**Capítulo 16**

**Blockchain Empresarial**

Neste capítulo, investigaremos blockchains empresariais. Qual é a arquitetura padrão dos blockchains empresariais? Por que eles são necessários? Responderemos a essas perguntas e também tentaremos responder à grande questão de por que blockchains públicos atuais não são necessariamente uma escolha adequada para casos de uso empresariais.

Também apresentaremos várias plataformas de blockchain empresarial, incluindo o Quorum. Ao longo do caminho, abordaremos os seguintes tópicos:

* Soluções empresariais e blockchain
* Fatores limitantes
* Requisitos
* Blockchain empresarial versus blockchain público
* Casos de uso de blockchains empresariais
* Arquitetura de blockchain empresarial
* Projetando soluções de blockchain empresarial
* Blockchain na nuvem
* Blockchains empresariais atualmente disponíveis
* Desafios do blockchain empresarial
* Quorum
* VMware Blockchain
* Configurando o Quorum com IBFT
* Outros projetos Quorum

Discutimos vários tipos diferentes de blockchain no Capítulo 1, Blockchain 101, incluindo blockchains permissionados, públicos, privados e de consórcio. Blockchains empresariais são um tipo de cadeia de consórcio permissionada que atende principalmente aos requisitos empresariais.

Permissionado não significa privado. Blockchains permissionados também podem ser públicos e permitir acesso apenas a participantes conhecidos. Blockchains empresariais geralmente são privados e permissionados e são executados entre membros do consórcio.

**Blockchain Empresarial**

Embora blockchains públicos forneçam garantias de integridade, consistência, imutabilidade e segurança, eles carecem de certos recursos, o que os torna menos adequados para uso empresarial. Discutiremos essas limitações em detalhes em breve.

Primeiramente, veremos o que são soluções empresariais e como o blockchain pode se encaixar em uma empresa. Em segundo lugar, veremos quais perguntas devem ser respondidas antes de introduzir uma solução de blockchain empresarial em um negócio.

**Soluções empresariais e blockchain**

Soluções empresariais integram diferentes fragmentos de um negócio e permitem que ele atinja seus objetivos, fornecendo informações críticas para os stakeholders. Aqui, consideraremos a questão: o blockchain se encaixa nessa definição e ajuda a alcançar objetivos empresariais?

Para descobrir se um blockchain é adequado para uma empresa ou não, podemos fazer algumas perguntas:

* Como os processos empresariais podem ser melhorados usando a tecnologia blockchain?
* Eu realmente preciso de um blockchain empresarial? Para isso, podemos fazer algumas perguntas para racionalizar se precisamos ou não de uma solução de blockchain empresarial. Meu caso de uso:
  + Precisa de dados compartilhados entre os participantes?
  + Tem participantes de outras organizações que não são necessariamente confiáveis e têm interesses conflitantes?
  + Precisa de auditoria rigorosa? Um blockchain pode fornecer isso, pois é uma cadeia de registros imutável e à prova de adulterações que pode fornecer uma trilha de auditoria definitiva das atividades realizadas na cadeia (sistema empresarial).
  + Precisa garantir a confidencialidade das transações?
  + Precisa garantir o anonimato dos participantes?
  + Precisa de atualizações controladas, mas transparentes, no livro razão?
  + Não precisa de uma autoridade confiável única? Em vez disso, as decisões na rede (atualizações no livro razão) devem ser conduzidas por membros do consórcio e acordadas entre os membros?

Se a resposta a qualquer uma das perguntas anteriores for sim, então usar uma solução de blockchain empresarial pode ser uma boa opção. Caso contrário, um banco de dados tradicional pode oferecer uma alternativa melhor. Além das perguntas mencionadas aqui, ao propor uma solução de blockchain empresarial, também precisamos responder a outras perguntas do ponto de vista empresarial que ajudam a estabelecer a visão geral e a estratégia da implementação da solução blockchain:

* Qual é o objetivo geral da solução blockchain proposta? Está alinhado com os objetivos de negócios da empresa? É um projeto de Prova de Conceito (PoC), destinado apenas a demonstrar uma ideia, ou um projeto de produção com entregas reais de negócios?
* Onde será implantado? Nuvem ou hospedagem local? Quem gerenciará a solução blockchain uma vez implantada?
* **Considerações de gerenciamento de risco** — a solução segue alguma diretriz estabelecida para gerenciamento de risco? Por exemplo, o NIST 800-37 (<https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>) é uma estrutura de gerenciamento de risco que fornece um processo usado para gerenciar riscos de segurança e privacidade para sistemas e organizações de TI.
* Existem outros projetos que essa organização já pode ter implementado usando blockchain empresarial? Podemos aprender com experiências anteriores e aproveitar alguns dos recursos e práticas recomendadas que podem ter sido desenvolvidos anteriormente?

Essas perguntas devem ser — e geralmente são — feitas ao desenvolver qualquer outra solução empresarial, mas em relação ao blockchain, essas questões se tornam ainda mais críticas devido à natureza nascente e imatura da tecnologia blockchain empresarial. Uma definição clara dos objetivos, juntamente com um alinhamento claro com os requisitos do negócio, resultará em uma implementação que atenda às metas empresariais.

A seguir, imaginaremos alguns fatores de sucesso que podem ajudar os blockchains empresariais a se tornarem bem-sucedidos e adotados nas empresas.

**Fatores de sucesso**

Existem alguns fatores orientados ao negócio que devem ser abordados para uma solução de blockchain empresarial bem-sucedida.

De suma importância é o requisito de que a solução blockchain deve trazer algum valor econômico e ajudar a alcançar metas reais de negócio. Além disso, as soluções empresariais devem estar alinhadas com os objetivos comerciais.

O principal valor dos blockchains empresariais está na propriedade de ser um livro razão compartilhável, replicável e permissionado entre organizações, o que resulta imediatamente em redução de custos ao eliminar a necessidade de troca de dados. Ao fazer isso, também eliminamos a necessidade de infraestrutura e ferramentas para suportar tais trocas. Além disso, devido à segurança, imutabilidade e auditoria fornecidas como recursos inerentes de um blockchain, não há necessidade de investir separadamente nesses requisitos.

Soluções blockchain que se integram fácil/nativamente com sistemas existentes oferecem melhor valor porque sistemas legados já maduros (pelo menos nesta fase) fornecem um mecanismo para se conectar ao blockchain, ler seus dados e salvá-los em um formato conhecido com o qual a empresa já esteja familiarizada. Além disso, apenas uma rede blockchain por si só não é inteiramente útil nas empresas se não for integrada com sistemas administrativos existentes, como sistemas de Planejamento de Recursos Empresariais (ERP), bancos de dados de backend, sistemas de reconciliação de registros ou outras ferramentas de relatórios organizacionais.

Uma solução de blockchain empresarial deve ser vista como uma solução empresarial completa de ponta a ponta como parte de uma arquitetura empresarial maior, em vez de apenas uma rede blockchain isolada. Exploraremos esse tópico mais adiante neste capítulo, na seção “Projetando soluções de blockchain empresarial”.

Governança, controle e segurança de nível empresarial também são recursos desejáveis do ponto de vista do negócio, pois permitem que as partes interessadas apliquem regras e políticas organizacionais já estabelecidas ao blockchain. Isso também pode ajudar a alcançar requisitos regulatórios e de conformidade.

**Fatores limitantes**

Discutimos vários benefícios da tecnologia blockchain em geral no Capítulo 1, Blockchain 101. Embora todos esses benefícios sejam alcançáveis usando blockchains públicos, diversos recursos estão ausentes nesses blockchains, o que os torna inadequados para casos de uso empresariais. O interesse em blockchains empresariais surge dessas limitações dos blockchains públicos, juntamente com requisitos específicos de qualquer negócio.

Descreveremos algumas das preocupações mais comuns a seguir:

* **Desempenho lento**: Blockchains públicos são lentos e podem processar apenas algumas transações por segundo. O Bitcoin processa de 3 a 4 transações por segundo, enquanto o Ethereum processa cerca de 14. Essa baixa taxa de transações não é adequada para empresas que geralmente exigem alta velocidade de transação. Por exemplo, empresas de pagamentos com cartão normalmente precisam processar milhares de transações por segundo.
* **Falta de governança de acesso**: Blockchains públicos estão disponíveis para qualquer um participar, o que facilita para investidores e entusiastas de criptomoedas aderirem e ajuda com o efeito de rede. No entanto, em uma empresa, todos os participantes devem ser conhecidos para que todos saibam com quem estão lidando. Essa falta de um mecanismo de controle de acesso e identificação torna os blockchains públicos bastante inadequados para os negócios.
* **Falta de privacidade**: Blockchains públicos são inerentemente transparentes, e tudo no livro razão é visível para todos. Isso significa que qualquer um pode facilmente visualizar detalhes de transações e os participantes envolvidos em uma transação. A falta de privacidade resulta em um problema de vazamento de estratégia, que descreveremos a seguir.
* **Problema de vazamento de estratégia**: Como blockchains públicos são abertos a todos, é possível que, usando análise de tráfego, alguém descubra qual parte está se comunicando com qual outra parte e, assim, possa inferir quem está fazendo mais negócios. Além disso, mesmo uma simples contagem de transações de um endereço pode ser usada para inferir a escala do negócio e, portanto, a receita que uma entidade pode estar gerando.
* **Consenso probabilístico**: Blockchains públicos tradicionais geralmente usam um mecanismo de consenso do tipo Prova de Trabalho (PoW), que é inerentemente um protocolo probabilístico que fornece finalização probabilística. Embora o mecanismo de confirmações, como discutido no Capítulo 6, Arquitetura do Bitcoin, forneça um certo nível de confiança de que uma transação é irrevogável, ainda é possível que a cadeia bifurque e as transações sejam perdidas. Essa questão é particularmente preocupante para empresas onde, uma vez que uma transação é confirmada, ela é considerada final. Imagine receber um documento de propriedade de imóvel em uma cadeia de alguém apenas para descobrir depois que o blockchain bifurcou e que você não é mais o proprietário da propriedade.
  + Para lidar com essa limitação, blockchains empresariais usam algoritmos de consenso determinísticos, que fornecem finalização imediata.
* Observe que alguns blockchains públicos mais novos, como Avalanche e Cosmos, têm finalização determinística. No entanto, tradicionalmente, cadeias públicas têm sido — e algumas ainda são — baseadas em PoW, por exemplo, o Bitcoin.
* **Taxas de transação**: No Ethereum ou outros blockchains semelhantes, uma taxa de transação é cobrada em criptomoeda nativa para cada execução de transação. Embora esse mecanismo forneça incentivos para os mineradores e proteção contra spam, não há necessidade de tal arranjo em blockchains empresariais. Se uma organização fosse usar blockchains públicos para suas transações comerciais, então ela precisaria manter criptomoeda em reserva para pagar pelas operações no blockchain. Esse custo extra pode ser indesejável para algumas empresas. Além disso, quando a rede está congestionada, as taxas de gás aumentam significativamente, o que resulta em ainda mais custos.
* **Congestionamento da rede**: É possível, em redes blockchain públicas, que devido a dApps movimentadas, meu próprio dApp seja impactado porque a rede está ocupada. Se toda a rede estiver congestionada devido a muitas transações, então todos os dApps funcionarão lentamente, e este é um risco que pode se mostrar prejudicial para um negócio. Embora as preocupações mencionadas aqui sejam consideradas limitações nos blockchains públicos, com base nessas preocupações e limitações, podemos derivar e definir vários requisitos, ou características, de um blockchain que o tornarão adequado para uso empresarial. Em outras palavras, as limitações nos blockchains públicos podem ser vistas como requisitos dos blockchains empresariais.

A próxima seção trata de vários recursos que um blockchain deve possuir para se tornar adequado às empresas.

**Requisitos**

Além de integridade e consistência, que também são fornecidas por blockchains públicos, há vários outros requisitos especificamente para blockchains empresariais que os tornam adequados para casos de uso empresariais. Em alguns casos, certos requisitos se tornam ainda mais rigorosos em blockchains empresariais em comparação com blockchains públicos. Por exemplo, em blockchains públicos, consistência eventual é aceitável. No entanto, em blockchains empresariais, no momento em que uma transação é confirmada, ela deve ser imediatamente finalizada e se tornar irrevogavelmente parte do registro global (estado). Assim, começaremos definindo brevemente integridade e consistência antes de introduzir requisitos específicos para blockchains empresariais:

* **Integridade**: Este atributo de um blockchain é fornecido pelo uso de funções hash e assinaturas digitais e desempenha um papel vital na segurança geral do blockchain. Funções hash permitem verificar quaisquer modificações nos dados, enquanto assinaturas digitais garantem que as mensagens que se originaram de um remetente não tenham sido alteradas.
* **Consistência**: Este atributo de um blockchain assegura que todos os nós honestos concordem sobre a mesma sequência de blocos. Para alcançar isso, são usados vários mecanismos, como protocolos de consenso PoW ou de Tolerância a Falhas Bizantinas (BFT).

Você pode consultar o Capítulo 1, *Blockchain 101*, para relembrar esses conceitos, pois introduzimos essas propriedades lá em mais detalhes.

Agora, apresentaremos três requisitos fundamentais que devem ser atendidos para que um blockchain se torne adequado para empresas. Esses requisitos são: **privacidade**, **desempenho** e **governança de acesso**.

**Privacidade**

A privacidade é de extrema importância em blockchains empresariais. A privacidade tem duas facetas: primeiro, confidencialidade, e segundo, anonimato.

A confidencialidade é um requisito fundamental em uma empresa. Espera-se que, em blockchains empresariais, todas as transações ocultem seus conteúdos, de modo que o valor das transações não seja revelado a ninguém que não tenha conhecimento da transação.

Transações privadas podem ser definidas como transações que atendem aos requisitos de privacidade de um caso de uso empresarial. Existem dois tipos de transações privadas, conforme definido pela Enterprise Ethereum Alliance (EEA):

* **Transações privadas restritas**: Esse tipo de transação privada é transmitido apenas às partes na rede blockchain que têm conhecimento da transação.
* **Transações privadas irrestritas**: Sob o paradigma de transação privada irrestrita, transações privadas são transmitidas a todos os participantes da rede, independentemente de terem ou não conhecimento da transação. O conteúdo ainda é criptografado e confidencial, mas a própria transação é transmitida para toda a rede.

Existem muitas abordagens para alcançar a privacidade em blockchains empresariais e em blockchain em geral. Esses métodos variam desde mecanismos fora da cadeia (off-chain), como gerenciadores de privacidade (usados no Quorum e em algumas outras cadeias empresariais), até o uso de provas de conhecimento zero (ZKPs), hardware confiável e computação multipartidária segura (SMPC). Abordaremos algumas dessas técnicas no próximo capítulo, Capítulo 17, *Escalabilidade*, mas neste capítulo nos concentraremos principalmente na privacidade baseada em gerenciadores de privacidade, onde um componente fora da cadeia é usado para fornecer serviços de privacidade. Discutiremos a abordagem baseada em gerenciadores de privacidade na seção sobre Quorum mais adiante neste capítulo.

O anonimato em blockchains empresariais pode não parecer um requisito rigoroso à primeira vista, pois todos os participantes são conhecidos e identificados. No entanto, ele é necessário para cenários com alguns participantes concorrentes realizando negócios na cadeia. Pode ser essencial, por exemplo, que em um cenário onde as partes X e Y estão transacionando entre si, a parte Z não descubra quais partes estão transacionando. Mesmo que os valores das transações não estejam visíveis, eles ainda podem revelar detalhes sobre o negócio que as duas partes estão fazendo. Se essa informação estiver disponível publicamente, então outras partes na cadeia do consórcio ganharão inteligência de mercado e poderão tentar influenciar esse processo por meio de marketing ou outros métodos.

**Desempenho**

Devido às exigências de alta velocidade nos negócios, blockchains empresariais devem ser capazes de processar transações a uma taxa elevada.

O desempenho tem duas facetas: **escalabilidade** e **velocidade**. Velocidade lida com quantas transações podem ser processadas em um determinado intervalo de tempo. Diz respeito à capacidade de um sistema lidar com um grande volume de transações a uma velocidade aceitável.

Por outro lado, temos o número de participantes em um sistema. Blockchains públicos podem suportar um grande número de usuários. Isso é especialmente verdadeiro em blockchains de criptomoedas, como Bitcoin e Ethereum.

Isso é possível devido aos algoritmos de consenso PoW ou Prova de Participação (PoS) usados nesses blockchains públicos. No entanto, em blockchains empresariais, uma classe diferente de algoritmos de consenso (mais comumente, BFT) é usada, os quais não funcionam bem com um grande número de nós. Isso resulta em limitação do número de usuários em uma cadeia de consórcio.

Aqui, devemos considerar uma troca. Idealmente, um blockchain empresarial deveria ter bom desempenho com um grande número de usuários; no entanto, dada essa troca, blockchains empresariais devem ser capazes de processar transações a uma alta taxa. É nisso que a maioria dos blockchains empresariais se concentra, já que, em muitos casos de uso, o número de nós não é tão alto, e a velocidade pode ser priorizada em detrimento da escalabilidade.

Em blockchains públicos, às vezes, a congestão da rede causada por altos volumes de tráfego pode gerar problemas de desempenho e aumentar os tempos de processamento de transações. Isso é prejudicial para dApps empresariais, que precisam de processamento de transações e tempos de resposta mais rápidos. A congestão da rede também resulta em aumento nos preços do gás, o que também pode ser uma preocupação para empresas do ponto de vista de custos.

**Governança de acesso**

Por outro ângulo, sendo um blockchain permissionado, o controle de acesso de nível empresarial (na forma de um novo mecanismo na cadeia ou controle conduzido por um SSO empresarial já existente) é um requisito fundamental nos blockchains empresariais. Como todos os participantes devem ser identificáveis em uma cadeia de consórcio, é essencial construir um mecanismo de controle de acesso que facilite esse processo. Esse recurso pode ser alcançado usando mecanismos de controle de acesso de nível empresarial, como o Controle de Acesso Baseado em Funções (RBAC).

O mecanismo de controle de acesso também pode abordar requisitos de Conheça Seu Cliente (KYC).

Além de privacidade, desempenho e governança de acesso — que geralmente são identificados como três requisitos fundamentais dos blockchains empresariais —, também há alguns outros requisitos que são altamente desejáveis, mas podem ser considerados um tanto opcionais, pois são mais dependentes do caso de uso. Descreveremos esses requisitos a seguir.

**Requisitos adicionais**

Nesta seção, apresentaremos alguns requisitos adicionais que são muito úteis e podem aumentar a adequação/eficácia das soluções de blockchain empresarial.

**Conformidade**

Uma preocupação comum é a conformidade. Blockchains públicos não são adequados para casos de uso empresariais devido a exigências legais e regulatórias rígidas em quase todos os setores, como financeiro, de saúde e governamental. Os desafios de conformidade incluem principalmente conformidade regulatória, conformidade com padrões, soberania de dados e preocupações com responsabilidade.

Vamos definir esses pontos brevemente a seguir:

* **Conformidade com padrões e regulamentações**: Frequentemente, em casos de uso empresariais, é exigida a conformidade com um padrão técnico ou leis. Por exemplo, a conformidade com o GDPR é obrigatória na União Europeia e no Espaço Econômico Europeu. Outro exemplo é a conformidade com as regulamentações da Autoridade de Conduta Financeira (FCA) no Reino Unido. Além disso, pode ser necessário, em certos casos de uso, cumprir padrões técnicos como os padrões de criptografia publicados pelo NIST. Um exemplo é o uso de curvas aprovadas pelo NIST, como descrito aqui:  
  <https://csrc.nist.gov/Projects/elliptic-curve-cryptography>
* **Soberania de dados**: A soberania de dados é um tópico amplo que, em essência, sujeita os dados às leis do país em que eles estão localizados. Por exemplo, sob o GDPR, a transferência de dados pessoais para fora da UE está sujeita a decisões de adequação (Artigo 45) e salvaguardas apropriadas (Artigo 46).

Como blockchains públicos são sistemas sem fronteiras e geograficamente distribuídos, o cumprimento de tais regulamentos pode ser desafiador.

* **Responsabilidade**: Em sistemas empresariais e de TI tradicionais, a responsabilidade legal muitas vezes recai sobre uma parte que presta um serviço específico; por exemplo, um provedor de serviços em nuvem é responsável por lidar com dados de acordo com as leis e regulamentações locais. Em um blockchain público descentralizado, os dados estão em um blockchain público e, portanto, torna-se desafiador manter uma única parte responsável pela gestão dos dados ou pela prestação dos serviços. Em caso de incidentes maliciosos, novamente, não é possível responsabilizar uma única parte.

Essa limitação representa um desafio significativo em ambientes empresariais onde, normalmente, uma parte responsável está no controle da prestação de serviços e pode ser responsabilizada. Por outro lado, sabemos que, em sistemas tradicionais, em caso de qualquer problema, o sistema jurídico pode ajudar. No entanto, em um blockchain descentralizado, pode se tornar bastante difícil culpar uma única parte por suas ações. Portanto, em blockchains empresariais, a capacidade de cumprir regulamentos e leis se torna um atributo muito desejado e pode ser alcançada por meio de identificação apropriada, KYC e mecanismos de controle de acesso. Em uma cadeia empresarial, os participantes são conhecidos e podem ser responsabilizados por suas ações.

**Interoperabilidade**

À medida que o ecossistema de blockchain empresarial evolui, também surge a necessidade de poder trocar dados entre blockchains empresariais e públicos distintos. A falta de padronização também agrava esse problema; no entanto, esforços de padronização estão em andamento, como a EEA (discutida na seção sobre desafios do blockchain empresarial). Também há soluções de interoperabilidade sendo desenvolvidas e disponíveis para blockchains que permitem interoperabilidade entre cadeias, como ION, protocolo IBC, Polkadot e Interledger.

**Integração**

Nenhum blockchain empresarial é uma solução isolada de ponta a ponta. Ele precisa se integrar com sistemas empresariais existentes ou outros sistemas fora da cadeia que fazem parte da solução empresarial completa para atingir os objetivos de negócios. Portanto, blockchains empresariais devem fornecer interfaces para integração. Isso pode ser tão simples quanto fornecer endpoints RPC ou tão complexo quanto construir conectores e plugins específicos para blockchain que se integrem a barramentos de serviço empresariais ou a outros sistemas legados — mais sobre isso na seção “Arquitetura de blockchain empresarial”.

A integração com dispositivos de segurança, como Módulos de Segurança de Hardware (HSMs), também é bastante desejável para muitos casos de uso empresariais em que segurança rigorosa é exigida, ou por exigências regulatórias ou de conformidade.

**Facilidade de uso**

Normalmente, sistemas empresariais são fáceis de implantar e usar. A implantação em empresas é fácil e rápida, e muitas vezes depende de estruturas e ferramentas maduras, como Ansible e outras ferramentas proprietárias, mas esse não é o caso com blockchain.

A implantação de sistemas empresariais é uma área bem estudada, compreendida e madura. Com ferramentas de orquestração empresarial e técnicas estabelecidas ao longo dos anos, a implantação empresarial tornou-se fácil. No entanto, blockchains não são tão fáceis de implantar quanto outros sistemas empresariais. Com a disponibilidade de Blockchain como Serviço (BaaS) e ferramentas de automação de implantação, isso está mudando. No entanto, ainda há trabalho a ser feito.

**Monitoramento**

O monitoramento com ferramentas de visualização desempenha um papel vital em qualquer solução empresarial. Sem a capacidade de monitorar e visualizar um sistema, é quase impossível garantir a integridade do sistema empresarial. Também é um recurso desejável em soluções de blockchain empresarial poder visualizar a rede blockchain. Monitorar um blockchain permite que um administrador acompanhe a saúde da rede e suas operações. Permite a um administrador monitorar e responder a eventos de interesse, como um nó caindo, lentidão no link de comunicação, um nó sendo incapaz de sincronizar com o blockchain e muitos outros cenários.

**Cálculo seguro fora da cadeia**

Em alguns cenários, é desejável poder descarregar alguns cálculos intensivos para sistemas fora da cadeia; por exemplo, se houver um requisito para fazer algum cálculo que exija recursos de Computação de Alto Desempenho (HPC).

Isso se sobrepõe um pouco com a integração, mas é mencionado aqui separadamente devido a requisitos específicos de segurança que os cálculos fora da cadeia devem ter — eles precisam ser comprovadamente corretos, com garantias de integridade e autenticidade.

**Melhores ferramentas**

Normalmente, em sistemas empresariais, há muitas ferramentas e utilitários de suporte agrupados com o produto principal para operar o software. Por exemplo, incluem-se ferramentas de administração, ferramentas de implantação, utilitários para desenvolvedores, ferramentas de visualização, ferramentas de gerenciamento e ferramentas para usuários finais. Plataformas de blockchain com melhor suporte de ferramentas são muito mais desejáveis devido ao melhor suporte ao usuário. Ferramentas como exploradores de blocos, módulos de administração de usuários e dApps para gerenciar contratos inteligentes são bastante úteis. Elas estão se tornando gradualmente mais maduras à medida que todo o ecossistema de blockchain cresce.

Agora que compreendemos os recursos dos blockchains empresariais, apresentaremos uma comparação entre blockchains públicos e empresariais para ajudar a entender as principais diferenças.

**Blockchain empresarial versus blockchain público**

Nesta seção, forneceremos uma comparação entre blockchains públicos e empresariais. Considere a tabela mostrada aqui, que avalia alguns pontos de comparação entre os dois tipos de blockchain. Esta não é uma lista exaustiva; no entanto, abordaremos os pontos mais importantes:

| **Aspecto** | **Cadeias públicas** | **Cadeias empresariais** |
| --- | --- | --- |
| Confidencialidade | Não. | Sim. |
| Anonimato | Não. | Sim. |
| Associação | Sem permissão. | Permissionada via votação, KYC, geralmente sob blockchain empresarial. |
| Identidade | Usuários anônimos. | Usuários conhecidos. |
| Consenso | PoW/PoS. | BFT. |
| Finalidade | Principalmente probabilística. | Requer finalização imediata/instantânea. |
| Velocidade de transação | Mais lenta. | Mais rápida (geralmente, deve ser). |
| Escalabilidade | Melhor. | Normalmente, não muito escalável, devido à escolha do consenso. |
| Conformidade regulatória | Normalmente não exigida - difícil. | Frequentemente exigida - relativamente mais fácil de atingir. |
| Confiança | Totalmente descentralizada. | Semi-centralizada, gerenciada via consórcio e mecanismos de votação. |
| Contratos inteligentes | Não são estritamente necessários (ex: Bitcoin). | Estritamente exigidos para dar suporte a funções empresariais. |

A tabela anterior compara vários aspectos importantes das plataformas públicas e empresariais. A seguir, consideraremos brevemente alguns dos casos de uso dos blockchains empresariais.

Na próxima seção, descreveremos a **arquitetura de blockchain empresarial**, que pode nos ajudar a nos comunicar com stakeholders, promover decisões iniciais de design, servir como um modelo reutilizável para desenvolvimento, construir entendimento compartilhado e compreender como o sistema é estruturado.

**Arquitetura de blockchain empresarial**

Uma arquitetura típica de blockchain empresarial contém vários elementos. Vimos uma arquitetura genérica de blockchain no Capítulo 1, *Blockchain 101*, e podemos expandi-la e modificá-la um pouco para transformá-la em uma arquitetura de blockchain empresarial que destaque os requisitos centrais de um blockchain empresarial. Esses requisitos são principalmente conduzidos pelas necessidades empresariais e pelos casos de uso:

<IMAGEM>

*Figura 16.1: Arquitetura em camadas de blockchain empresarial*

Discutiremos cada uma dessas camadas da seguinte forma:

* **Camada de rede**: A camada de rede é responsável pela implementação dos protocolos de rede, como os protocolos peer-to-peer (P2P) usados para disseminação de informações.
* **Camada de protocolo**: Esta é a camada do livro-razão propriamente dita, ou camada de blockchain, onde os elementos centrais de consenso, gerenciamento de transações e armazenamento são implementados.
* **Camada de privacidade**: Esta camada é responsável por fornecer um dos principais recursos do blockchain empresarial: a privacidade. Existem várias formas de alcançar privacidade, incluindo gerenciadores de privacidade off-chain, conhecimento zero (zero knowledge) e privacidade assistida por hardware. A privacidade baseada em hardware geralmente é suportada usando ambientes de execução confiáveis (TEEs). Por outro lado, privacidade baseada em software ou algoritmos, como as ZKPs, também são bastante comuns em blockchains empresariais.
* **Camada de governança**: Esta camada é responsável por fornecer o mecanismo de controle de acesso de nível empresarial que controla a associação à rede de consórcio. Isso pode ser controlado por um sistema de permissões on-chain implementado em contratos inteligentes, como parte do cliente de software, ou pode ser integrado a sistemas de permissão empresariais off-chain existentes, como Single Sign-On (SSO) ou Active Directory (AD).
* **Camada de integração**: Esta camada fornece APIs e um mecanismo utilizado para integrar com sistemas legados ou sistemas administrativos existentes. Pode ser algo simples como uma camada RPC que fornece APIs sobre RPC ou constituir conectores e plugins integrados para integração com o barramento de serviço empresarial.
* A camada de integração é responsável por garantir a integração com sistemas administrativos, legados e outros sistemas off-chain existentes. Ela não faz parte do protocolo central, mas, como parte da visão holística da solução blockchain de ponta a ponta, essa camada é vital para a entrega de resultados comerciais. Embora existam muitas técnicas disponíveis, uma estrutura comum de integração usada em ambientes empresariais é o Apache Camel. Isso também pode ser usado em soluções blockchain, pois vem com o componente de biblioteca Web3J para Ethereum.

Apache Camel é uma estrutura de integração empresarial de código aberto. Ele permite integração fácil entre vários sistemas usando padrões de integração empresarial. Possui centenas de componentes para diferentes sistemas, como bancos de dados, APIs e MQs para integração fácil entre sistemas.

Por exemplo, o conector Web3J (conector Ethereum do Apache Camel) é um conector rico em recursos disponível no Apache Camel que permite integração entre cadeias Ethereum e outros sistemas. Mais detalhes sobre o componente Web3J estão disponíveis aqui:  
<https://camel.apache.org/components/latest/web3j-component.html>

O conector Ethereum do Apache Camel funciona com nós Ethereum Geth, Quorum, Parity e Ganache. Ele oferece suporte à API JSON RPC via HTTP e IPC, com implementações para diferentes operações blockchain como net, eth, shh e assim por diante. Ele oferece suporte a filtros Ethereum, ao Ethereum Name Service (ENS) e à API JSON RPC, e é também uma solução totalmente testada (testes unitários e de integração).

<IMAGEM>

*Figura 16.2: Design de alto nível do Apache Camel, que permite integração com blockchain*

* **Camada de aplicação**: A camada de aplicação, como o nome sugere, consiste em dApps, contratos inteligentes, ferramentas e outros softwares relevantes para dar suporte a casos de uso empresariais.
* **Segurança, desempenho, escalabilidade, monitoramento**: No lado esquerdo do diagrama de arquitetura (Figura 16.1), segurança, escalabilidade, desempenho e monitoramento são mostrados. Como cada camada no blockchain empresarial se beneficia (e, na verdade, exige) segurança, escalabilidade e desempenho, esta camada é mostrada como englobando todas as outras. O monitoramento também desempenha um papel vital em qualquer solução empresarial. Sem visualizações eficazes em redes tão complexas, é quase impossível acompanhar tudo. Portanto, essa camada é mostrada como relevante para todas as camadas de blockchain empresarial.

**Projetando soluções de blockchain empresarial**

Um blockchain isolado em uma empresa não é suficiente para resolver problemas de negócios. Além de escolher uma plataforma de blockchain, há outros fatores a considerar ao introduzir um blockchain em uma empresa. No topo da lista desses fatores está a **integração com os sistemas administrativos e legados existentes**.

No diagrama anterior, podemos ver vários blockchains empresariais conectando-se ao Apache Camel usando conectores Ethereum do Apache Camel. Além disso, outros sistemas se conectam ao Apache Camel por meio de seus respectivos conectores. O Apache Camel, via conectores, é responsável por integrar todos esses sistemas. Por exemplo, é totalmente possível usar o Apache Camel para extrair dados de blockchains empresariais e armazená-los em bancos de dados SQL tradicionais da empresa por meio de conectores apropriados.

Sem qualquer estrutura de arquitetura, torna-se bastante desafiador ter uma visão holística de uma empresa e ver como todos os processos de negócios se encaixam. Assim, surge a pergunta sobre se podemos aproveitar estruturas existentes para atender às necessidades arquitetônicas do blockchain empresarial. A resposta é sim. Já existem estruturas estabelecidas e maduras para facilitar o desenvolvimento de arquitetura empresarial.

O objetivo das **estruturas de arquitetura empresarial** é permitir que uma organização execute sua estratégia de negócios de forma eficaz. Ela permite que a organização se enxergue sob diferentes perspectivas, incluindo negócio, informação, processo e tecnologia, e tome decisões comerciais eficazes para alcançar os objetivos.

Agora, vamos explorar as estruturas de arquitetura empresarial mais populares, o **The Open Group Architecture Framework (TOGAF)** e o **Zachman Framework**.

**TOGAF**

TOGAF significa The Open Group Architecture Framework. Ele é desenvolvido pelo Open Group.

É uma estrutura que permite às organizações projetar, planejar e implementar soluções empresariais sistematicamente. Ela possui quatro domínios arquitetônicos:

* **Domínio de arquitetura de negócios**: Este domínio define a estratégia de negócios, estrutura organizacional, processos de negócios e governança da organização.
* **Domínio de arquitetura de dados**: Este domínio descreve as estruturas dos ativos de dados da organização e os recursos relevantes de gerenciamento de dados.
* **Domínio de arquitetura de aplicações**: Este domínio descreve os aplicativos empresariais, os planos de implantação, os relacionamentos e interações entre os aplicativos, juntamente com os relacionamentos que esses aplicativos têm com os processos de negócios dentro da empresa.
* **Domínio de arquitetura tecnológica**: Este domínio define os requisitos da arquitetura técnica para implementação dos aplicativos empresariais. Isso inclui a descrição do hardware, software, middleware e infraestrutura de rede necessários para a implementação das aplicações empresariais.

Agora, reexaminando cada domínio com o blockchain em mente, podemos incluir blockchain em cada camada e tomar decisões como: requisitos de negócios, arquitetura de aplicações, ativos lógicos e físicos de dados e, finalmente, a infraestrutura necessária para implementar a solução de blockchain empresarial.

Após essa introdução básica ao TOGAF, vamos nos aprofundar um pouco para entender o método que o TOGAF usa para desenvolver uma arquitetura de TI.

O site oficial do TOGAF pode ser encontrado aqui: <https://www.opengroup.org/togaf>

**Método de desenvolvimento da arquitetura (ADM)**

O TOGAF ADM é um método para desenvolver uma arquitetura de TI que atenda às necessidades comerciais organizacionais. Ele descreve o processo de transição da arquitetura fundacional do TOGAF para uma arquitetura específica da organização. Esse é um processo iterativo com gerenciamento contínuo de requisitos, que resulta no desenvolvimento de uma arquitetura específica para uma organização e que atenda às suas necessidades. Uma vez concluído o desenvolvimento da arquitetura, ela pode ser publicada em toda a organização para criar um entendimento comum.

O ADM é um processo testado e repetível para o desenvolvimento de arquiteturas empresariais. O processo segue as seguintes etapas: estabelecer uma estrutura de arquitetura, desenvolver o conteúdo da arquitetura, governança da arquitetura e implementação das arquiteturas.

O ADM possui nove fases, e cada fase pode ser dividida em múltiplas etapas. O modelo ADM é mostrado aqui:

<IMAGEM> \*Figura 16.3: Modelo ADM\*

Agora, descreveremos cada fase em mais detalhes:

* **Fase preliminar**: Esta fase define as bases da arquitetura. Define metodologias, princípios de arquitetura, o escopo da arquitetura e suposições sobre a arquitetura. Também define os responsáveis pela entrega da arquitetura. Do ponto de vista do blockchain, podemos definir a estratégia geral de blockchain nesta fase.
* **Visão da arquitetura**: Esta fase valida os princípios de negócio, metas e estratégia de negócios. Define os principais requisitos de negócios, bem como uma descrição de alto nível do valor esperado do trabalho arquitetônico. Esta fase também analisa o impacto da nova arquitetura em outros processos.
* **Arquitetura de negócios**: Esta fase propõe a arquitetura de negócios atual (baseline) e desenvolve uma arquitetura de negócios alvo, juntamente com uma análise de lacunas. Em um cenário de blockchain, podemos definir a arquitetura do estado atual e a arquitetura de estado alvo neste estágio.
* **Arquitetura dos sistemas de informação**: Esta fase define a arquitetura de dados e a arquitetura de aplicações. A arquitetura de dados inclui: construção da arquitetura de dados atual, descrição da arquitetura de dados, construção de modelos de arquitetura de dados, análise de impacto, revisão de modelos de referência e pontos de vista. A arquitetura de aplicações define: a arquitetura de aplicações atual, construção de modelos da arquitetura de aplicações e proposição de aplicações. Ambas as atividades também realizam uma análise de lacunas para validar a arquitetura em desenvolvimento, bem como encontrar quaisquer deficiências entre a arquitetura atual e a arquitetura alvo. Semelhante à arquitetura de negócios, para uma solução de blockchain empresarial, podemos definir a arquitetura atual e a arquitetura alvo.
* **Arquitetura tecnológica**: Esta fase está principalmente preocupada com a revisão das arquiteturas atuais de negócios, dados e aplicações, e a construção de uma descrição da arquitetura tecnológica atual da empresa. Também propõe a arquitetura tecnológica alvo. Nesta fase, podemos propor uma plataforma de blockchain empresarial alvo e a solução alvo.
* **Oportunidades e soluções**: Esta fase realiza avaliações e seleciona várias arquiteturas alvo propostas. Além disso, uma estratégia e plano de implementação são propostos neste estágio. Podemos aplicar isso ao blockchain de forma semelhante, avaliando ou selecionando a arquitetura alvo que abrange soluções de blockchain empresarial. Ao avaliar soluções de blockchain, vários recursos apresentados anteriormente na comparação entre blockchain empresarial e público também podem ser utilizados; por exemplo, confidencialidade, escalabilidade e finalização.
* **Planejamento de migração**: Esta fase cria e finaliza o plano abrangente de implementação para a migração da arquitetura atual para a arquitetura alvo.

O diagrama original pode ser encontrado em: <https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html>

* **Governança da implementação**: Esta fase trata da implementação da arquitetura alvo. Uma estratégia para governar a implantação e migração geral é desenvolvida aqui. Também podemos realizar testes da solução blockchain e elaborar uma estratégia de implantação durante esta fase.
* **Gerenciamento de mudanças da arquitetura**: Esta fase é responsável por criar diretrizes e procedimentos de gerenciamento de mudanças para a arquitetura alvo recém-implementada. Do ponto de vista do blockchain, esta fase pode fornecer procedimentos de gestão de mudanças para a solução blockchain empresarial recém-implementada.

Com isso, concluímos nossa introdução ao TOGAF e exploramos a ideia de que soluções de blockchain empresarial devem ser vistas sob a ótica da arquitetura empresarial.

A ideia fundamental a ser compreendida aqui é que soluções de blockchain empresarial **não** são meramente uma questão de iniciar rapidamente uma rede, criar alguns contratos inteligentes, criar uma interface web e esperar que isso resolva os problemas de negócio. Essa configuração pode ser útil como uma **prova de conceito (PoC)** ou para um caso de uso extremamente simples, mas certamente **não** é uma solução empresarial.

Sugerimos que uma solução de blockchain empresarial deve ser analisada pela perspectiva da **arquitetura empresarial** e considerada como uma **solução empresarial completa**, de nível profissional. Isso para que possamos alcançar efetivamente os objetivos de negócio que se pretende resolver com soluções de blockchain empresarial.

**Blockchain na nuvem**

A computação em nuvem oferece excelentes benefícios às empresas, incluindo eficiência, redução de custos, escalabilidade, alta disponibilidade e segurança. A computação em nuvem fornece serviços de computação como infraestrutura, servidores, bancos de dados e software pela internet. Existem diferentes tipos de serviços em nuvem disponíveis; uma comparação padrão é feita entre **Infraestrutura como Serviço (IaaS)**, **Plataforma como Serviço (PaaS)** e **Software como Serviço (SaaS)**. Surge então a pergunta: **onde o blockchain se encaixa?**

**Blockchain como Serviço**, ou **BaaS**, é uma extensão do SaaS, na qual uma plataforma blockchain é implementada na nuvem para uma organização. A organização gerencia suas aplicações no blockchain, e o restante do gerenciamento de software, gerenciamento da infraestrutura e outros aspectos, como segurança e sistemas operacionais, são gerenciados pelo provedor da nuvem. Isso significa que o software e a infraestrutura do blockchain são fornecidos e mantidos pelo provedor da nuvem. O cliente ou empresa pode se concentrar em suas aplicações de negócio sem se preocupar com outros aspectos da infraestrutura.

A seguir está uma comparação entre diferentes abordagens:

<IMAGEM> \*Figura 16.04: Soluções em nuvem\*

O BaaS pode ser considerado um tipo de SaaS, onde o software é um blockchain. Nesse caso, assim como no SaaS, todos os serviços são gerenciados externamente. Em outras palavras, os clientes recebem uma rede blockchain totalmente gerenciada sobre a qual podem construir e gerenciar seus próprios dApps. Observe que, no diagrama anterior, sob a coluna "Blockchain como Serviço", **Aplicações** foram substituídas por **Blockchain**, como um diferencial em relação a outros serviços de nuvem. Aqui, o blockchain é o software (aplicação) fornecido e gerenciado pelo provedor de serviços de nuvem. Além disso, observe que os dApps foram adicionados no topo, os quais são gerenciados internamente pela empresa.

Há muitos provedores de BaaS. Alguns deles são listados a seguir:

* **AWS**: <https://aws.amazon.com/blockchain/>
* **Azure**: <https://azure.microsoft.com/en-gb/solutions/blockchain/>
* **Oracle**: <https://www.oracle.com/uk/application-development/cloud-services/blockchain-platform/>
* **IBM**: <https://www.ibm.com/uk-en/cloud/blockchain-platform>

**Blockchains empresariais atualmente disponíveis**

Como esta é uma área muito promissora para pesquisa — e, de fato, o mercado está muito ativo nesse espaço — diversas soluções de blockchain empresarial foram desenvolvidas e disponibilizadas nos últimos anos. Notavelmente, o ano de **2019** foi chamado de “o ano do blockchain empresarial”, à medida que muitas startups e empresas com foco nessa área surgiram.

Nesta seção, não cobriremos todas essas plataformas em detalhes, mas forneceremos uma breve introdução e links para mais detalhes sobre essas cadeias:

* **Quorum** é uma plataforma de blockchain empresarial de código aberto. Ela visa dar suporte às necessidades empresariais e permite que uma empresa atinja seus objetivos de negócio (e desbloqueie valor econômico) aproveitando a tecnologia blockchain. Ela aborda requisitos empresariais cruciais, incluindo **privacidade**, **desempenho** e **permissão empresarial**. Exploraremos o Quorum com mais profundidade posteriormente neste capítulo.
* **Fabric** é um projeto da Hyperledger. Trata-se de um livro-razão distribuído de nível empresarial que permite o desenvolvimento de soluções blockchain com uma arquitetura modular. Possui uma arquitetura permissionada, oferece suporte à modularização e consenso plugável, e permite contratos inteligentes. Discutimos o Hyperledger e outros projetos relacionados, como o Sawtooth, em detalhes no Capítulo 14, *Hyperledger*.

Vamos considerar uma comparação entre as principais plataformas de blockchain empresarial. Cobriremos a maioria dos recursos desejáveis de blockchains empresariais. Isso pode ser usado como referência para uma comparação rápida entre essas plataformas. Esta comparação é baseada nas implementações atuais disponíveis dessas plataformas no momento da redação. No entanto, como esta é uma área que muda rapidamente, alguns recursos podem mudar com o tempo, ou novos recursos podem ser adicionados ou aprimorados:

| **Recurso** | **Quorum** | **Fabric** | **Corda** |
| --- | --- | --- | --- |
| Indústria-alvo | Intersetorial | Intersetorial | Intersetorial |
| Desempenho (TPS aproximado) | 700 (\*) | 560 (∞) | 600 (@) |
| Mecanismo de consenso | Múltiplos plugáveis: Raft, IBFT, PoA | Plugável: Raft | Plugável, baseado em notários |
| Ferramentas | Ferramentas empresariais ricas | SDKs | Ferramentas empresariais ricas |
| Linguagem de contrato inteligente | Solidity | Golang | Kotlin/Java |
| Finalidade | Imediata | Imediata | Imediata |
| Privacidade | Sim (transações privadas restritas) | Sim (transações privadas restritas) | Sim (transações privadas restritas) |
| Controle de acesso | Mecanismo de permissão empresarial | Provedores de serviço de associação/certificado | Serviço de aprovação (Doorman)/KYC |
| Linguagem de implementação | Golang, Java | Golang | Kotlin |
| Associação de nós | Contrato inteligente e software do nó | Via provedor de serviços de associação | Gerenciado por arquivos de configuração |
| Identificação de membros | Chaves públicas/endereços | Baseado em PKI via provedor de associação | Baseado em PKI, com suporte à identidade organizacional |
| Criptografia usada | SECP256K1, AES, Keccak256, Curve25519, etc. | SECP256R1, RSA – PKCS1 | Curve25519 + XSALSA20 + POLY13050, ED25519 |
| Runtime de contrato inteligente | EVM | Containers Docker isolados | JVM determinística |
| Contrato inteligente atualizável | Possível com alguns padrões, não nativo | Permitido via transações de atualização | Permitido com privilégios administrativos |
| Suporte à tokenização | Flexível — herdado dos padrões do Ethereum | Programável | SDK de token Corda |

* “Resultados de TPS para Quorum baseados em: <https://arxiv.org/pdf/1809.03421.pdf>  
  ∞ Resultados de TPS para Hyperledger Fabric baseados em: <https://hyperledger.github.io/caliper-benchmarks/fabric/performance/2.0.0/nodeContract/nodeSDK/submit/empty-contract/>  
  @ Resultados de TPS para Corda baseados em: <https://www.r3.com/corda-enterprise/>”

Essa comparação também pode ser usada para avaliação rápida dessas plataformas e sua adequação para um caso de uso empresarial.

**Desafios do blockchain empresarial**

Embora os blockchains empresariais tenham abordado os principais requisitos empresariais (privacidade, desempenho e governança) até certo ponto, ainda existem mais desafios que precisam ser enfrentados. Há progresso significativo sendo feito no sentido de resolver essas questões. No entanto, ainda há muito trabalho necessário para lidar adequadamente com essas limitações. Alguns desses desafios são listados a seguir:

**Interoperabilidade**

Soluções de blockchain são construídas por diferentes equipes de desenvolvimento com diferentes requisitos-alvo. Como resultado, existem agora muitos tipos diferentes de blockchains, variando desde blockchains públicos de criptomoeda até blockchains específicos de aplicação, desenvolvidos para um único aplicativo de negócio. A troca de dados entre essas cadeias é uma preocupação crucial. Enquanto as redes blockchain continuam a crescer de forma independente, a integração e interoperabilidade entre essas cadeias permanecem uma grande preocupação.

Esse problema também decorre da falta de padronização. Se uma especificação padrão estivesse disponível, todas as cadeias que seguissem esse padrão se tornariam compatíveis automaticamente. Mas e quanto às cadeias que já estão implantadas em produção, incluindo cadeias públicas? Como alcançamos interoperabilidade entre elas? Muitos casos de uso de negócios possuem o requisito de obter dados de uma organização para outra ou de uma rede blockchain para outra. Isso também é verdade no caso de requisitos de troca de dados entre uma blockchain pública e uma rede de consórcio.

**Falta de padronização**

A falta de padronização é uma preocupação comumente destacada nos blockchains empresariais e, em geral, em todo o ecossistema blockchain. Sistemas tradicionais são desenvolvidos, em sua maioria, alinhados com padrões definidos por órgãos de padronização, como os padrões NIST FISMA para segurança da informação.

O Federal Information Security Management Act (FISMA) de 2002 é uma lei federal dos Estados Unidos que exige que todas as agências federais desenvolvam, documentem e implementem um programa de segurança da informação em toda a agência. O FISMA foi alterado em 2014 como a Federal Information Security Modernization Act. Mais informações sobre o FISMA aqui: <https://www.congress.gov/bill/113th-congress/senate-bill/2521>

Padrões também são essenciais para alcançar interoperabilidade. Diversas iniciativas foram tomadas para abordar os desafios mencionados aqui e também para padronizar plataformas de blockchain empresarial. Uma organização líder neste campo é a **EEA**, uma organização de padronização gerida por seus membros que visa desenvolver especificações de blockchain empresarial.

A EEA publica regularmente especificações técnicas que podem ser baixadas no link fornecido aqui:

<https://entethalliance.org/technical-specifications/>  
Site oficial da EEA: <https://entethalliance.org>

**Conformidade**

A conformidade continua sendo uma preocupação significativa nos blockchains empresariais. Os blockchains públicos, por exemplo, são, por definição, sem fronteiras e descentralizados. Os dados armazenados em blockchains públicos não podem ser alterados ou excluídos. Além disso, uma vez que os dados são propagados e armazenados em uma rede de nós global, a soberania dos dados é desafiada. Isso levanta várias preocupações, como:

* Como garantir que os dados não sejam armazenados em nós em países que não sejam compatíveis com certas regulamentações?
* Como aplicar a exclusão de dados sob o GDPR?
* Como manter a conformidade com padrões de segurança como FISMA, NIST, ISO/IEC 27001 e ISO/IEC 27002?

Essas são apenas algumas das muitas preocupações de conformidade que surgem com blockchains empresariais. O desenvolvimento de políticas, procedimentos e mecanismos técnicos adequados para permitir conformidade em soluções blockchain é essencial. Isso inclui suporte a criptografia padrão, anonimato, privacidade, gerenciamento de identidade e integração com provedores de identidade externos e confiáveis.

**Desafios de negócios**

Junto com desafios técnicos, existem diversos desafios de negócios enfrentados por soluções de blockchain empresarial. Eles incluem:

* **Custo**: Custos associados à adoção e integração de soluções blockchain, incluindo custos de desenvolvimento, treinamento, licenciamento e migração.
* **Resistência organizacional à mudança**: Equipes técnicas ou administrativas existentes podem resistir a adotar novas tecnologias que mudam significativamente processos estabelecidos.
* **Falta de compreensão de requisitos**: As organizações muitas vezes não têm clareza suficiente sobre o que esperam alcançar com blockchain, o que resulta em adoção sem justificativa de negócio clara.
* **Adoção limitada do ecossistema**: Um consórcio blockchain requer colaboração entre múltiplas organizações. Se partes importantes não participarem, o valor da rede pode ser comprometido.

**VMware Blockchain**

O VMware Blockchain é uma plataforma blockchain empresarial desenvolvida pela VMware. Ela foi construída para fornecer uma solução empresarial pronta para produção e com foco especial em privacidade, desempenho e confiança.

Ele fornece os seguintes recursos principais:

* **Tolerância a falhas bizantinas (BFT)**: O VMware Blockchain utiliza um protocolo BFT chamado Scalable Byzantine Fault Tolerance (SBFT) para garantir resiliência contra falhas bizantinas.
* **Alta taxa de transferência e baixa latência**: A plataforma é projetada para oferecer alto desempenho, mantendo baixa latência de transação.
* **Privacidade e confidencialidade**: O VMware Blockchain oferece suporte a contratos inteligentes confidenciais e privacidade seletiva de dados.
* **Compatibilidade com Ethereum**: A plataforma é compatível com contratos inteligentes do Ethereum, permitindo portabilidade de aplicações já existentes.
* **Implantação corporativa**: O VMware Blockchain é adequado para ambientes empresariais com requisitos de implantação sob demanda, alta disponibilidade e gerenciamento de políticas de segurança.

**Quorum**

O Quorum é uma plataforma de blockchain empresarial baseada no Ethereum, originalmente desenvolvida pela J.P. Morgan. É uma plataforma de blockchain de código aberto que visa permitir que empresas aproveitem os recursos do Ethereum enquanto atendem aos requisitos empresariais de **privacidade**, **desempenho** e **governança empresarial**.

Ele é mantido pela ConsenSys, e o repositório pode ser encontrado aqui:  
<https://github.com/ConsenSys/quorum>

A arquitetura do Quorum pode ser resumida nos seguintes componentes:

* **Geth modificado (GoQuorum)**: É uma versão modificada do Geth (cliente Go Ethereum). Ele fornece as funcionalidades básicas do nó, adicionando suporte a transações privadas e mecanismos de consenso plugáveis como IBFT e Raft.
* **Gerenciador de transações (Tessera)**: Trata da privacidade das transações. Ele isola os dados privados das transações confidenciais, assegura que apenas os participantes relevantes tenham acesso, e utiliza criptografia para proteger os dados.
* **Enclave de criptografia**: Parte do gerenciador de transações, responsável por lidar com operações criptográficas, como criptografar e descriptografar cargas úteis e gerenciar chaves criptográficas.
* **Contrato inteligente de permissão empresarial**: Permite que os administradores configurem quem pode se juntar à rede, quem pode executar contratos inteligentes, e quem pode participar de transações.

**Privacidade no Quorum**

A privacidade é um dos principais pilares do Quorum. Ao contrário do Ethereum público, onde todas as transações e dados de contrato inteligente são visíveis para todos, o Quorum fornece dois modos de transações privadas:

1. **Transações privadas restritas**: As cargas úteis são visíveis apenas para os participantes autorizados.
2. **Transações privadas irrestritas**: A carga útil é transmitida a todos os nós, mas criptografada — apenas os participantes autorizados podem vê-la.

Essa privacidade é habilitada por meio do **Tessera**, o componente de gerenciamento de transações. Ele garante que as cargas úteis confidenciais sejam armazenadas fora da cadeia e criptografadas, com apenas os hashes mantidos on-chain para prova de integridade.

**Consenso no Quorum**

O Quorum suporta múltiplos mecanismos de consenso que podem ser trocados conforme necessário:

* **Raft**: Um algoritmo de consenso tolerante a falhas crash (não bizantinas), baseado em líderes, que oferece finalização imediata e alta velocidade.
* **IBFT (Istanbul BFT)**: Um protocolo de Tolerância a Falhas Bizantinas adequado para cenários onde os nós podem se comportar de forma maliciosa. Oferece finalização imediata e segurança aprimorada, à custa de um pouco de desempenho.
* **Clique (PoA)**: Um algoritmo baseado em autoridade que oferece alta velocidade e é útil quando os validadores são confiáveis.

**Permissões no Quorum**

O Quorum fornece um modelo de permissão que permite o controle de acesso granular em nível empresarial. Isso inclui controle sobre:

* Quem pode ingressar na rede.
* Quem pode implantar ou chamar contratos inteligentes.
* Quem pode enviar transações.

O modelo de permissão pode ser estendido com contratos inteligentes personalizados e configurado para refletir a estrutura organizacional de uma empresa.

**R3 Corda**

O **Corda**, desenvolvido pela empresa R3, é uma plataforma de blockchain empresarial projetada especificamente para o setor financeiro. Diferente de muitas outras plataformas blockchain que derivam diretamente de arquiteturas tradicionais como Ethereum ou Bitcoin, o Corda foi desenvolvido do zero, com foco em **privacidade**, **escalabilidade**, **confiança** e **transações ponto a ponto**.

O Corda não é, tecnicamente, um blockchain no sentido tradicional, pois não há um livro-razão compartilhado por todos os participantes. Em vez disso, **os dados são compartilhados apenas entre as partes envolvidas em uma transação**, permitindo confidencialidade e eficiência.

**Características principais do Corda:**

* **Privacidade ponto a ponto**: Apenas as partes envolvidas em uma transação têm acesso às informações relevantes.
* **Arquitetura baseada em contratos legais**: Cada contrato inteligente é vinculado a um texto legal correspondente, permitindo aplicabilidade jurídica.
* **Alta escalabilidade**: Ao evitar a disseminação de dados para toda a rede, o Corda reduz drasticamente o overhead de comunicação e armazenamento.
* **Plataforma extensível com SDKs de tokenização**: Suporte nativo a tokens empresariais.
* **Baseado na JVM**: Os contratos e aplicativos (chamados **CorDapps**) são escritos em **Kotlin** ou **Java**, linguagens comuns no ecossistema corporativo.

**Arquitetura do Corda**

A arquitetura do Corda é centrada em alguns componentes principais:

* **Nós Corda**: Cada participante possui um nó Corda próprio, que executa os CorDapps e mantém o histórico de transações do próprio participante.
* **Notary**: Um serviço que fornece consenso e prevenção de gasto duplo. Pode ser configurado como um notário baseado em tempo, notário confiável ou notário com tolerância a falhas bizantinas.
* **Network Map**: Responsável por manter e distribuir informações sobre a rede, como os nós disponíveis e seus serviços.
* **CorDapps**: Aplicações descentralizadas que definem os fluxos de transações, contratos e esquemas de dados. Elas são instaladas em nós e contêm a lógica de negócios.

**Privacidade no Corda**

Privacidade é um princípio central do Corda. Em contraste com blockchains tradicionais, onde todas as transações são visíveis a todos os nós, no Corda os dados **só são compartilhados com os nós participantes diretamente na transação**. Isso é alcançado utilizando-se de criptografia, canais de comunicação privados e controles de acesso.

**Contratos inteligentes no Corda**

Os contratos no Corda são escritos em **Kotlin** ou **Java** e são vinculados a um documento legal. O Corda utiliza um modelo determinístico de execução para garantir que todos os nós executem os contratos da mesma forma, sem divergências.

**Fluxos (Flows)**

Fluxos são o coração da lógica de negócios no Corda. Um **Flow** define o processo de negociação e troca de mensagens entre os nós, garantindo que todos os passos sejam realizados em ordem e com a validação necessária. Flows são escritos como classes que estendem a API FlowLogic.

**O futuro do blockchain empresarial**

Embora o blockchain esteja sendo pesquisado, desenvolvido e discutido há mais de uma década, o blockchain empresarial ainda é uma área relativamente nova. Vários projetos empresariais estão sendo conduzidos como **provas de conceito (PoCs)** ou **projetos-piloto**, e alguns poucos já estão em **produção**. O setor está amadurecendo, mas ainda há muitos desafios a serem superados.

O futuro do blockchain empresarial é promissor, com as seguintes tendências esperadas:

* **Padronização**: A padronização entre plataformas ajudará na **interoperabilidade** e adoção em larga escala. Organizações como a EEA (Enterprise Ethereum Alliance) e o W3C estão trabalhando ativamente para definir padrões para blockchain.
* **Integração com tecnologias emergentes**: Blockchain será cada vez mais integrado com outras tecnologias disruptivas como **IA (inteligência artificial)**, **IoT (Internet das Coisas)**, **computação em nuvem** e **computação confidencial**. Isso ampliará significativamente os casos de uso empresariais.
* **Governança aprimorada**: Modelos de governança em blockchains empresariais evoluirão para permitir maior **flexibilidade**, **resiliência organizacional**, **tomada de decisões baseada em votos**, e conformidade regulatória.
* **Privacidade e segurança mais robustas**: Com o amadurecimento de técnicas como **provas de conhecimento zero (ZKPs)**, **computação multipartidária segura (MPC)** e **ambientes de execução confiáveis (TEEs)**, a **privacidade dos dados empresariais** em blockchain será significativamente reforçada.
* **Adoção setorial**: Espera-se que setores como **finanças**, **cadeia de suprimentos**, **saúde**, **seguros**, **imobiliário** e **governos** liderem a adoção do blockchain empresarial devido aos seus requisitos de confiança, transparência e eficiência.
* **Blockchain como Serviço (BaaS)**: Com a ascensão das ofertas BaaS de empresas como AWS, Azure e IBM, a barreira de entrada técnica será reduzida, permitindo que mais empresas experimentem soluções blockchain sem o ônus da gestão da infraestrutura.
* **Redes híbridas**: Redes que combinam características de blockchains públicos e privados — por exemplo, blockchains com transações privadas, mas ancoradas publicamente — se tornarão mais comuns.

**Resumo**

Nesta seção, abordamos os requisitos de blockchain empresarial, comparando com blockchains públicos, discutimos desafios e exploramos algumas plataformas proeminentes como **Quorum**, **Hyperledger Fabric** e **R3 Corda**. Também apresentamos uma estrutura de arquitetura empresarial usando o **TOGAF**, exploramos o papel da **nuvem** no contexto do blockchain, e consideramos o **futuro** da tecnologia blockchain no setor empresarial.

O blockchain empresarial, com sua promessa de descentralização controlada, transparência com privacidade, e confiança sem intermediários, está amadurecendo e pronto para desempenhar um papel fundamental no próximo salto da transformação digital empresarial.