

Governo eletrônico, ou *e-government*, é um paradigma no qual tecnologias da informação e comunicação são utilizadas para fornecer serviços públicos aos cidadãos. O conceito não é novo e já foi implementado em vários países ao redor do mundo, mas com a tecnologia blockchain, uma nova via de exploração foi aberta. Muitos governos estão pesquisando a possibilidade de usar a tecnologia blockchain para gerenciar e fornecer serviços públicos, incluindo, mas não se limitando a, carteiras de identidade, carteiras de motorista, compartilhamento seguro de dados entre diversos departamentos governamentais e gerenciamento de contratos. Transparência, auditabilidade e integridade são atributos da tecnologia blockchain que podem contribuir significativamente para a gestão eficaz de várias funções governamentais. Uma dessas funções é o controle de fronteiras, que abordaremos a seguir.

**Controle de fronteiras**

Sistemas automatizados de controle de fronteiras estão em uso há décadas para impedir a entrada ilegal em países e prevenir o terrorismo e o tráfico humano. Documentos de viagem legíveis por máquina, especificamente passaportes biométricos, abriram caminho para o controle automatizado de fronteiras; no entanto, os sistemas atuais são limitados até certo ponto, e a tecnologia blockchain pode oferecer soluções. Um padrão de Documento de Viagem Legível por Máquina (*Machine-Readable Travel Document – MRTD*) é definido no documento 9303 da Organização da Aviação Civil Internacional (ICAO) e foi implementado por muitos países ao redor do mundo.

<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

Cada passaporte contém vários atributos de segurança e identidade que podem ser usados para identificar o proprietário do passaporte e evitar tentativas de falsificação desses documentos. Esses atributos incluem características biométricas, como escaneamento de retina, impressões digitais, reconhecimento facial, e características especificadas pelo padrão da ICAO, como a Zona Legível por Máquina (MRZ) e outros textos visíveis na primeira página do passaporte.

Um problema chave com os sistemas atuais de controle de fronteiras é o compartilhamento de dados, pois os sistemas são controlados por uma única entidade e os dados não são compartilhados prontamente entre as agências de segurança. Essa incapacidade de compartilhar dados dificulta o rastreamento de documentos de viagem ou indivíduos suspeitos. Outro problema está relacionado à implementação imediata de listas negras de documentos de viagem — por exemplo, quando há uma necessidade urgente de rastrear e controlar documentos suspeitos. Atualmente, não há um mecanismo disponível para colocar um passaporte sob suspeita em uma lista negra de forma imediata e transmiti-lo aos postos de controle de fronteiras em todo o mundo.

A tecnologia blockchain pode fornecer uma solução para esse problema ao manter uma lista negra em um contrato inteligente que pode ser atualizado conforme necessário. Quaisquer alterações serão imediatamente visíveis para todas as agências e pontos de controle de fronteira, permitindo assim o controle imediato sobre a movimentação de um documento de viagem suspeito.

Pode-se argumentar que mecanismos tradicionais como Infraestruturas de Chave Pública (PKI) e redes P2P também podem ser utilizados para esse propósito, mas eles não fornecem os benefícios que uma blockchain pode oferecer. Com uma blockchain, todo o sistema pode ser simplificado sem a necessidade de redes complexas e configurações de PKI, o que também resultará em redução de custos. Além disso, sistemas baseados em blockchain fornecerão imutabilidade garantida criptograficamente, o que auxilia na auditoria e desencoraja atividades fraudulentas.

O banco de dados completo de todos os documentos de viagem pode não ser armazenado na blockchain atualmente devido a limitações inerentes de armazenamento, mas um banco de dados distribuído de backend como o BigchainDB, IPFS ou Swarm pode ser usado para esse propósito. Nesse caso, um hash do documento de viagem com a ID biométrica de um indivíduo pode ser armazenado em um contrato inteligente simples, e um hash do documento pode então ser usado para referenciar os dados detalhados disponíveis no sistema de arquivos distribuído, como o IPFS. Dessa forma, quando um documento de viagem for colocado na lista negra em qualquer lugar da rede, essa informação estará imediatamente disponível com a garantia criptográfica de sua autenticidade e integridade em todo o livro-razão distribuído. Essa funcionalidade também pode oferecer suporte adequado em atividades antiterrorismo, desempenhando assim um papel vital na função de segurança nacional de um governo.

Um contrato simples em Solidity pode ter um array definido para armazenar identidades e registros biométricos associados. Esse array pode ser usado para armazenar as informações de identificação sobre um passaporte. A identidade pode ser um hash da MRZ do passaporte ou documento de viagem concatenado com o registro biométrico do chip RFID. Um campo booleano simples pode ser usado para identificar passaportes incluídos na lista negra. Uma vez que essa verificação inicial seja aprovada, uma verificação biométrica detalhada pode ser realizada por sistemas tradicionais. Eventualmente, quando uma decisão for tomada sobre a entrada do portador do passaporte, essa decisão pode ser propagada de volta para a blockchain, permitindo assim que todos os participantes da rede compartilhem imediatamente o resultado da decisão.

Uma abordagem de alto nível para construir um sistema de controle de fronteiras baseado em blockchain pode ser visualizada conforme mostrado no diagrama a seguir. Nesse cenário, o passaporte é apresentado para escaneamento a um leitor RFID e a um escâner de página, que lêem a página de dados e extraem as informações legíveis por máquina, junto com um hash dos dados biométricos armazenados no chip RFID. Nesse momento, uma foto ao vivo e um escaneamento de retina do portador do passaporte também são realizados. Essas informações são então transmitidas à blockchain, onde um contrato inteligente é responsável por verificar a legitimidade do documento de viagem, primeiro consultando sua lista de passaportes incluídos na lista negra e, em seguida, solicitando mais dados ao banco de dados de backend IPFS para comparação. Observe que os dados biométricos, como a foto ou o escaneamento da retina, não são armazenados na blockchain; em vez disso, apenas uma referência a esses dados no backend (IPFS ou BigchainDB) é armazenada na blockchain.

Se os dados do passaporte apresentado corresponderem aos que estão armazenados no IPFS como arquivos ou no BigchainDB e passarem na verificação lógica do contrato inteligente, então o portão de fronteira pode ser aberto:

<IMAGEM>

**Figura 22.14: Controle de fronteiras automatizado utilizando uma blockchain**

Após a verificação, essa informação é propagada pela blockchain e fica instantaneamente disponível para todos os participantes da rede blockchain de controle de fronteiras. Esses participantes podem ser um consórcio mundial de departamentos de segurança nacional de diversas nações. Outra função importante do governo são as eleições, que abordaremos a seguir.

**Eleições**

A votação em qualquer governo é uma função essencial e permite que os cidadãos participem do processo democrático de eleições. Embora a votação tenha evoluído para um processo muito mais maduro e seguro, ela ainda apresenta limitações que precisam ser abordadas para alcançar o nível de maturidade desejado. Normalmente, as limitações nos sistemas de votação atuais giram em torno de fraudes, fragilidades nos processos operacionais e, especialmente, da falta de transparência. Ao longo dos anos, mecanismos de votação seguros (máquinas) foram desenvolvidos para garantir segurança e privacidade, mas ainda assim apresentam vulnerabilidades que podem ser exploradas. Essas vulnerabilidades podem levar a sérias implicações para todo o processo eleitoral e resultar em desconfiança do público no governo.

Sistemas de votação baseados em blockchain podem resolver esses problemas ao introduzir segurança e transparência de ponta a ponta no processo. A segurança é proporcionada sob a forma de garantia de integridade e autenticidade dos votos, utilizando criptografia de chave pública, que já faz parte dos blockchains. Além disso, a imutabilidade garantida por uma blockchain assegura que votos lançados uma vez não possam ser lançados novamente. Isso pode ser alcançado por meio de uma combinação de recursos biométricos e de um contrato inteligente que mantenha uma lista de votos já lançados. Por exemplo, um contrato inteligente pode manter uma lista de votos já lançados junto com identificações biométricas (por exemplo, uma impressão digital) e pode usar isso para detectar e evitar votos duplicados. Em segundo lugar, provas de conhecimento zero (*Zero-Knowledge Proofs – ZKPs*) também podem ser utilizadas na blockchain para proteger a privacidade dos eleitores. Com uma ZKP, um eleitor pode permanecer anônimo ao ocultar sua identidade, e o próprio voto pode ser mantido confidencial.

**Identificação do cidadão**

IDs eletrônicos ou carteiras nacionais de identidade são emitidos por vários países ao redor do mundo atualmente. Esses cartões são seguros e possuem muitos recursos de segurança que impedem duplicação ou tentativas de adulteração. No entanto, com o advento da tecnologia blockchain, várias melhorias podem ser feitas nesse processo.

Identidade digital não está limitada apenas a cartões de identidade emitidos pelo governo; é um conceito que também se aplica a redes sociais e fóruns online. Podem existir múltiplas identidades sendo utilizadas para diferentes propósitos. Uma identidade digital baseada em blockchain permite o controle sobre o compartilhamento de informações pessoais. Os usuários podem ver quem usou seus dados e para qual finalidade, bem como controlar o acesso a esses dados. Isso não é possível com a infraestrutura atual, que é controlada centralmente.

Recentemente, eleições presidenciais foram realizadas em Serra Leoa utilizando tecnologia blockchain, tornando-a o primeiro país a usar blockchain em eleições:  
<https://www.coindesk.com/sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote/>

Outro exemplo é a votação na cidade de Zug. Um relatório sobre isso pode ser encontrado em:  
<https://www.stadtzug.ch/_docn/1938568/eVoting_Final_Report_ENG.pdf>

O principal benefício é que uma única identidade emitida pelo governo pode ser usada de forma fácil e transparente para múltiplos serviços por meio de uma única blockchain governamental. Nesse caso, a blockchain atua como uma plataforma na qual um governo fornece diversos serviços, como pensões, tributação ou benefícios, e uma única identificação é usada para acessar todos esses serviços. A blockchain, neste caso, fornece um registro permanente de cada alteração e transação feita por uma identidade digital, garantindo assim a integridade e a transparência do sistema. Além disso, os cidadãos podem registrar certidões de nascimento, casamentos, escrituras e muitos outros documentos na blockchain vinculados à sua identidade digital como prova de existência. A prova de existência fornece evidência digital de que algo ou algum dado existe ou existiu no passado em uma data e hora específicas.

Atualmente, existem implementações bem-sucedidas de esquemas de identidade em vários países que funcionam bem, e há argumentos de que talvez a blockchain não seja necessária para sistemas de gerenciamento de identidade. Embora existam diversos benefícios, como privacidade e controle sobre o uso das informações de identidade, devido à imaturidade atual da tecnologia blockchain, talvez ela ainda não esteja pronta para uso em sistemas de identidade do mundo real. No entanto, pesquisas estão sendo conduzidas por diversos governos para explorar o uso de blockchains para gerenciamento de identidade. Abordaremos mais sobre identidade no Capítulo 20, *Identidade Descentralizada*.

Além disso, leis como o direito ao esquecimento podem ser bastante difíceis de incorporar à blockchain devido à sua natureza imutável.

Outras funções governamentais onde a tecnologia blockchain pode ser implementada para melhorar os custos e a eficiência incluem: arrecadação de impostos, gerenciamento e desembolso de benefícios, gerenciamento de registros de propriedade de terras, registro de eventos vitais (casamentos, nascimentos), registro de veículos automotores e licenças. Esta não é uma lista exaustiva e, com o tempo, muitas funções e processos de um governo poderão ser adaptados para um modelo baseado em blockchain. Os principais benefícios da blockchain, como imutabilidade, transparência e descentralização, podem ajudar a promover melhorias na maioria dos sistemas governamentais tradicionais.

**Saúde**

O setor de saúde enfrenta muitos desafios relacionados a dados, incluindo interoperabilidade, privacidade, segurança e integridade dos dados. Muitos sistemas de saúde ainda usam bancos de dados centralizados que são vulneráveis a ataques cibernéticos, perda de dados, erros humanos e fraude. Além disso, o compartilhamento seguro de dados entre diferentes entidades, como hospitais, clínicas, laboratórios e seguradoras, ainda é um problema significativo.

A tecnologia blockchain pode fornecer uma solução para esses problemas ao permitir um registro imutável e auditável de dados de saúde, ao mesmo tempo em que mantém a privacidade do paciente por meio de técnicas criptográficas, como criptografia de chave pública e zero-knowledge proofs. Além disso, a blockchain pode facilitar o consentimento gerenciado pelo paciente para o compartilhamento de dados, onde o paciente controla quem tem acesso aos seus dados e pode revogar esse acesso a qualquer momento.

Além do registro e compartilhamento de dados, a blockchain também pode ser usada para garantir a integridade dos registros médicos eletrônicos, rastrear a cadeia de custódia de amostras de laboratório e medicamentos, e combater a falsificação de medicamentos. Por exemplo, um sistema baseado em blockchain pode rastrear cada passo da cadeia de suprimentos de um medicamento desde o fabricante até o paciente, garantindo a autenticidade do produto.

**Aplicações em mídia**

A indústria da mídia está passando por uma transformação digital com o crescimento da distribuição online e dos serviços de streaming. Entretanto, o modelo tradicional de distribuição de conteúdo apresenta desafios, incluindo a monetização inadequada para criadores de conteúdo, pirataria e questões de direitos autorais.

A tecnologia blockchain pode ajudar a resolver alguns desses problemas, permitindo um sistema de distribuição de conteúdo descentralizado e transparente. Os criadores podem registrar seus direitos de propriedade intelectual na blockchain, garantindo prova de autoria e data. Além disso, contratos inteligentes podem ser usados para automatizar pagamentos diretos aos criadores de conteúdo, sem a necessidade de intermediários.

Plataformas descentralizadas baseadas em blockchain podem permitir aos usuários pagar diretamente pelos conteúdos que consomem, incentivando a criação de conteúdo de alta qualidade. Além disso, a blockchain pode ajudar a combater a pirataria, pois a autenticação e validação de conteúdo podem ser feitas de maneira transparente e segura.

**Tendências emergentes**

À medida que a tecnologia blockchain continua a amadurecer, várias tendências importantes estão surgindo que provavelmente moldarão seu futuro e impacto em diversos setores:

* **Escalabilidade:** A escalabilidade permanece um dos maiores desafios para as blockchains públicas, como Bitcoin e Ethereum. Soluções de segunda camada, como Lightning Network para Bitcoin e canais de estado para Ethereum, estão sendo desenvolvidas para aumentar a capacidade de transações por segundo e reduzir taxas, mantendo a segurança.
* **Interoperabilidade:** Com o aumento do número de blockchains independentes, surge a necessidade de interoperabilidade para permitir que diferentes redes se comuniquem e transfiram ativos de forma segura e eficiente. Protocolos de interoperabilidade, como Polkadot e Cosmos, estão ganhando destaque.
* **Privacidade:** Técnicas avançadas de privacidade, como provas de conhecimento zero, zk-SNARKs e zk-STARKs, estão sendo incorporadas em blockchains para permitir transações privadas e contratos inteligentes que preservam a confidencialidade dos dados.
* **Governança descentralizada:** A governança em blockchains está evoluindo para incluir modelos descentralizados que permitem aos detentores de tokens ou participantes da rede votar em decisões importantes, promovendo transparência e participação comunitária.
* **Tokenização:** A tokenização de ativos reais, como imóveis, obras de arte e até ações, está crescendo, permitindo que ativos físicos sejam representados digitalmente em blockchains, facilitando negociação, liquidez e propriedade fracionada.

**Desafios da tecnologia blockchain**

Apesar do enorme potencial, a tecnologia blockchain enfrenta diversos desafios que precisam ser superados para uma adoção mais ampla e eficiente:

* **Consumo de energia:** Algoritmos de consenso como o Proof of Work (PoW) são criticados por seu alto consumo energético, levando à busca por alternativas mais eficientes, como Proof of Stake (PoS).
* **Regulação:** A ausência de regulamentação clara em muitos países cria incertezas para empresas e usuários, especialmente em áreas sensíveis como finanças e identidade digital.
* **Complexidade técnica:** A complexidade do desenvolvimento e manutenção de sistemas baseados em blockchain exige profissionais especializados, o que limita a adoção em larga escala.
* **Escalabilidade e desempenho:** Blockchains públicas ainda enfrentam limitações em transações por segundo e latência, que impactam aplicações em tempo real.
* **Privacidade e anonimato:** Equilibrar transparência com privacidade dos usuários permanece um desafio técnico e regulatório.

**Previsões futuras e considerações finais**

A tecnologia blockchain está posicionada para transformar muitos setores da economia e sociedade. À medida que as barreiras técnicas, regulatórias e sociais forem superadas, espera-se que a blockchain se torne uma infraestrutura fundamental para a economia digital.

Prevê-se que blockchains híbridas — combinando elementos públicos e privados — serão amplamente adotadas para equilibrar segurança, privacidade e eficiência. Além disso, a integração com outras tecnologias emergentes, como inteligência artificial, Internet das Coisas e computação em nuvem, abrirá novas possibilidades inovadoras.

A maturidade da tecnologia também dependerá de desenvolvimentos em governança, regulamentação e padrões abertos para garantir interoperabilidade e adoção global.

Por fim, o futuro da blockchain não está apenas na tecnologia em si, mas na forma como a sociedade a abraça e a utiliza para construir sistemas mais transparentes, seguros, eficientes e inclusivos.