KPMG

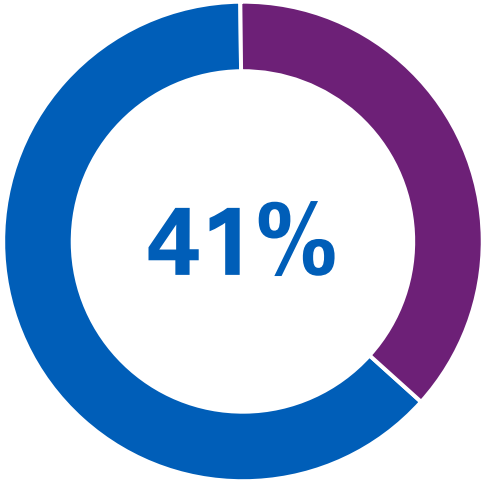
Blockchain

Insights de riscos de tecnologia KPMG

Março de 2022

O que é *blockchain*?

Blockchain é um sistema em que um registro de transações é mantido em diversos computadores (os *nós*) que estão vinculados em uma rede *peer-to-peer*. Isso elimina a necessidade de intermediários, como bancos ou corretoras, atuarem como terceiros.



dos líderes empresariais acreditam que suas empresas deveriam ter investido mais em *blockchain* nos últimos cinco anos[1].

US$ 19 bi

Esse é o valor previsto para 2024 em gastos globais em soluções de *blockchain*.[2]

[1] CISION PR NEWSWIRE. CFOs *Are Ready for Digital Transformation in 2021, New Survey Shows*. Disponível em: <https://apnews.com/press-release/pr-newswire/technology-public-opinion-computer-and-data-security-blockchain-social-affairs-aa60e382d418d63c3f8c72a523c89c5a>. 2021.

[2] YAHOO! FINANCE. *Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024, According to New IDC Spending Guide*. Disponível em: <https://finance.yahoo.com/news/global-spending-blockchain-solutions-forecast-123000872.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS5ici8&guce_referrer_sig=AQAAAK5BEmMLSJixGf8aUEemlG6nQMAqzBYzlT3jubFbbx6wfmJF5qWLEfXC1iY-p1WRxVXhmsC3DewvT6BlmnsVKLMlwK-Zfc_OoIzesLwrb1moMX6PPkdCx6WBORuIm3RL-IAS670eMTHECos80gzWuhp-yfVO3Xib85d5g1FydgNt>. 2021.

Como o *blockchain* funciona?

Criptografia

Um *blockchain* é uma cadeia de blocos que contém informações de transações:

- Cada bloco de dados contém uma chave *hash* exclusiva, que é como uma impressão digital, utilizada para identificar um bloco e seu conteúdo.
- Cada um desses blocos contém transações, um hash e uma cópia do *hash* do bloco anterior (com exceção do bloco gênesis, que não possui o *hash* do bloco anterior). Esse conceito torna o *blockchain* imutável. Caso os dados de um bloco anterior mudem, seu *hash* será modificado, desconectando-o da cadeia dos blocos subsequentes.

Registro distribuído

Em vez de depender de uma autoridade central para gerenciar o registro, os *blockchains* usam uma rede *peer-to-peer* distribuída:

- Quando alguém ingressa na rede, é realizado o *download* de uma cópia completa do *blockchain*. Cada novo usuário ou computador na rede é chamado de nó.
- A arquitetura *peer-to-peer* distribuída oferece maior disponibilidade do que as redes tradicionais baseadas em cliente-servidor, pois não há um ponto único de falha.

Consenso

Novas transações são enviadas para todos os *nós*, que são validadas e agrupadas em blocos:

- O consenso garante que os pares na rede cheguem a um acordo sobre um estado consistente de registros.
- Uma vez que o consenso é obtido, o novo bloco é postado no *blockchain* de cada *nó*.
- Os *nós* rejeitarão blocos cujos dados violem as regras do protocolo ou pareçam ter sido adulterados.

Mecanismos de consenso comuns incluem a Prova de Trabalho (*Proof of Work* ou PoW) e a Prova de Participação (*Proof of Stake* ou PoS).

Contratos inteligentes

A principal diferença entre um contrato tradicional e um inteligente é que os últimos são automatizados:

- Um contrato é criado entre as partes.
- As partes podem optar por continuar anônimas.
- Gatilhos predefinidos são iniciados.
- O contrato é executado automaticamente, conforme definido pelo código-fonte.
- Um participante pode analisar todas as atividades e tomar decisões fundamentadas.
- Os dados capturados podem ser usados para análises e relatórios.
- Os dados são então alimentados nos *blockchains* e usados para execução de contratos inteligentes de fontes externas, especificamente feeds de dados e APIs. Um *blockchain* não pode buscar dados diretamente. Esses *feeds* em tempo real são chamados de oráculos, que funcionam de maneira muito similar ao *middleware* entre os dados e os contratos inteligentes.

Principais riscos do *blockchain*

A adoção da tecnologia de *blockchain* exemplifica o investimento de uma empresa em inovação, mas surgem novos riscos. Para explorar todo o potencial das tecnologias de registros distribuídos, as organizações devem identificar e mitigar todos os riscos apresentados pela adoção da tecnologia de maneira proativa.
A KPMG pode contribuir para maximizar o investimento da sua empresa, enquanto ajuda a gerenciar riscos potenciais.

Governança

— Projeto e padrões de *blockchain*.
— Políticas e procedimentos.
— Gestão de fornecedores.
— Gerenciamento de acesso de identidades.
— Regulamentação e *compliance*.
— Procedência dos ativos.
— Prevenção à lavagem de dinheiro.
— Sanções.

Infrastructure

— Riscos da rede de *blockchain*.
— Vulnerabilidades de *software*.
— Gerenciamento de protocolos.
— Integração.
— Interoperabilidade.
— Gerenciamento de nós.
— Mecanismos de consenso.

Contratos inteligentes

— Desenvolvimento e projeto de contratos inteligentes.
— Revisão e manutenção do código.
— Riscos de negação de serviço.
— Risco de fontes externas.
— Riscos legais.

Dados

—Gerenciamento de dados.
— Gerenciamento de privacidade.
— Recuperação de desastres.
— Gerenciamento das informações *offchain*.
— *Blockchain bloat*.
— Integridade de dados.
— *Know your Customer* (Conheça o seu Cliente).

Gerenciamento de chaves

— Gerenciamento de chaves públicas e privadas.
— Entropia.
— Segurança de chaves/protocolos.
— Fragmentação (*sharding*).
— Assinatura múltipla.
— Gerenciamento de carteira.
— Acesso do Módulo de Segurança de *Hardware* (*Hardware Security Module* - HSM).

Principais riscos *do blockchain*

Desenvolvimento

— **Padrões subdesenvolvidos:**
  - O *blockchain* atualmente não tem padrões adequados devido ao seu rápido crescimento. Com diferentes organizações trabalhando no seu próprio *blockchain*, é difícil padronizá-los.

— **Padronização entre indústrias e *blockchains*:**
  - A grande variedade de estruturas significa que há uma falta de padronização. Esse é potencialmente um dos maiores riscos que os projetos de *blockchain* atuais enfrentam. Esses padrões aplicam-se a todo o seu ecossistema, incluindo ofertas iniciais de moedas, criptomoedas, estruturas e assim por diante.

— **Integração e interoperabilidade em sistemas existentes e entre *blockchains.***

— **Código não testado:**
  - A qualidade do código continua sendo uma grande preocupação para a maioria das soluções de *blockchain*. As organizações descentralizadas precisam ter um cuidado adicional ao implementar suas soluções. Um exemplo é a Organização Autônoma Descentralizada (*Decentralized Autonomous Organization* - DAO). Trata-se de um sistema autônomo que automatiza toda a organização.
  - O DAO Hack é um dos piores *hacks* em relação à tecnologia de *blockchain*. Criado em 2016 e conhecido como The DAO, o incidente resultou na perda de aproximadamente US$ 50 milhões em *Ether* por meio de uma exploração no código-fonte aberto[3].

[3] FINLEY, Klint. *A $50 million hack just showed that DAO was all too human.* Disponível em: <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>. 2016.

Os casos de uso de *blockchain* abrangem diversos setores e áreas de atuação

Varejo

Fidelidade *tokenizada*

Preparação de um ecossistema de fidelidade entre aliados impulsionado por uma única carteira baseada em *blockchain*, que permite que os clientes acumulem, resgatem ou convertam pontos de fidelidade facilmente nas lojas e em ofertas de serviços da empresa.

Assistência médica e ciências da vida

Cadeia de suprimentos de medicamentos

A infraestrutura de confiança digital, apoiada pelo *blockchain*, possibilita que os profissionais autentiquem vacinas, validem a capacidade de atender pedidos, prevejam a demanda e tomem ações preventivas contra a escassez.

Moeda digital de bancos centrais

Moeda virtual

Aproveitamento do registro distribuído para implementar uma estratégia de moeda virtual, com o objetivo de apoiar o desenvolvimento da economia nacional e diversificar as fontes de receita dos bancos centrais.

Compras

Monitoramento de ativos imobilizados

Rastreamento do ciclo de vida da expedição, descarte, distribuição e arrendamento de ativos físicos, como *laptops*, impressoras e copiadoras, entre outros, para reduzir custos administrativos e automatizar processos manuais ineficientes.

Manufatura

Procedência de peças e rastreamento aduaneiro

Aproveitamento do registro digital para rastrear peças conforme elas são enviadas, importadas, montadas e exportadas por meio de locais internacionais para otimizar pagamentos de impostos e gestão de estoques.

Governo Federal

Gestão de subsídios

Transparência e rastreabilidade na distribuição de fundos com um registro de transações auditável e meios simplificados para identificar e verificar destinatários qualificados.

Como a KPMG pode ajudar

A KPMG disponibiliza sua experiência para entender, desenvolver e manter a segurança e a conformidade de tecnologias de registros distribuídos.

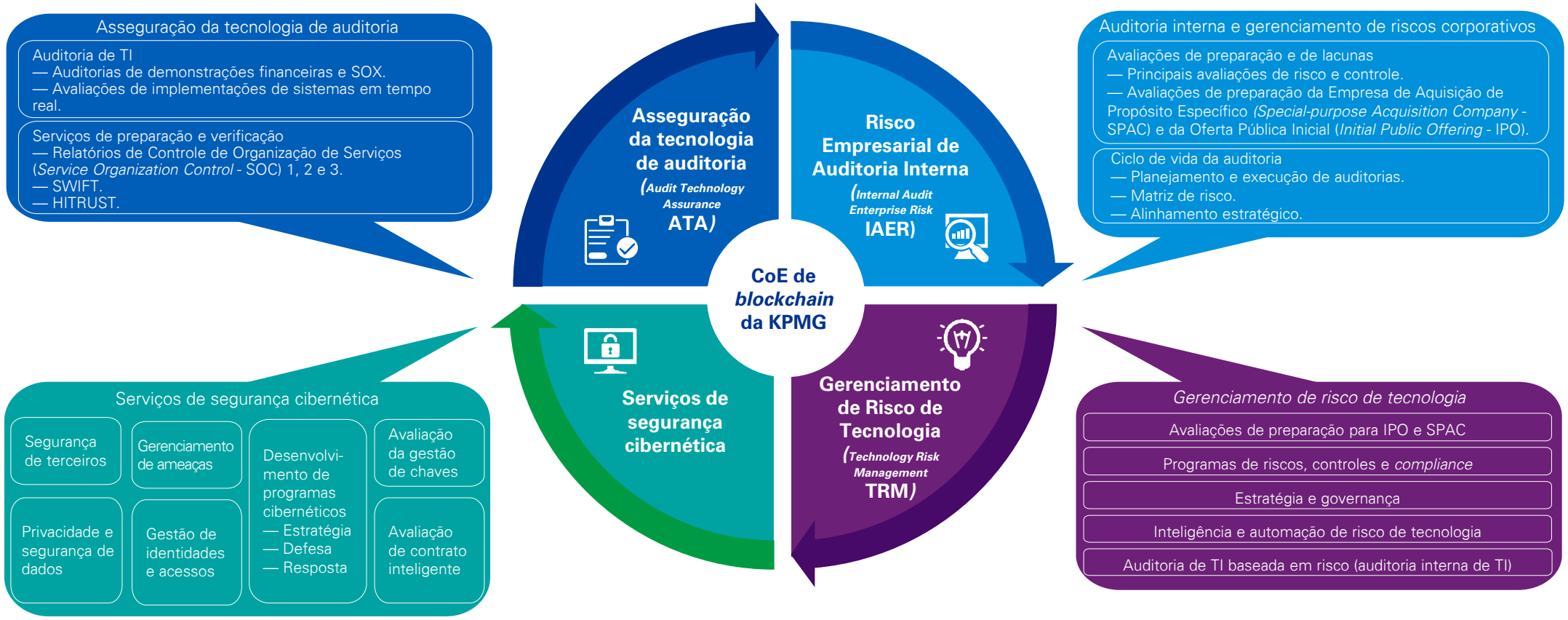
Nossos serviços abrangem todo o ciclo de vida de soluções de *blockchain* e negócios de criptomoedas. Essa atuação inclui planejamento estratégico, orientação regulatória, avaliação de riscos, projeto e avaliação de controles, auditoria de TI e suporte à verificação, além de segurança cibernética e da informação.

Além disso, trabalhamos em estreita colaboração com as linhas de serviços de auditoria, tributos e consultoria para ajudar a disponibilizar uma oferta completa de serviços para os nossos clientes.

Como a KPMG pode ajudar

Soluções de *blockchain* da KPMG

Nossos serviços ajudam nossos clientes a identificar, gerenciar e mitigar os riscos apresentados pela adoção de tecnologias de registros distribuídos.



Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber Security da KPMG no Brasil
lantonio@kpmg.com.br

A prestação de todos ou de alguns dos serviços aqui descritos pode não ser permitida para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br

/kpmgbrasil