BLOCKCHAIN
TECHNOLOGY PRIMER

Versão 1.0

Este material é uma tradução livre do documento de mesmo nome:
"Blockchain Technology Primer - Version 1.0 | July 2018", desenvolvido por grupo de trabalho do IAB TECH LAB.

Sumário Executivo

A tecnologia Blockchain gerou uma publicidade sem precedentes nos últimos anos. Tendo começado como uma rede de bitcoins para gerenciar transações financeiras, esta tecnologia tem sido vista como uma solução milagrosa para resolver todos os problemas, desde a gestão de crises de refugiados à energia para o rastreamento de abastecimento de alimentos.

Este documento é um mergulho na tecnologia blockchain para entender a história e os fundamentos, assim como para explicar seus vários componentes e implementações comercialmente disponíveis.

O objetivo é educar o leitor sobre os detalhes da tecnologia para que eles possam desenvolver:

1. Uma perspectiva sobre sua aplicação para casos de uso específico da tecnologia em publicidade.
2. Uma compreensão sobre as opções tecnológicas disponíveis
3. Uma compreensão sobre as implicações operacionais e de negócios da implementação de uma solução blockchain

Este documento é acompanhado por *IAB Tech Lab Resources Wiki*, uma coleção com curadoria de recursos de outras leituras disponíveis na Web para aprender mais e se aprofundar em tópicos específicos.

Sobre o IAB Tech Lab

O Laboratório de Tecnologia do IAB é um grupo de pesquisa e desenvolvimento, independente, internacional encarregado de produzir e ajudar as empresas a implementar normas técnicas globais do setor. Composto por profissionais de marketing, agências de publicidade, editoras digitais e empresas de tecnologia, bem como por outras empresas com interesses na área de marketing interativo, o objetivo do Laboratório de Tecnologia do IAB é reduzir o atrito associado à cadeia de fornecimento de publicidade e marketing digital, enquanto contribui para o crescimento seguro do setor. Aprenda mais sobre o IAB Tech Lab **aqui**.

Mais informações disponíveis no link: https://www.iabtechlab.com

AS NORMAS, ESPECIFICAÇÕES, DIRETRIZES DE MEDIÇÃO E QUAISQUER OUTROS MATERIAIS OU SERVIÇOS PRESTADOS OU USADOS POR VOCÊ, DE ACORDO COM ESTE INSTRUMENTO, (OS "PRODUTOS E SERVIÇOS") SÃO FORNECIDOS "NO ESTADO EM QUE SE ENCONTRAM" E "CONFORME DISPONÍVEIS" E O IAB TECHNOLOGY LABORATORY, INC. ("TECH LAB") NÃO DÁ GARANTIA COM RESPEITO AOS MESMOS E, POR MEIO DESTE, NEGA TODAS AS GARANTIAS EXPRESSAS, IMPLÍCITAS OU LEGAIS, INCLUINDO, SEM LIMITAÇÃO, QUAISQUER GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA, DISPONIBILIDADE, OPERAÇÃO SEM ERROS OU ININTERRUPTA, E QUAISQUER GARANTIAS DECORRENTES DO CURSO DE NEGOCIAÇÕES, DE DESEMPENHO OU USO DE COMÉRCIO. NA MEDIDA EM QUE, COMO UMA QUESTÃO DE LEI APLICÁVEL, O TECH LAB NÃO PODE NEGAR QUALQUER GARANTIA IMPLÍCITA, O ESCOPO E A DURAÇÃO DESSAS GARANTIAS SERÃO O MÍNIMO PERMITIDO POR TAL LEGISLAÇÃO. OS PRODUTOS E SERVIÇOS NÃO CONSTITUEM ACONSELHAMENTO JURÍDICO OU DE NEGÓCIOS. O TECH LAB NÃO GARANTE QUE OS PRODUTOS E SERVIÇOS PRESTADOS OU UTILIZADOS POR VOCÊ FARÃO COM QUE VOCÊ E/OU SEUS PRODUTOS OU SERVIÇOS ESTEJAM EM CONFORMIDADE COM TODAS AS LEIS, REGULAMENTOS OU ESTRUTURAS AUTO-REGULATÓRIAS APLICÁVEIS, E VOCÊ É O ÚNICO RESPONSÁVEL PELA CONFORMIDADE COM OS MESMOS, INCLUINDO, MAS SEM LIMITAR-SE A: LEIS DE PROTEÇÃO DE DADOS, TAL COMO A LEI DE PROTEÇÃO DE INFORMAÇÕES PESSOAIS E DOCUMENTOS ELETRÔNICOS (CANADÁ), A DIRETIVA DE PROTEÇÃO DE DADOS (UE), A E-DIRETIVA DE PRIVACIDADE (UE), O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (UE) E O E-REGULAMENTO DE PRIVACIDADE (UE) COMO E QUANDO ELES ENTRAREM EM VIGOR.

Grupo de Trabalho de Blockchain

A Blockchain Technology Primer foi desenvolvida por um subgrupo do Grupo de Trabalho de Blockchain do IAB Tech Lab. Os principais contribuidores deste subgrupo foram:

Michael Freyberger	*AppNexus*
Christopher Beach	*Receptiv*
Ezgi Cengiz	*Twitter*
Breaux Walker	*Kochava Inc.*
Alexei Furs	*Optimatic*
Archie Sharma	*OpenX*
David Jung	*Meredith Digital*
Pooja Nayak	*Starcom Worldwide*
Adrian Domek	*Parsec Media*
Ryan Gauss	*AerServ*
Demitri Nikolaou	*Spectrum Reach*
Miguel Morales	*Lucidity*
Amit Shetty	*IAB*
Jeremy Stanton	*Amino Payments*
Dustin Suchter	*SRAX*

*Em 26 de junho de 2018

Índice

Introdução

Atualmente, muitas vezes *"Blockchain é uma solução que procura por um problema"* é o título de muitos artigos à medida que a tecnologia Blockchain evoluiu de Bitcoin para Ethereum para vários outros protocolos e aplicativos que tratam não apenas de serviços financeiros, mas diversos outros setores, incluindo tecnologia de mídia e publicidade.

Blockchain foi desenvolvida para solucionar um problema muito específico de armazenamento e transferência de ativos digitais entre dois pares sem a necessidade de um intermediário. À medida que o mundo transita para a representação digital de ativos, existem apenas duas maneiras de gerenciar as transações digitais - seja através de terceiros intermediários, por exemplo, bancos ou processadores de cartão de crédito, que é o que fazemos atualmente, ou redes como as de bitcoins com protocolos bem definidos para autenticar as empresas, validar as suas participações de ativos e confirmar as transações entre duas empresas.

Como a tecnologia blockchain possibilita transações digitais sem erros e sem a necessidade de um intermediário para fazer as verificações e balanços necessários?

Como intermediário, o banco processa transações a fim de que elas ocorram e, portanto, conheçam o valor detido por uma empresa em seu sistema. É, portanto, capaz de realizar uma autorização de fundos sem erros.

Em uma blockchain, esta tarefa é realizada por usuários da blockchain para resolver um quebra-cabeça criptográfico e acrescentar uma transação a um conjunto anterior de transações na ordem correta. Este conjunto de transações é um "bloco".

Uma maioria de usuários deve aceitar a validade deste bloco adicionando outros blocos a esta "cadeia" de blocos. Como os futuros blocos dependem dos blocos anteriores, é impossível alterar ou apagar um bloco. Razão pela qual o blockchain é "imutável".

Cada uma das transações é visível a todos, de forma que os usuários podem verificar se o remetente tem os ativos que alegam ter, o que elimina um terceiro. Isto é feito pelo compartilhamento de um banco de dados ou livro-razão e cada usuário, teoricamente, pode ter uma cópia de todas as transações. Assim, um blockchain é um livro-razão “distribuído”.

Embora muitas pessoas prefiram entender blockchain como sendo um banco de dados, ele é muito mais do que um banco de dados. É uma combinação de bancos de dados distribuídos ou compartilhados com permissão pública ou privada para armazenar e acessar transações, métodos consensuais para aprovar e registrar transações, uso inteligente de criptografia para autenticar uma empresa, moeda para pagar a manutenção do sistema e recompensar aqueles que fornecem os recursos para manter o sistema, bem como para armazenar o valor de um ativo, e com contratos inteligentes, uma maneira de impor condições ou automatizar processos a serem seguidos.

É devido a esses componentes que a tecnologia blockchain pode ser aplicada a muitos casos de uso além de dinheiros ou bitcoins, por exemplo, o protocolo Ethereum acrescenta capacidades para executar programas ou contratos não hierárquicos e aplicativos que permitem que ele seja aplicado a diversas operações além de um caso de uso de transferência de dinheiro.

Neste documento exploraremos todos os diversos componentes e conceitos da tecnologia blockchain e dos elementos operacionais.

Tecnologias de Livro-razão Distribuído

Tecnologias de livro-razão distribuído (DLT) foram precursoras do blockchain e compreender as DLTs é um bom ponto de partida. Podemos até mesmo considerar o blockchain como sendo uma implementação de DLT.

Um livro-razão ou registro, por definição, é um processo pelo qual mantém-se registros de todas as transações de uma empresa ou organização. Desde o início da civilização, os livros-razão foram usados para manter transações econômicas para registrar participações de ativos, contratos e pagamentos de bens e serviços. Um livro-razão central é regido por uma única entidade a quem é confiada a manutenção adequada de verificações e balanços. Um livro-razão distribuído funciona como uma "rede" na qual os usuários aprovam registros de transações. Os dados são replicados para múltiplos usuários e não há um banco de dados.

Cada usuário ou computador da rede de DLT tem que determinar por si mesmo e em seguida os usuários "votam" na versão correta do registro de transações. Com a aprovação de consenso, o livro-razão é atualizado com os detalhes da transação. Todos os usuários ou computadores da rede mantêm suas próprias cópias do livro-razão. Não existe um proprietário ou administrador central do livro-razão distribuído. Os dados são armazenados e compartilhados entre todos na grande rede, independentemente da sua localização ou instituição. Qualquer alteração no registro reflete imediatamente em todas as cópias do livro-razão distribuído. Pode ser eletrônico, financeiro, jurídico ou físico. A segurança e precisão do livro-razão distribuído são mantidas por meio de criptografia.

Bancos de Dados e Aplicativos Descentralizados

Bancos de dados e aplicativos descentralizados existem há muito tempo.

Implementações populares de aplicativos descentralizados incluem *Bittorrent* e IPFS[1], bem como outros como o *Emule*[2] para música e outros aplicativos de compartilhamento de mídia. Atributos comuns entre sistemas distribuídos incluem a capacidade de escalonar adicionando novos nós, balanceamento de carga de dados entre nós e capacidade de confirmar os conteúdos replicados entre muitos nós.

Privada versus Pública

Quem pode participar de uma DLT?

Toda rede de DLT tem seu próprio protocolo que rege as regras de participação, confirmando o registro das transações e mantendo o registro. A participação pode ser pública ou privada. Na DLT pública qualquer um pode participar da rede, enquanto que na DLT privada existe um mecanismo de permissão sobre quem pode ser autorizado a entrar na rede.

Pública

Exemplos populares de livros-razão públicos distribuídos incluem Bitcoin e Ethereum. As vantagens de uma rede pública é que uma entidade ou grupo de entidades não pode facilmente assumir o controle do livro-razão e injetar transações fraudulentas. Parte da segurança dos livros-razão públicos vem da capacidade de qualquer pessoa ser capaz de confirmar transações atuais e passadas sem depender de terceiros intermediários.

Outra família dos livros-razão públicos inclui zCash e Monero. Esses livros-razão, embora públicos e auditáveis, são totalmente privados. Somente as entidades que participaram de uma transação podem visualizar os conteúdos dessas transações.

Ambas as famílias de livros-razão públicos usam mecanismos de consenso altamente

[1] "IPFS é a Web Distribuída". https://ipfs.io/.
[2] https://www.emule-project.net/home/perl/general.cgi?l=1

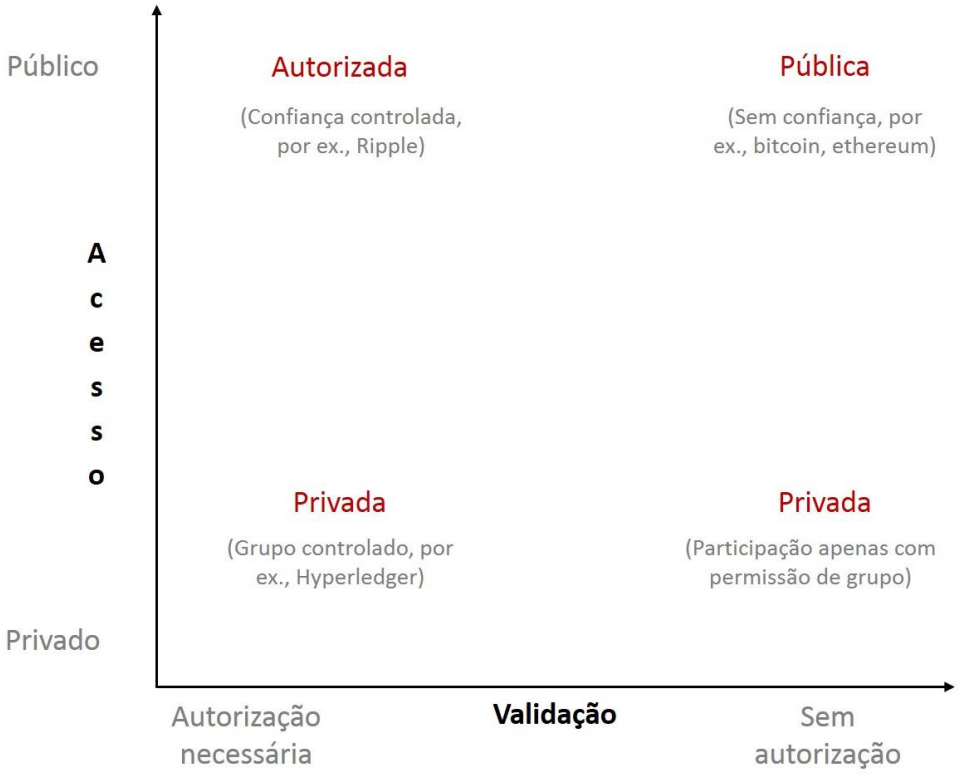
distribuídos como Prova de Trabalho ou Prova de Participação. Esses tipos de mecanismos de consenso exigem *tokens* ou moedas para criar os incentivos econômicos para proteger a rede. No entanto, devido à grande distribuição de nós (nodes), o número de transações que os livros-razão públicos podem lidar limita-se atualmente a ~15/seg[3].

Privada

Uma terceira família de livros-razão distribuídos são livros-razão privados, como Quorum e HyperLedger. Os livros-razão são propriedades exclusivas, sendo completamente protegidos contra participantes não autorizados, mantêm todos os dados de transação privados e são acessíveis apenas a participantes do livro-razão. No entanto, devido ao menor número de nós de confirmação de participantes, é mais vulnerável a 51% de ataques.

Os livros-razão privados tendem a empregar mecanismos de consenso de baixa distribuição, tais como a Tolerância Prática a Falhas Bizantinas (PBFT), Raft ou Paxos. Devido a limitações inerentes nesses mecanismos de consenso, somente um número limitado de nós poderá participar deles. Essa família de mecanismos de consenso não exige *tokens* ou moedas para funcionar. Devido ao número limitado de nós, o número de transações de livros-razão privados é muito mais alto do que os atuais livros-razão públicos e poderão ser limitados a ~20k/seg[4] dependendo do número de nós participantes.

[3] "Desempenho e Escalabilidade de Redes Blockchain e Inteligentes ... - DiVA". https://umu.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf
[4] "Desempenho e Escalabilidade de Redes Blockchain e Inteligentes ... - DiVA". https://umu.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf Acessado em 9 de fevereiro de 2018.



Consenso

Blockchains são redes *peer-to-peer* (ponto-a-ponto) sem administrador ou poder central. É crucial garantir que os participantes da rede cheguem a um consenso sobre o estado do livro-razão, como por exemplo, a singularidade e a ordem dos registros. Isto é feito por meio de algoritmos de consenso que utilizam métodos diferentes para garantir que a ordem certa e a singularidade das transações sejam determinadas e validadas por um número suficiente de usuários a serem acrescentados ao livro-razão.

Métodos de Consenso

Abaixo seguem alguns métodos de consenso:

Prova de Trabalho

A Prova de Trabalho descreve um sistema que exige uma quantia substancial, porém, viável de esforço para determinar usos mal-intencionados do poder de processamento, tal como o envio de e-mails spam ou lançamento de ataques de negação de serviços. O conceito foi adaptado para uma rede *peer-to-peer* por Hal Finney, em 2004, por meio da ideia de "prova de trabalho reutilizável". Bitcoin se tornou a primeira aplicação amplamente adotada da ideia de Finney. A prova de trabalho também forma a base de muitas outras criptomoedas. Em bitcoin, a prova de trabalho requer que o minerador identifique e confirme corretamente o bloco anterior, verifique a lista de transações corretamente desde o bloco anterior e adivinhe um número especial chamado *nonce*.

Prova de Participação

O conceito da Prova de Participação (PoS) afirma que um indivíduo pode explorar ou aprovar uma transação com base em quantas moedas ele ou ela detém por meio de votação. Isto implica que, quanto mais Bitcoins ou altcoins uma carteira tiver, mais poder de voto o usuário terá.

Além do número de moedas detidas outros fatores, como idade ou saldo mínimo de endereço, também podem ser incluídos para determinar a participação.

Prova de Queima

A Prova de Queima é um método de consenso pelo qual um minerador é obrigado a queimar ou desperdiçar moedas de uma prova de trabalho geralmente diferentes de moedas da prova de queima que estão sendo verificadas, tornando-as indisponíveis. Isto é feito enviando-as para um *eater address* (endereço indisponível). Esta transação “queimada” é registrada e confirmada e o usuário que “queimar” a moeda é recompensado com as moedas de sua própria moeda blockchain. A ideia principal por

trás da prova de queima é que o usuário está demonstrando comprometimento a longo prazo ao assumir uma perda a curto prazo. Quanto mais moedas um usuário queimar, mais recompensas ele terá, o que pode gerar o problema de uma pessoa rica ficar ainda mais rica. As vantagens da prova de queima são mais estabilidade enquanto os usuários apostam no longo prazo, bem como distribuição e descentralização justas.

Prova de Atividade

A Prova de Atividade é uma abordagem cruzada que combina Prova de Trabalho e Prova de Participação. Primeiro, a Prova de Trabalho é realizada para identificar um bloco vencedor e, a seguir, um conjunto de usuários escolhidos faz a validação, alcançando assim o consenso.

Prova de Tempo Decorrido (PoET)

A Prova de Tempo Decorrido (PoET) da Fabricante de Chips Intel é outro algoritmo de consenso que objetiva alcançar um consenso usando instruções seguras colocadas nos chips de computador amplamente disponíveis da Intel. A PoET explora características de chips de computador (de nós) com um alto grau de aleatoriedade segura, seleciona um líder (nó) para criar um novo bloco. A PoET assemelha-se à Tolerância Simplificada a Falhas Bizantinas (SBFT) no que se refere a eliminar a exigência de dispendiosos recursos computacionais. Cada nó de validação ou validador requer um tempo de espera de um Ambiente de Execução Confiável (TEE), o qual refere-se à uma área especialmente designada dentro de um chip, também chamado de *Software Guard Extension (SGX)*. O líder dentre um grupo de nós de validação é eleito por meio de um sistema de loteria no qual o nó com o menor tempo de espera é considerado o vencedor. As instruções do protocolo no SGX produzem um certificado (prova de espera) para o nó vencedor, o qual pode ser confirmado por outros nós na rede.

Tolerância Simplificada a Falhas Bizantinas (SBFT)

Os principais inconvenientes de se usar o consenso Prova de Trabalho (PoW) é o seu

imenso consumo de energia e capacidade limitada de processar as transações rapidamente. Assim, o PoW mostra-se inadequado para aplicativos empresariais que precisam de escala e fornecer transações rápidas.

Uma vez que todos os participantes da rede são confiáveis e se conhecem em um blockchain autorizado, todas as partes interessadas podem concordar com uma arquitetura personalizada com um protocolo de consenso que possa atender aos requisitos de escalabilidade e desempenho dos aplicativos de negócios. A Tolerância Simplificada a Falhas Bizantinas (SBFT) é um desses algoritmos de consenso e foi projetado especificamente para escalabilidade e rapidez. Diferentemente do que ocorre na PoW, onde todos os nós são idênticos entre si, os nós especializados da SBFT têm papéis diferentes para alcançar o consenso e gerenciar o estado do livro-razão.

A SBFT é mais eficiente em termos computacionais do que a PoW porque os nós não competem entre si e nem gastam grandes quantidades de recursos computacionais tentando solucionar um quebra-cabeça. Ao contrário, um nó gerador (replicador máster) é pré-selecionado para criar um novo bloco, o qual contribui tanto para a necessidade de rapidez como de escalabilidade dos aplicativos de negócios. A natureza modular da rede facilita a identificação e a remoção rápida de nós defeituosos e mal-intencionados, adicionando uma camada extra de segurança à rede.

Mineração

Assim como cavamos fundo a terra à procura de materiais valiosos como ouro, cobre ou outros minerais e commodities de materiais, como o carvão, a mineração no blockchain é realizada para obter moedas ou moeda da rede.

A mineração de moedas no blockchain é diferente da mineração de ouro. Além de obter moedas (por exemplo, bitcoins), os mineradores também prestam um serviço para a rede blockchain, isto é, eles validam e registram as transações de maneira descentralizada usando algum dos métodos de consenso supramencionados e aplicados pelo protocolo da rede.

As redes blockchain dependem dos mineradores para realizar tarefas que um intermediário pode fazer normalmente em transações de negócios, por exemplo, no caso da rede Bitcoin, os mineradores realizam tarefas semelhantes aos caixas bancários, verificando se uma determinada transferência de bitcoins esteja entre duas contas válidas, validando a autenticidade das assinaturas do remetente e que as moedas sendo transferidas são de propriedade do remetente.

Assim, a mineração permite a descentralização em uma rede blockchain.

Contratos Inteligentes

O que é um Contrato Inteligente?

Contrato inteligente é um conceito introduzido pela rede blockchain Ethereum. É um programa de computador capaz de executar um conjunto de funções pré-definidas quando ocorre uma condição especificada ou conjunto de condições. O programa é armazenado no livro-razão distribuído e é capaz de escrever a alteração resultante no livro-razão distribuído.

Um contrato “inteligente” é uma relação que pode ser estabelecida por meio da interação de agentes eletrônicos e/ou que pode ser realizada ou aplicada, no todo ou em parte, mediante a satisfação de um conjunto de condições pré-programadas. Nick Szabo forneceu um exemplo inicial de um contrato “inteligente”, o qual era simplesmente uma máquina de venda automática que dispensa mercadorias mediante pagamento de uma soma específica.

Um contrato “inteligente” poderá, mas não precisa, envolver o emprego ou implantação de uma blockchain. Ao usar um contrato “inteligente” que incorpora tecnologia blockchain, o algoritmo adjacente se baseia em um consenso entre as

partes ou por meio da metodologia contratual[5].

Um outro exemplo de contrato "inteligente" que não emprega uma blockchain é quando se usa um agente eletrônico para determinar quando comprar um item. Por exemplo, a empresa ABC usa um agente eletrônico para determinar quando comprar um determinado item com base em necessidade combinada com preços disponíveis e quantos itens distintos comprar. A empresa XYZ vende este item específico e usa um agente eletrônico para negociar seus contratos baseado em seu fornecimento disponível e no mercado em geral. ABC precisa de 1 milhão desses itens e está disposta a pagar até $1/item. A XYZ tem 100 milhões desses itens, os quais ela pode vender e está disposta a vender por $0,50/item. A ABC e a XYZ entram em negociações usando agentes eletrônicos que foram programados para estabelecer condições de entrega, volumes e preços baseados nos parâmetros estabelecidos. Desta forma, ABC e XYZ chegam a um acordo por meio da interação dos agentes eletrônicos; a ABC recebe o item necessário e paga a XYZ o valor acordado. Em nenhum ponto da transação, após os agentes eletrônicos terem sido programados e implantados, houve qualquer intervenção humana no contrato para analisar, negociar ou acordar, nem houve a necessidade de usar blockchain para executar ou realizar a dita transação[6].

Implicações de Contratos Inteligentes

Desintermediação total de contratos: a moeda do blockchain elimina o intermediário de reconciliação e distribuição de fundos. Portanto, os contratos inteligentes podem eliminar intermediários contratuais[8].

Programas autoaplicáveis: contratos inteligentes podem conter códigos que

[5] Craig A. de Ridder, Mercedes K. Tunstall, Nathalie Prescott, *Recognition of Smart Contracts* [Reconhecimento de Contratos Inteligentes] https://www.pillsburylaw.com/en/news-and-insights/recognition-of-smart-contracts.html
[6] Max Raskin, *The Law and Legality of Smart Contracts* (A Lei e Legalidade dos Contratos Inteligentes), abril de 2017, Georgetown Law Review https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/

preveem recursos jurídicos ou mecanismos de aplicação que ocorrem automaticamente com base em determinadas condições, gerando, assim, contratos autoaplicáveis.

Contratos flexíveis: e mais, contratos inteligentes e blockchain podem marcar o retorno dos contratos comerciais de consumo com disposições padrão. Atualmente, contratos com condições de serviços digitais não contemplam nenhuma disposição para alterar ou declinar determinadas disposições contratuais. Mas com os contratos inteligentes autoexecutáveis e autoaplicáveis, a possibilidade de prévia programação de condições pode permitir estruturas de preços variáveis de bens ou serviços, dependendo de uma série de condições que são aceitas ou rejeitadas. A escolha do consumidor ou da empresa pode ser feita por agentes automáticos programados no blockchain para se comportarem conforme as preferências estabelecidas.

Criptografia e *Hashing*

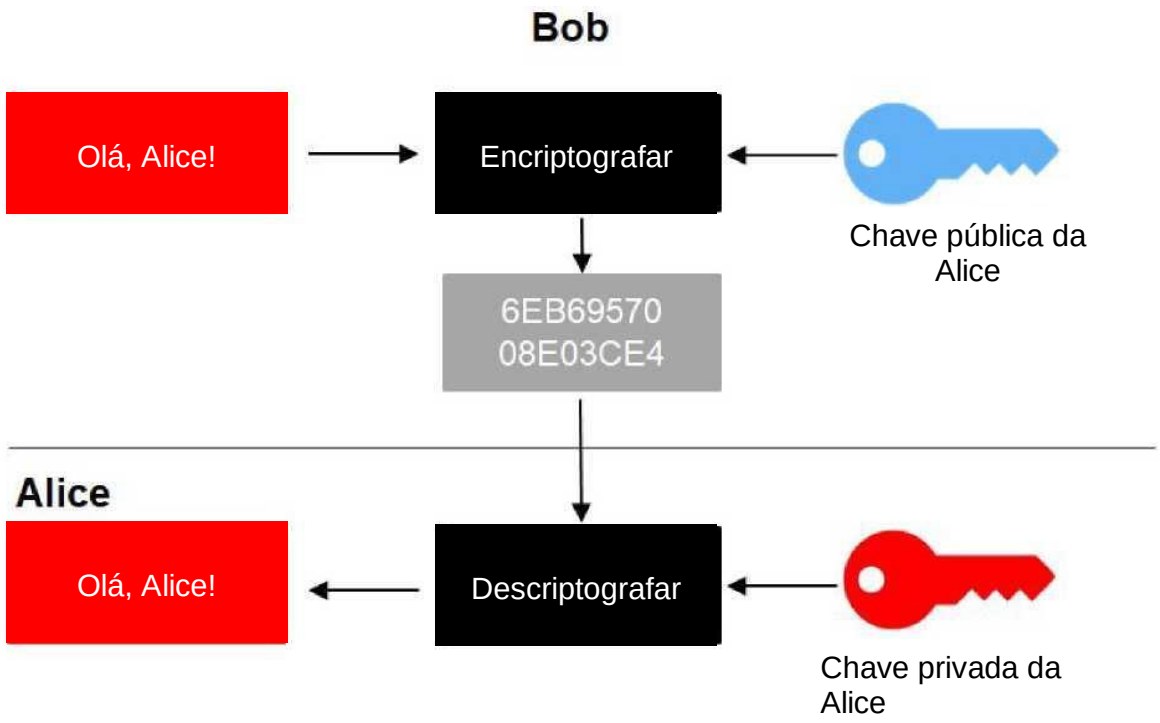
Criptografia é uma maneira de ocultar e revelar, mais comumente conhecida como criptografando e descriptografando dados ou conteúdo de mensagens. Desenvolve ou usa regras que impedem partes externas ou o público de ler mensagens encriptografadas para segurança da informação. Na criptografia, dados ou informações são convertidos em textos inúteis ou sem sentido com base em regras matemáticas. Geralmente isto é feito usando a chamada “chave”, comumente chamada de “chave privada”. Para descriptografar ou recuperar a mensagem para o seu formato original, é preciso da chave privada ou de uma chave pública emitida por um proprietário de chave privada. Isto garante a segurança da informação.

Criptografia em Blockchain

No blockchain, a criptografia é usada para as duas finalidades a seguir:

1. Proteger a identidade do remetente de transações;
2. Garantir que registros passados não possam ser adulterados.

O blockchain usa uma forma de criptografia conhecida como chave pública ou criptografia assimétrica. Esta forma usa a combinação de chave privada de um remetente e a chave pública do destinatário para criptografar a transação e a chave privada do destinatário e a chave pública do remetente para descriptografar a mensagem. Um usuário pode compartilhar sua chave pública com qualquer pessoa sem medo de revelar a própria chave privada. Isto garante a segurança da informação, assim como a identidade do remetente e do destinatário.



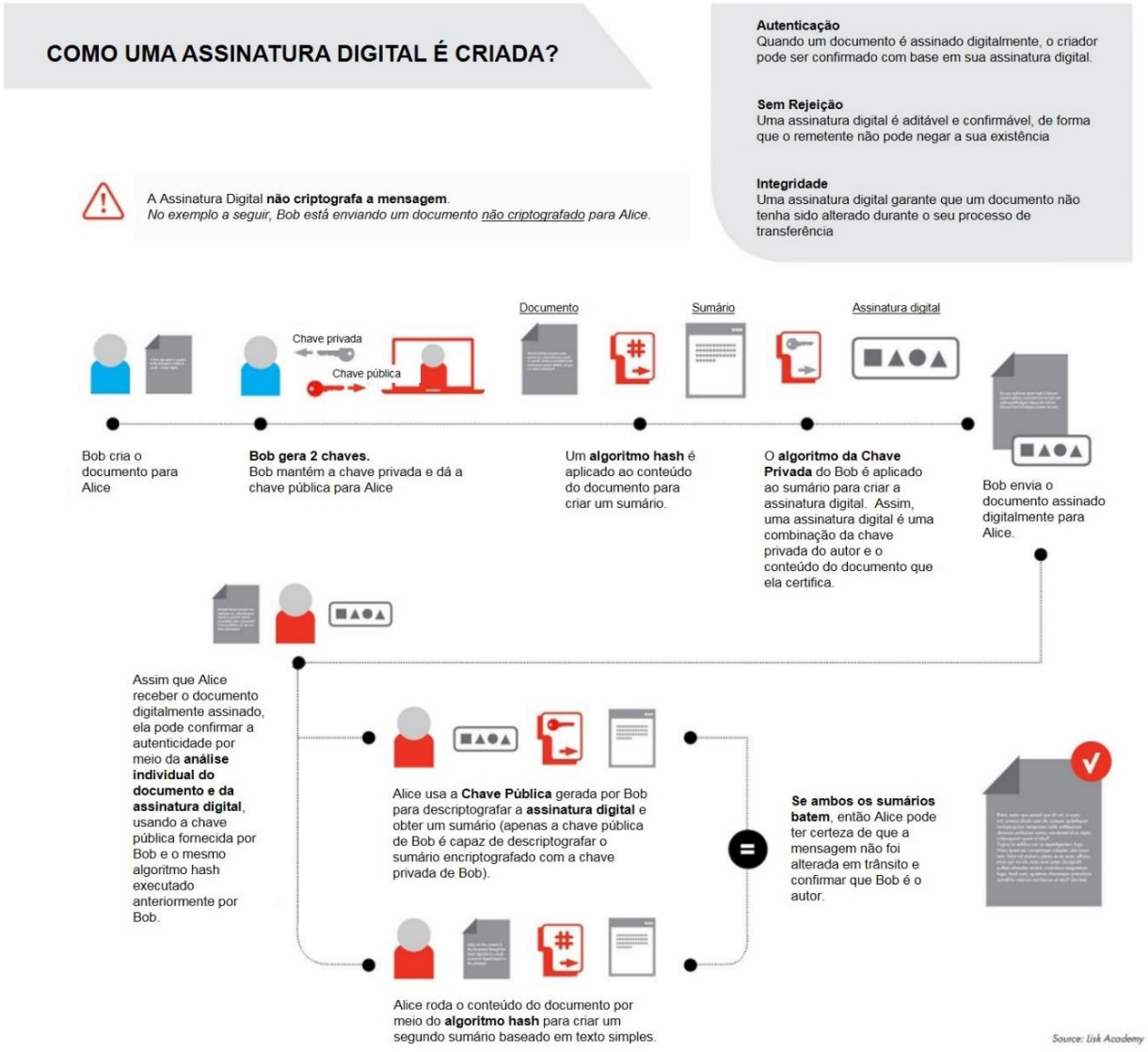
A criptografia de chave pública também pode produzir uma assinatura digital, uma combinação da identidade de um usuário e dos dados que ele/ela desejar proteger.

Assinatura Digital

Assinaturas digitais são a chave para a segurança e integridade dos dados registrados no blockchain. Assinaturas digitais garantem segurança por meio da encriptografia e integridade, assegurando que, caso os dados sejam alterados, a

assinatura também será alterada. Isto é o que garante a imutabilidade no blockchain. Ela também garante autenticidade, pois só podem ser vinculadas a um usuário. Assinaturas digitais são exclusivas de um assinante e baseadas em três algoritmos:

- Chave pública e privada de propriedade do usuário;
- Um algoritmo de assinatura que combina a chave privada e os dados sendo assinados;
- Um algoritmo que confirma e determina se a mensagem é autêntica ou não com base na mensagem ou nos dados, na chave pública e na assinatura.



E se eu perder minha chave privada?

Na criptografia de chave pública, pense na chave pública como sendo o nome de usuário visível a todos e a chave privada como sendo a senha. Se você perder a chave privada não existe a opção de senha. Se você perder sua chave privada, você perde tudo e todos os recursos controlados por essa chave privada. Se alguém roubar a chave privada, esta pessoa terá acesso ao controle de tudo que é controlado por essa chave privada.

É muito importante manter sua chave privada segura e administrada de maneira que não possa ser destruída ou pirateada. Isto é feito por meio de carteiras de hardware ou cópias impressas trancadas em um local seguro.

Multisig (Múltiplas Assinaturas)

Normalmente os blockchains funcionam com uma única assinatura, isto é, um usuário gera uma chave privada para controlar todas as próprias transações.
Mas, a maior parte dos blockchains, incluindo o Bitcoin, permite que múltiplos participantes da rede controlem transações em conjunto. Isto torna o sistema mais seguro e ajuda a se recuperar de um desastre ou perda acidental da chave privada.
Isto se chama sistema de múltiplas assinaturas ou "*multisig*". Nele, um conjunto pré-determinado de participantes concordam em assinar todas as suas assinaturas. Normalmente, é um conjunto de potenciais signatários e assinaturas mínimas necessárias para uma transação válida. É como um conselho de diretores de três fundos de manutenção para uma organização. A menos que pelo menos dois diretores assinem, os fundos não podem ser gastos. Ou uma conta bancária do marido e esposa, em que ambas as assinaturas são necessárias.

Carteira

Uma carteira é uma forma segura de armazenar a chave pública e privada. Por meio da chave privada, a carteira lhe permite realizar transações rotineiras, como enviar e

receber moedas ou verificar o saldo geral. É como um número de conta ao qual todas as atividades dos participantes do blockchain está vinculado.

As carteiras podem ser simples como uma chave privada por escrito em um pedaço de papel ou podem ser dispositivos sofisticados de armazenamento que armazenam chaves privadas e conectam-se à internet quando o usuário quiser realizar uma transação.
Aplicativos de software estão disponíveis para serem instalados em seu computador ou em nuvem, da mesma forma que os aplicativos móveis estão disponíveis, como as carteiras.

Hashing

Hashing é uma tecnologia no centro da manutenção da confiabilidade dos dados em blockchains. É um método que converte qualquer entrada em um resultado criptografado de comprimento fixo. Quaisquer alterações na entrada alteram completamente os resultados. O *hashing* aumenta muitas vezes a segurança e a integridade dos dados. Isto é feito usando as funções *hash* com as seguintes características:

- Impossível produzir o mesmo valor para diferentes entradas;
- A mesma entrada sempre produz o mesmo resultado;
- Rápido para produzir um *hash* para qualquer dada entrada;
- Impossível determinar entrada com base em valor *hash*
- A menor alteração na entrada altera completamente o *hash*

O *hash* proporciona a segurança de que os dados não foram adulterados. Você pode rodar um arquivo recebido por meio de um algoritmo de *hash*, calcular o *hash* daqueles dados e compará-los a aquele mostrado por quem quer que seja que lhe enviou os dados. Se os *hashes* não baterem, você pode ter certeza de que o arquivo foi adulterado antes de você recebê-lo.

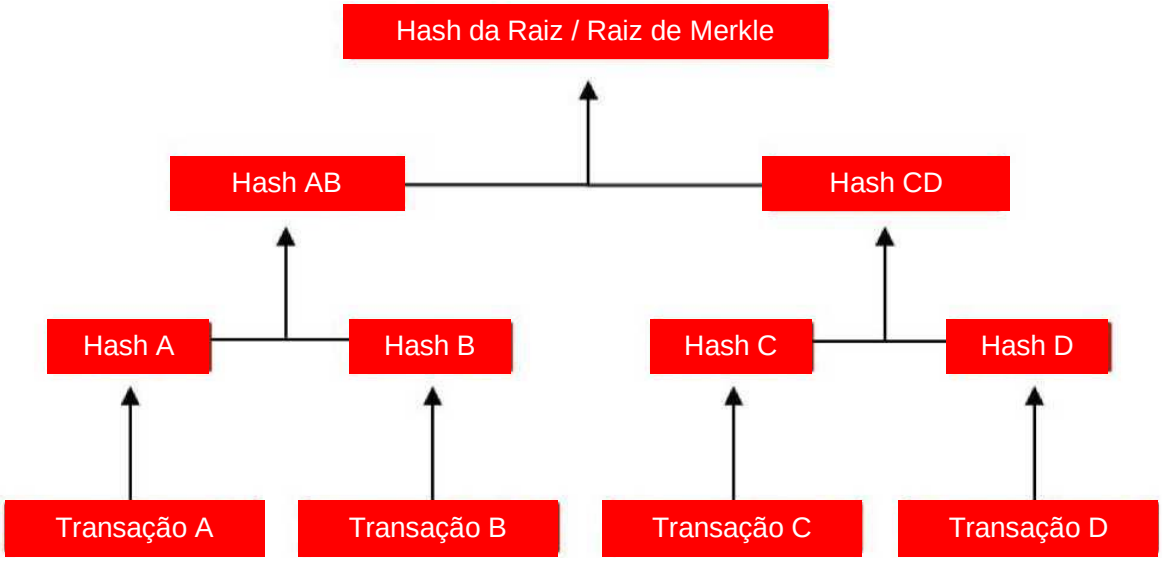
Em blockchain, o *hash* é usado para representar o estado atual do blockchain. Qualquer nova entrada ou transação gera um novo *hash* ou novo estado do mundo, mas inclui o estado anterior. Alterar qualquer registro anterior exigiria que todos os *hashes* fossem alterados, tornando quase impossível alterar ou adulterar quaisquer registros, pois os dados são compartilhados por todos os participantes e as alterações ficarão visíveis para todos e não passarão pela confirmação de consenso.

Estrutura de Dados Blockchain / Árvore de Merkle

A estrutura de dados do blockchain é uma lista vinculada de transações conectadas a uma outra por meio de links *hash*. Na verdade, é uma sequência de blocos (ou *hashes* de blocos) e cada bloco contém muitas transações ou *hashes* de transações.

Blockchains usam a Árvore de Merkle — um método que usa *hashes* de todas as transações, em seguida, o *hash* do conjunto todo de transações ou o próprio bloco até que sobre apenas uma transação. A última transação é chamada de raiz de Merkle. Isto fornece as principais características a seguir:

- Capacidade de confirmar se uma transação está inclusa em um bloco;
- Clientes leves (desde que não tenhamos que fazer o download da cadeia inteira);
- Desempenho em geral e escalabilidade;
- A Confirmação Simplificada de Pagamento (ou SPV) confirma as transações em um bloco sem fazer o download do bloco inteiro.



Na imagem acima, o *hash* da raiz pode fornecer informação para as transações A, B, C e D. Se alguma das transações mudar, ou outra transação for acrescentada, o *hash* da raiz também mudará.

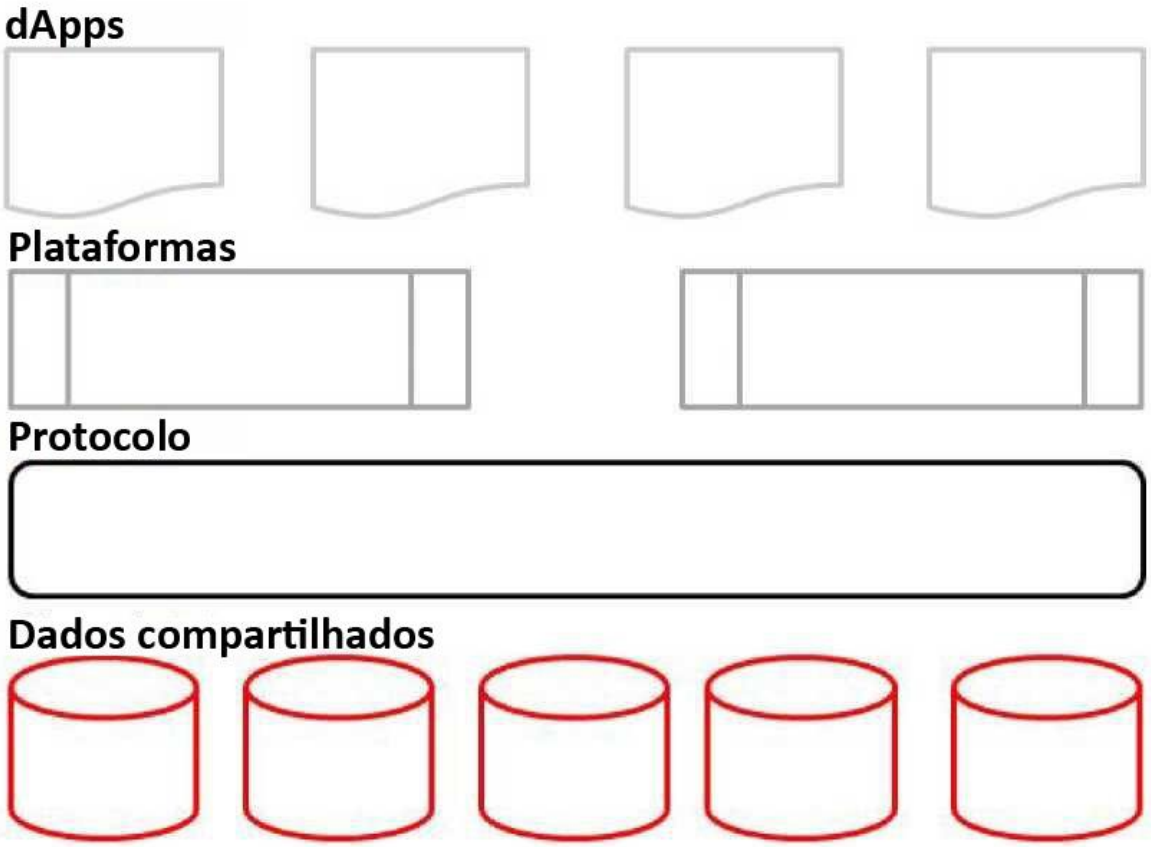
Juntos, a criptografia, as assinaturas digitais e o *hashing* proporcionam imutabilidade, segurança e confiabilidade ao blockchain, ao mesmo tempo em que a Árvore de Merkle acrescenta eficiência, desempenho e escalabilidade.

Pilha de Tecnologias de Blockchain

Como tudo isso funciona junto? Como os diferentes componentes de tecnologia são reunidos para criar um aplicativo utilizável completo?

A pilha de tecnologias de Blockchain pode ser vista como quatro camadas de componentes:

- Dados Compartilhados;
- Protocolo;
- Plataformas;
- Produtos / dApps (Aplicativos Descentralizados) / Contratos Inteligentes;



Dados Compartilhados

Este é um banco de dados descentralizado, que armazena todas as transações em formato *hash*.

Para obter maiores detalhes, consulte a seção “Tecnologias de Livro-razão Distribuídas”.

Protocolos

Seguem exemplos de infraestrutura de protocolos existentes na web atualmente, TCP/IP, SMTP, HTTP e HTTPS. Os protocolos são basicamente a infraestrutura à qual todos que participam do ecossistema de blockchain devem aderir. Os protocolos de Blockchain implementam regras de consenso, validação, incentivo e participação. Bitcoin e Ethereum são exemplos de protocolos. Bitcoin, como o primeiro e maior exemplo, possui protocolos em vigor para impedir um ataque de "gasto duplo",

permitir pagamentos *peer-to-peer* e garantir uma camada de liquidação forte e confirmada. Outros tipos de protocolos incorporam outros aspectos que permitem mais recursos e tratam de conjuntos de problemas diferentes.

Plataformas

As plataformas são uma espécie de software intermediário. Eles permitem que os desenvolvedores construam aplicativos em cima de protocolos. As plataformas de Blockchain (Blockchain 2.0) aproveitam os conceitos introduzidos pelo protocolo de blockchain do Bitcoin e tentam expandi-lo para torná-lo universal e “Turing completo”. As plataformas procuram atuar como um “computador universal” que permitem o desenvolvimento de aplicativos em cima de sua camada de protocolo. Exemplos de plataformas de blockchain conhecidas incluem Ethereum, NEO e EOS. Cada uma utiliza a tecnologia pioneira do Bitcoin e visa expandir sobre o protocolo por meio da incorporação de “contratos inteligentes”. Este novo avanço no protocolo de blockchain permite o uso de funções universais a serem construídas na infraestrutura de blockchain.

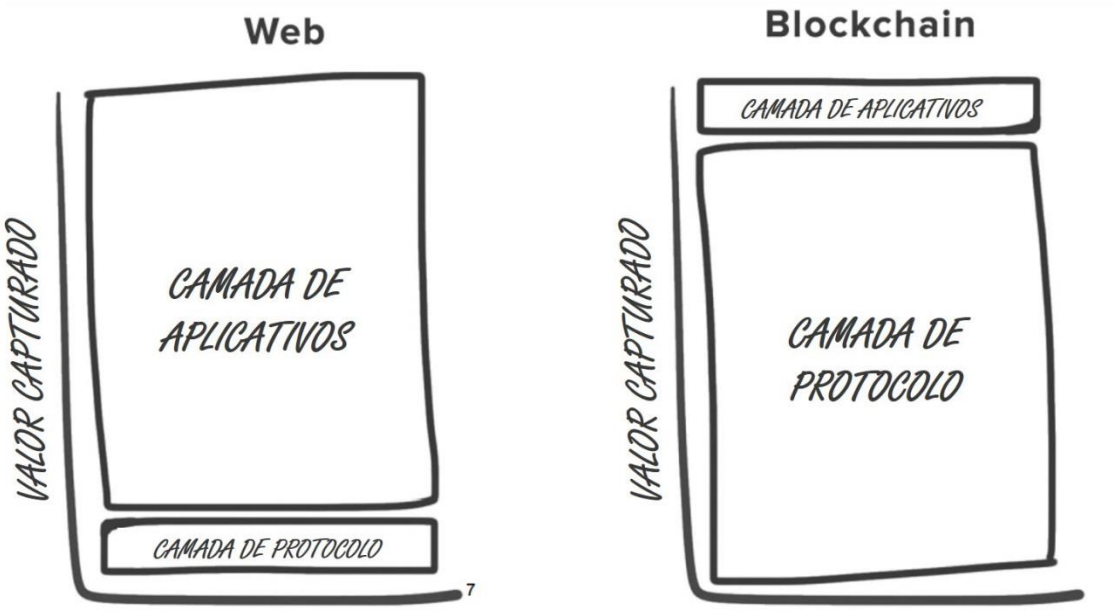
Produtos

Produtos são interfaces para protocolos e plataformas. Eles permitem aos usuários interagir com o protocolo e os dados compartilhados. Desenvolvedores utilizam plataformas para construir produtos. Exemplos de produtos são os *dApps* (Aplicativos Descentralizados). Esses "*dApps*" utilizam tecnologia blockchain juntamente com recursos como "contratos inteligentes" para fornecer não apenas a segurança do blockchain, mas, também, a capacidade de autoexecutar as operações. "*dApps*" são a fina camada de aplicativo construída sobre uma camada de protocolo blockchain e possibilitam aplicativos descentralizados*, peer-to-peer* e não confiáveis.

Protocolos robustos

Seguem exemplos de infraestrutura de protocolos existentes na web atualmente: TCP/IP, SMTP, HTTP e HTTPS. Eles existem como blocos de construção

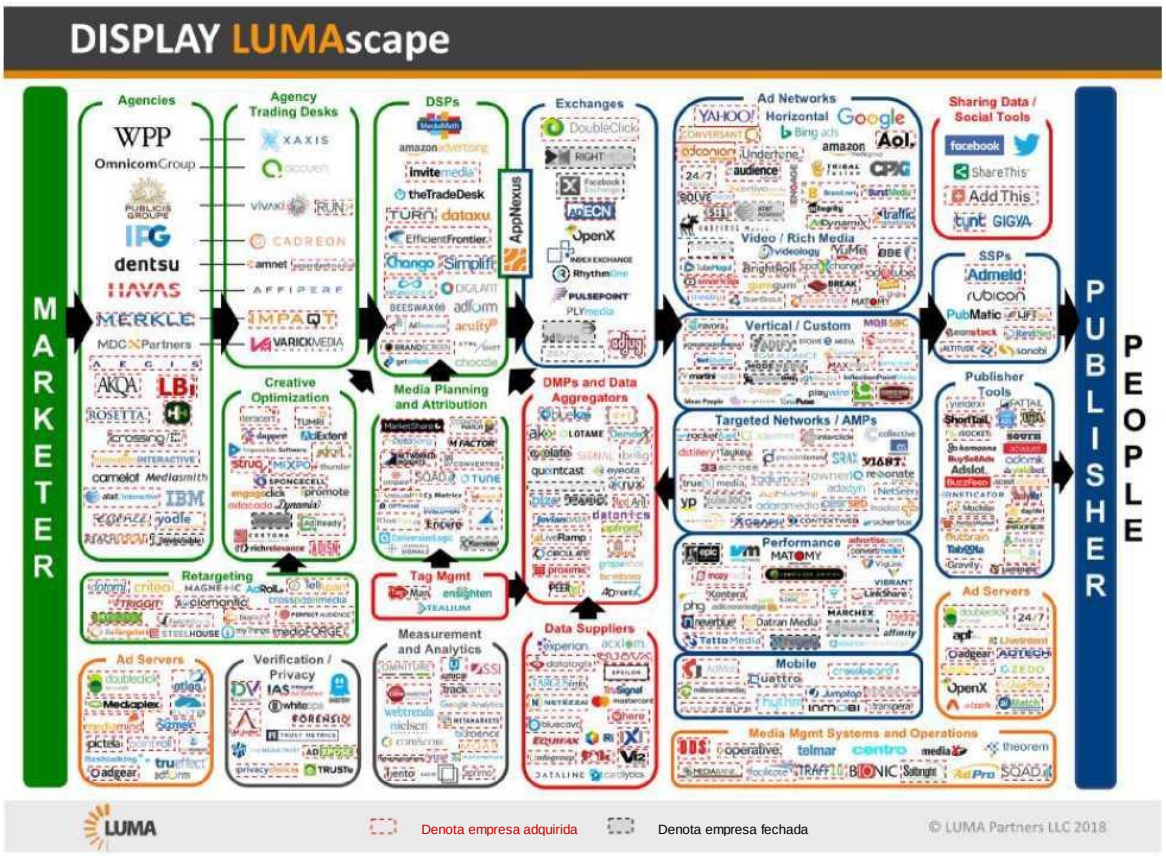
fundamentais da internet hoje em dia, mas tendo dito isto, eles são camadas de protocolo relativamente “finas”. Embora forneçam orientação e estrutura para a utilização da internet, eles não são robustos o suficiente para lidar com a maioria das ações que o ambiente online atual exige. Como resultado desta camada "fina", uma camada “grossa” de aplicativo foi construída para criar ecossistemas e infraestrutura viáveis aos quais todos os participantes aderem. A maior parte do valor, portanto, é capturado nesta camada "grossa” de aplicativos, enquanto os aplicativos podem coletar e utilizar os dados como bem entenderem.



Os blockchains invertem essa distribuição entre a camada de aplicativo e a camada de protocolo. Os blockchains permitem a criação de camadas de protocolo "robusto" com funções muito específicas e diretrizes em vigor. Este novo protocolo pode lidar com governança, comunicação e liquidações, anteriormente reservados para a camada de aplicativo. Por outro lado, ao construir protocolos robustos, os aplicativos podem ser muito “finos” e se beneficiarem de uma rede sem confiança e descentralizada, sem depender de entidades centralizadas.

Casos de Uso de Publicidade

A cadeia de publicidade digital envolve múltiplas partes, como anunciante, agência, trading desk, DSP, DMP, exchange, SSP, ad network, provedor de medição e veículo em apenas uma transação. A LUMAScape[7] abaixo mostra essa complexidade.

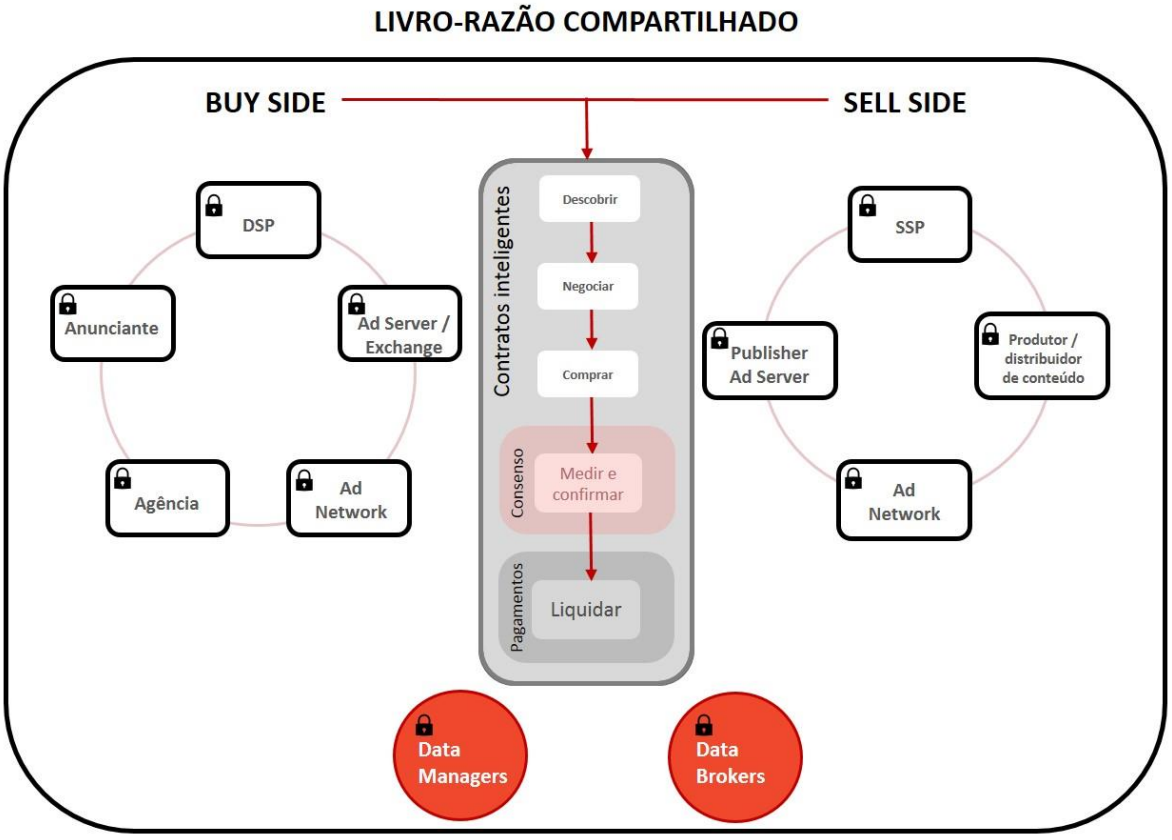


Descobrir, combinar, negociar, medir e fazer liquidações exige compartilhamento de dados entre diversos parceiros em uma transação. Dadas as principais características da tecnologia de blockchain:

- Banco de dados compartilhado;
- Governança de protocolo;

[7] https://www.lumapartners.com/luma-institute/lumascapes/display-ad-tech-lumascape/

- Contratos Inteligentes;
- Imutabilidade;
- Criptografia e assinaturas digitais.



Pode ser uma tecnologia facilitadora para ajudar a aplicar as regras e acordos necessários para concluir a transação, bem como inaugurar uma nova era de redefinição da moeda de transação para publicidade digital.

A tecnologia blockchain está nos estágios iniciais de evolução e várias indústrias estão em desenvolvimento inicial e em ciclos de adoção. Existem algumas áreas onde é preciso mais trabalho, por exemplo, a rapidez da transação é limitada no blockchain, embora esteja sendo feito um trabalho para superar esses desafios com conceitos

avançados, como processamento fora da cadeia ou de cadeia lateral.

Algumas áreas imediatas onde o Grupo de Trabalho de Blockchain do Laboratório de Tecnologia do IAB prevê a aplicação de tecnologia blockchain são:

Prevenção de Fraude

Forte autenticação à base de criptografia e imutabilidade de dados pode garantir a confirmação das empresas participantes em uma rede ou transações e os registros públicos baseados em consenso podem ser mantidos por vendedores e compradores.

Identidade, Dados e Privacidade

Dadas as novas regulamentações sobre privacidade e a necessidade de compartilhamento de identidade e de dados do consumidor entre várias partes, o livro-razão compartilhado com permissões criptográficas pode permitir soluções elegantes para reproduzir o consentimento do consumidor e a identidade segura, bem como as PII (Informações Pessoais Identificáveis).

Medição

Com diversas partes envolvidas em uma típica impressão de anúncio, é preciso validação e acordo entre todas as partes de negócios, e pode ser um processo que exige muito tempo, ineficiente e ineficaz. Bancos de dados compartilhados e contratos inteligentes, juntamente com consenso imposto por protocolo, podem fornecer acordos muito mais eficientes de medição de impressão de anúncio entre parceiros de negócios.

Transparência

O uso inteligente de criptografia, dados compartilhados e consenso podem ajudar a construir um sistema transparente para negociação e congruência das empresas participantes em uma transação.

Liquidação

A primeira rede blockchain, Bitcoin, foi desenvolvida para pagamentos, de forma que o blockchain possa realmente ajudar fornecendo um sistema de pagamento que efetue pagamentos para todos os parceiros envolvidos em uma transação com precisão, rigor e rapidez.

Apêndice 1: Uma breve história do Blockchain

Satoshi Nakamoto é majoritariamente reconhecido como um dos fundadores do bitcoin e, portanto, do blockchain. No entanto, muitos especialistas, como Jim Robinson, afirmam que a história do blockchain é anterior ao Documento Informativo de Nakamoto de 2008, que primeiramente pesquisou os detalhes do protocolo bitcoin.

As origens da criptomoeda

A tecnologia da internet conecta as pessoas entre si diretamente, o que abre uma vasta gama de possibilidades. Ao dissolver as fronteiras físicas e políticas pré-existentes, o planeta inteiro ganhou acesso às mesmas informações pela primeira vez na história. Este nível de acesso é garantido pelo design descentralizado da internet. Na ausência de hub centralizado, não há um único ponto de falha ou controle.

Moedas digitais

Satoshi Nakamoto escreveu o Documento Informativo, em 2008, *Bitcoin: Um Sistema de Caixa Eletrônico Peer-to-Peer.*

Primeira ideia-chave: os mecanismos de caixa eletrônico *peer-to-peer* não precisam de banco intermediário para transferir pagamentos entre os pares. O bitcoin baseia-se em décadas de pesquisa criptográfica, incluindo a realizada na Árvore de Merkle, funções *hash*, criptografia de chave pública e assinaturas digitais.

David Chaum: Assinaturas às cegas e *Ecash* (1982)

As propostas iniciais para criar caixa digital remontam ao inícios dos anos 1980. Em 1982, David Chaum propôs um plano que usava assinaturas às cegas para desenvolver moeda digital irrastreável. Neste plano, um banco emitiria dinheiro digital assinando um número de série às cegas e aleatoriamente apresentado ao banco pelo usuário. O usuário poderia então usar o *token* digital assinado pelo banco como moeda. A limitação a este plano era que o banco tinha que manter o controle de todos os números de série usados para esta finalidade. Este era um sistema de design centralizado e requeria a confiança dos usuários.

Adam Back: *Hashcash* (1997)

O *hashcash*, introduzido em 1997, foi originalmente proposto para impedir e-mails não desejados, não solicitados ou spam. A ideia por trás do *hashcash* era resolver um quebra-cabeças computacional fácil de verificar, mas comparativamente difícil de calcular.

Wei Dai: B-Money (1998)

O conceito e a ideia de usar Prova de Trabalho para criar dinheiro. Uma grande fraqueza no sistema B-Money era que um adversário com maior poder computacional poderia gerar dinheiro não solicitado sem permitir à rede ajustar-se para um nível de dificuldade adequado. Este sistema carecia de detalhes sobre o mecanismo de consenso entre nós (nodes) e algumas questões de segurança, tais como ataques Sybil, também não foram abordados.

Nick Szabo: Bitgold (1998)

Apesar de basear-se no mecanismo de Prova de Trabalho, o Bitgold tinha os mesmos problemas do b-money (com a exceção que o nível de dificuldade da rede era ajustável). Em 1999, Tomas Sander e Ammon TaShama introduziram um plano de *Ecash* que, pela primeira vez, usava Árvores de Merkle para representar moedas e *zero-knowledge proofs* (provas de conhecimento zero) para provar a posse de moedas. No plano *Ecash*, um banco central era necessário para manter um registro de todos os números de série usados. Este plano permitia aos usuários serem totalmente anônimos, embora a um custo computacional.

Hal Finney: RPoW (2004)

A RPoW (Prova de Trabalho Reutilizável) foi introduzida por Hal Finney em 2004 e usou o plano hashcash de Adam Back como uma prova dos recursos computacionais gastos para gerar o dinheiro. Este era também um sistema central que mantivesse uma base de dados central para se manter a par de toda a prova usada do símbolo do trabalho. Além disso, este era um sistema online que utilizava certificação remota,

viabilizado por uma plataforma de computação confiável (também conhecida como Trusted Platform Module ou TPM, hardware).

Bitcoin (2008)

Satoshi Nakamoto aproveitou a atual tecnologia da rede para implementar um sistema de P2P para fazer a troca virtual de dinheiro. Todos os pares na rede operam-se como os atores iguais que participam através do mesmo protocolo. A política monetária de Bitcoin é definida e autorregulada por sua rede aberta dos computadores. Assim, através do bitcoin, o mundo testemunhou o aparecimento de uma nova etapa de dinheiro.

Apêndice 2: Glossário

Contrato Inteligente: código de computador que, mediante a ocorrência de circunstância ou circunstâncias especificadas, é capaz de funcionar automaticamente de acordo com funções pré-determinadas. O código pode ser armazenado e processado em um livro-razão distribuído e registraria toda a mudança resultante no livro-razão distribuído.

Contrato Inteligente legal: um contrato inteligente que articule e seja capaz de autoexecutar, em bases legalmente exequíveis, os termos de um acordo entre duas ou mais partes.

Livro-razão distribuído: software de computador que emprega uma arquitetura de bancos de dados compartilhados para manter cópias múltiplas, idênticas de um registro digital distribuído e atualizadas das transações ou dados. Os livros-razão distribuídos mantêm a segurança e a precisão das transações, implantando chaves criptográficas e assinaturas para controlar o acesso e as permissões no livro-razão compartilhado. Normalmente, as regras de controle de acesso são acordadas e aplicadas pela rede (Crown, 2016:5).

Blocos: em Blockchain, as transações são agrupadas em blocos, onde cada bloco é vinculado pela referência cruzada de um *hash* criptográfico do bloco anterior no cabeçalho, fornecendo, assim, rastreabilidade de volta ao primeiro bloco ou bloco de gênese. A articulação criptográfica entre blocos resulta na propriedade da "inviolabilidade" (ou apenas anexar) do livro-razão, porque, se um ator mal-intencionado tentar adicionar, remover, ou mudar uma transação em qualquer um dos blocos, ele afetará todos os blocos a seguir. Em um blockchain bitcoin, o bloco normalmente contém 500 transações e as árvores de Merkle são usadas para juntá-las e melhorar a eficiência.

Blockchain: um blockchain é um tipo especial de livro-razão distribuído que sustenta o bitcoin ou qualquer outra camada do protocolo (Ethereum, Eos, etc.). Uma característica chave do blockchain é que ele emprega uma estrutura de dados na qual as transações são organizadas e juntadas em um bloco. Cada bloco é ligado ou associado ("encadeado") a um bloco anterior usando uma função *hash* criptográfica (Crown, 2016:17).

Consenso: Blockchains são descentralizados ou baseados em uma rede P2P, o fato de que não há nenhuma autoridade central significa que alcançar o consenso no estado do livro-razão (a ordem e a singularidade das transações) é uma matéria crucial.

Funções hash: técnica onde os conjuntos de dados de comprimentos e tamanhos variados são convertidos em comprimentos fixos. Isto é necessário para fins de verificação para comparar diferentes entradas de dados. As funções *hash* criptográficas são úteis ao determinar se dois objetos são iguais.

Árvores de Merkle: estruturas de dados especiais que garantem a integridade do livro-razão. Este *hash* final no topo é a raiz de Merkle e fornece a prova de validade para todas as transações acrescentadas à árvore.

Mineração: a mineração pode ser definida como sendo o processo no qual um nó (node) encontra um bloco válido para resolver um quebra-cabeças computacional chamado de prova de trabalho. Muitas vezes, a prova de trabalho é mal-entendida, como sendo prova de que algo funciona; em vez disso, ela indica a prova de que o minerador fez o trabalho no blockchain.

Blockchain público: um blockchain que permite que qualquer um com capacidade adequada para cálculo envie mensagens para processamento, seja envolvido no processo de alcance de consenso ou participe de outra maneira na rede. O blockchain

de bitcoin é um exemplo de um blockchain público.

Blockchain privado: um blockchain cujos participantes são previamente selecionados ou sujeitos à entrada faseada, com base na satisfação de determinados requisitos ou na aprovação de um administrador.

Ativo baseado no blockchain: um ativo que consiste unicamente em um token em um blockchain.

Ativo transformado em token: ativo que consiste de bens tangíveis ou intangíveis além de um blockchain, tal como bens móveis ou bens imóveis ou um interesse legal em algum ativo, mas que é representado por um token em um blockchain.

Moeda Virtual: um meio de troca e que opera como uma moeda em alguns ambientes, mas que não tem todos os atributos do papel-moeda, em especial, que não tem o status de moeda corrente em nenhuma jurisdição.

Carteira de moeda virtual: um meio (aplicativo de software ou o outro mecanismo/meio) de deter, armazenar e transferir uma moeda virtual.

Assinatura de chave pública/privada: um método de assegurar a integridade de dados e a autenticidade da origem, que usa a chave privada de uma parte (para assinar) e sua chave pública correspondente (para verificar a validade de sua assinatura).