TUDO SOBRE A TECNOLOGIA BLOCKCHAIN

O GUIA MAIS COMPLETO PARA INICIANTES SOBRE CARTEIRA BLOCKCHAIN, MINERAÇÃO, BITCOIN, ETHEREUM, LITECOIN, ZCASH, MONERO, RIPPLE, DASH, IOTA E CONTRATOS INTELIGENTES

ALAN T. NORMAN

TEKTIME

Alan T. Norman
Tudo Sobre A Tecnologia Blockchain

http://www.litres.ru/pages/biblio_book/?art=57158556
Tudo Sobre A Tecnologia Blockchain:
ISBN 9788835406983

Аннотация

Ao invés de falar sobre investimento, este livro irá focar em como a tecnologia blockchain funciona, e como ela pode ser usada no futuro. Ao invés de falar sobre investimento, este livro irá focar em como a tecnologia blockchain funciona, e como ela pode ser usada no futuro. Tópicos que você pode esperar ver neste livro incluem: • Que problema a blockchain resolve? • Como a tecnologia pode deixar nossas instituições mais rápidas e menor caras? • Poderia a tecnologia substituir nossas instituições (como governos, bancos, etc) completamente? • Como a blockchain constrói confiança entre estranhos? • Como a blockchain aumenta a segurança de transações e contratos? • A blockchain pode ser usada fora do setor financeiro? • O que é um bloco? • O que é a cadeia e por que precisamos delas? • Qual é a explicação técnica do que acontece na blockchain? • O que é mineração e por que precisamos dela? • Existem alternativas à mineração para criar uma blockchain? • Qual é a história do Bitcoin? • O Bitcoin tem problemas? • O que é Ethereum, e o que é um contrato

inteligente? • Existem outras tecnologias blockchain que eu deveria conhecer? • Como as empresas estão adotando a blockchain? • Que problemas regulatórios poderiam atrasar a adoção da blockchain? Ufa, essas são muitas questões. Se você está preparado para enfrentá-las, eu também estou.

Содержание

Alan T. Norman
Tudo Sobre A Tecnologia Blockchain

Tudo Sobre A Tecnologia Blockchain

O Guia Mais Completo Para Iniciantes Sobre Carteira Blockchain, Mineração, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA e Contratos Inteligentes

Alan T. Norman

Tradutor: Tarcísio Ladeia de Oliveira

Obtenha Grátis Seu Livro Sobre Baleias do Bitcoin

(Presente no fim do livro)

VOCÊ GOSTOU DO LIVRO?

Se você nunca ouviu falar de blockchain ou se você tem apenas uma vaga ideia de como essa tecnologia funciona, este livro é para você. Neste curto guia eu vou te conduzir pelo essencial do funcionamento da tecnologia blockchain, usando explicações simples e dando exemplos pelo caminho. Eu introduzi muitas pessoas à blockchain, então eu sei onde iniciantes tendem a ficar confusos e quais as principais dúvidas que eles têm. Todos os princípios básicos são abordados passo a passo neste livro. Você não precisa de qualquer conhecimento especial ou tecnológico para entender os conceitos presentes neste livro. A blockchain é uma tecnologia, como a internet e o computador pessoal, que foi feita para ser usada pelas massas. Ela tem o potencial de revolucionar quase qualquer interação em nossas vidas. Vários leitores devem ter ouvido falar de Bitcoin e criptomoedas. Essas são aplicações importante da tecnologia blockchain, e a primeiras aplicações. Porém, a blockchain não está restrita ao uso em sistemas financeiros e de pagamento. Embora abordaremos Bitcoin e outras criptomoedas neste livro, também falaremos sobre potenciais aplicações da blockchain em diversas outras indústrias.

Este Não É Um Livro Sobre Investimento Em Bitcoin Ou Outras Criptomoedas

Nos últimos anos, centenas de novas moedas foram criadas, todas elas exclusivamente digitais, baseadas na blockchain. Para novatos à tecnologia, pode parecer surpreendente que pessoas estejam realmente investindo em moedas digitais recém-criadas como o Bitcoin. Embora essas moedas sejam interessantes e tenham o potencial para serem usadas em larga escala, este não é um livro sobre criptomoedas. Se você estiver procurando ajuda para investir ou informações privilegiadas sobre quais moedas serão as mais bem-sucedidas, você precisa de outro livro meu – "**A Bíblia do Investimento em Criptomoeda**".

Para vocês que ainda estão conhecendo a blockchain, a ideia de investir em criptomoedas pode parecer atraente. Um aviso: investir em uma criptomoeda é entrar em um mercado altamente volátil e extremamente arriscado. Pesquise bem antes de investir em uma criptomoeda para ter certeza que ela é legítima, e não invista mais dinheiro do você está disposto a perder. Blockchain e criptomoedas ainda estão em seus primeiros dias, e qualquer coisa pode acontecer a qualquer momento.

O Que Você Vai Aprender Neste Livro

Ao invés de falar sobre investimento, este livro irá focar em como a tecnologia blockchain funciona, e como ela pode ser usada no futuro. Tópicos que você pode esperar ver neste livro incluem:

- Que problema a blockchain resolve?
- Como a tecnologia pode deixar nossas instituições mais rápidas e menos caras?
- Poderia essa tecnologia substituir nossas instituições (como governos, bancos, etc) completamente?
- Como a blockchain constrói confiança entre desconhecidos?
- Como a blockchain aumenta a segurança de transações e contratos?
- A blockchain pode ser usada fora do setor financeiro?
- O que é um bloco?
- O que é a cadeia e por que precisamos delas?
- Qual é a explicação técnica do que acontece na blockchain?
- O que é mineração e por que precisamos dela?
- Existem alternativas à mineração para criar uma blockchain?
- Qual é a história do Bitcoin?
- O Bitcoin tem problemas?
- O que é Ethereum, e o que é um contrato inteligente?
- Existem outras tecnologias blockchain que eu deveria

conhecer?

- Como as empresas estão adotando a blockchain?
- Que problemas regulatórios poderiam atrasar a adoção da blockchain?

Ufa, essas são muitas questões. Se você está preparado para enfrentá-las, eu também estou. Vamos começar.

O Que A Blockchain Faz?

Antes de entrarmos nos detalhes técnicos da tecnologia blockchain, é importante entender os problemas que a blockchain resolve. Por que precisamos da blockchain blockchain, e o que ela faz que a nossa tecnologia atual não consegue fazer? Os primeiros usuários de Bitcoin e perceberam o que eles consideravam um defeito fundamental na forma como pensamos em transações, confiança e instituições sociais. As formas mais antigas de blockchain surgiram mais ou menos ao mesmo tempo que a crise financeira de 2007 nos Estados Unidos, quando várias pessoas perderam fé em instituições sociais que deveriam proteger os interesses do cidadão comum. É claro, as pessoas se desiludiram com o sistema bancário com o surgimento da crise, mas também perderam fé na capacidade do governo de regular mercados financeiros e de imprensa de investigar potenciais crises. Inclusive, tanto pesquisas da Gallup quanto o Barômetro de Confiância da Edelman (Edelman Trust Barometer) mostram uma constante diminuição da confiança da população nas instituições, governos, mídia, academia e instituições sem fins lucrativos na última década. Confiança em instituições está em seu ponto mais baixo da história americana, e problemas similares atingem a UE (Brexit, ascenção de Marine Le Pen, independência Catalã, crise do governo grego). A ideia fundamental por trás de instituições é criar confiança entre

estrangeiros em uma sociedade. Nós temos leis e sistemas que tornam possível que milhões de pessoas que não se conhecem possam viver uma do lado da outra. Porém, os criadores da blockchain sentiram que essas instituições estavam falhando.

O Problema Com Instituições

Para ver porque os criadores da blockchain querem substituir as instituições, é muito útil pensar sobre porque chegamos ao ponto em que a confiança nelas está tão baixa. Que fraquezas elas têm, e como a blockchain poderia resolvê-las?

Lentas

A primeira e principal fraqueza é a velocidade. Instituições, por suas próprias naturezas, são lentas. Elas precisam de aprovações e várias rodadas de verificação para cada relação, contrato, transação. Mudanças de políticas a nível institucional são lentas. Podem levar meses ou anos para aprovar novas leis ou implementar novos procedimentos. Por exemplo, fazer seu imposto de renda leva horas de trabalho e dor de cabeça. Após isso, o governo precisa verificar as informações que você enviou antes de preparar sua restituição. Meses ou até anos depois, o governo pode escolher te auditar, caso em que você vai precisar de cópias de transações financeiras de anos atrás.

Outro exemplo é a demora de transações bancárias. Não existe motivo, tecnologicamente falando, para uma transferência bancária demorar mais do que alguns minutos. Porém, normalmente demoram alguns dias úteis para a transação ser feita devido à combinação de sistemas ultrapassados,

procedimentos internos e regulação governamental que requerem que a transição seja analisada e processada. A tecnologia blockchain é governada por seus usuários e utiliza criptografia para manter a privacidade do usuário. Dependendo de como o sistema é projetado, ele pode ser incrivelmente rápido. Os novos contratos inteligentes podem automaticamente calcular e desembolsar algo como uma declaração de imposto ou um holerite assim que certas condições sejam atendidas. Como são baseados em consenso, a comunidade pode coletivamente decidir implementar uma mudança no funcionamento do sistema, resolvendo problemas ao aparecerem.

Custosas

Instituições tradicionais também são caras. É fácil apontar os impostos como sendo um dos gastos das instituições, mas todas as taxas de transação e assinatura que você paga todo mês são outras formas de gastos institucionais. Por exemplo, bancos cobram taxas para processar transferências bancárias, converter moedas e até para gerenciar a sua conta. Agências de seguro cobram taxas administrativas que são embutidas nos prêmios do seguro. Várias lojas online cobram taxas do uso de cartão de crédito. Se você tem uma pequena empresa, você vai encontrar taxas em tudo, de marketing a processamento de pagamentos. Nós ficamos muito acostumados a essas pequenas taxas serem o preço de viver em sociedade, mas a blockchain

espera desafiar crença. Contratos e transações da blockchain ocorrem em uma rede compartilhada. Os usuários na rede também contribuem para verificar as transações dos outros. Ao invés de uma autoridade central cobrar uma taxa para verificar sua transação, você verifica a transação na rede em troca do processamento da sua própria transação. Nem todas as tecnologias blockchain funcionam exatamente assim, mas a ideia é a mesma para a maioria. Participando da rede, você acaba com menos taxas do que você pagaria para uma instituição tradicional.

Sujeitas a Ataques

O cibercrime está em alta, e agora é comum ouvir sobre grandes instituições sendo hackeadas ou tendo vazamento de dados pessoais. Vulnerabilidade a ataques é uma razões da diminuição da confiança em instituições. Quando você centraliza dados, você está propenso a encontrar pessoas de má índole que buscam capitalizar com essas informações.

O hackeamento da Equifax de 2017 nos Estados Unidos é um dos principais exemplos. A Equifax coleta informação de crédito dos consumidores dos Estados Unidos, incluindo números de cartão de crédito, informação de seguridade social, nomes completos, endereços e históricos de pagamento. O vazamento de dados em setembro de 2017 afetou 143 milhões de consumidores, ressaltando os perigos de confiar

segurança de dados a uma instituição de grande porte. As tecnologias blockchain usam múltiplas camadas de criptografia para proteger as informações dos usuários. Algumas tecnologias blockchain são mais seguras que outras, e cada tecnologia tem seu próprio método de assegurar a privacidade. Porém, como cada relação, contrato e transação é criptografada individualmente, mesmo se você conseguisse vazar um pedaço de informação pessoal, você não conseguiria acesso às informações de mais ninguém no processo.

Substituindo Instituições por Tecnologia

A maioria das pessoas concorda que nossas instituições tem falhas e não são soluções perfeitas. Mas elas com certeza resolvem problemas de confiança, e o fazem a centenas de anos. Inclusive, estamos provavelmente vivendo a era mais pacífica e mais confortável da história humana. A ideia por trás da blockchain é substituir instituições por tecnologias que possam fazer melhor esse trabalho e empoderar indivíduos. Se você pudesse criar uma forma para que desconhecidos confiassem uns nos outros sem precisar de um banco ou governo como intermediário, você enfrentaria um dos maiores gargalos da sociedade. Mas para fazer isso, você precisaria de um sistema poderoso para criar consenso entre desconhecidos, e os criadores da blockchain acreditam que o poder se encontra na descentralização. Basicamente todas as aplicações da blockchain (e outras tecnologias criptográficas) são baseadas no conceito de descentralização. Ao invés de uma autoridade rígida, lenta e centralizada fazendo as decisões e governando relações, a blockchain busca retornar o poder de regulação aos indivíduos. Ao invés de confiar em uma instituição de grande porte, a blockchain cria confiança através do consenso.

Um Novo Paradigma Tecnológico

A fundação de todas as tecnologias blockchain e criptográficas é a rede ponto-a-ponto (ou *peer-to-peer*, P2P). Tradicionalmente, quando pensamos em confiança, pensamos em instituições como intermediárias. Neste momento, se eu quisesse te enviar $100, precisaríamos usar um banco para transferir:

1. Primeiro, eu submeteria a transação ao banco;
2. Em seguida, meu banco pegaria uma taxa percentual para processar a transação;
3. Meu banco verificaria que eu tenho $100 na minha conta;
4. Meu banco perguntaria para o seu banco se sua conta é válida e está aberta para depósitos;
5. Meu banco atualizaria seu livro-razão de contas para subtrair $100 da minha conta; e
6. Seu banco atualizaria seu livro-razão para adicionar $100 a sua conta.

Uma rede ponto-a-ponto não precisa de um intermediário. Ao invés disso, ela usa um livro-razão (*ledger*) distribuído para processar suas transações. Todo computador que faça parte da rede mantém uma cópia do livro-razão, e transações são adicionadas ao livro-razão sistematicamente. É incrivelmente difícil mudar o livro-razão após ele ser escrito, pois isso

requereria modificar a cópia do livro-razão em milhares de computadores ao longo da rede ponto-a-ponto. Aqui está como funcionaria a mesma transferência de $100 em uma rede ponto-a-ponto com livro-razão distribuído:

1. Primeiro, eu submeto a requisição de transferência à rede;
2. Em seguida, os computadores mais próximos à rede verificam que eu tenho dinheiro o suficiente em minha conta e que a sua conta de recebimento é válida;
3. Assim que eles verificam a transação, eles difundem a transação a todos os computadores próximos a eles na rede; e
4. Por sua vez, esses computadores verificam novamente a transação e a passam adiante, levando a um efeito cascata até que a transação seja adicionada a todos os livros-razão da rede.

Como os computadores em uma rede ponto-a-ponto são tanto usuários como verificadores, transações blockchain têm o potencial para serem gratuitas. O efeito cascata de verificar transações significa que uma transação pode ser processada em minutos ou horas, ao invés de dias.

Baseado nesses benefícios por si só, a blockchain é frequentemente vista como o fim da instituições. Imagine fazer transações rápidas e sem gasto para qualquer pessoa no mundo. Não é difícil ver as vantagens potenciais, mas a blockchain apresenta oportunidades para mudanças sociais ainda maiores.

Construir Confiança

A natureza ponto-a-ponto da blockchain constrói confiança sem instituições. Como todo mundo que usa a rede tem uma cópia do livro-razão, a blockchain promete uma nova era de transparência em contabilidade. Eu posso facilmente ver se você me enviou $100 e a transação foi verificada. Assim que você faz, eu sei que você não vai poder rescindir a transação ou cancelar a cobrança, porque ela foi verificada pela rede. Novos avanços na blockchain também significam que eu posso criar um contrato entre nós que só será pago assim que certas condições sejam atingidas, permitindo que façamos negócios sabendo que o contrato está financiado e será pago somente se o trabalho for completo.

Aumentar A Conexão

Um dos maiores benefícios potenciais da tecnologia blockchain é o aumento da conexão global. Quando você pode facilmente enviar dinheiro para qualquer um no mundo, fronteiras nacionais e regionais começam a desaparecer. Fica mais fácil confiar em desconhecidos, onde quer que você esteja no mundo. Da mesma forma que a internet conectou o mundo, a blockchain agora promete criar confiança entre pessoas no

mundo. Mas redes ponto-a-ponto protegidas por blockchain não servem somente para transações financeiras. A blockchain pode ser usada para criar contratos entre desconhecidos, permitir que cidadãos votem anonimamente e acabar com fraudes eleitorais e conectar dispositivos inteligentes que mantêm os cidadãos seguros. É até possível que a blockchain seja usada para referendos públicos diária ou semanalmente para novas leis, em que você poderia votar do seu computador pessoal. Uma verdadeira democracia popular mudaria permanentemente a forma como o governo funciona, dando o controle de leis e políticas à população.

Aumentar A Produtividade

Um benefício secundário da blockchain é o aumento da produtividade. Atualmente, as instituições são um atraso para a economia, pois governos cobram impostos para manter a burocracia e bancos cobram taxas para transferir e manter dinheiro. Uma economia e sociedade baseadas na blockchain tem o potencial de ser significativamente mais eficiente. Como efeito colateral, o mesmo nível de confiança social poderia ser mantido com uma diminuição significativa da quantidade de trabalho necessária

Segurança & Privacidade

Então, a blockchain tem o potencial de verificar relações, contratos e transações mais eficientemente que instituições de grande porte. Mas a eficiência é inútil se o sistema também não for altamente seguro. Embora a tecnologia ponto-a-ponto exista desde a criação da internet, essas redes não eram seguras da forma que esperamos que instituições financeiras e governos sejam. Um banco tradicional protege a privacidade limitando o acesso à informação para apenas as partes envolvidas. Livros-razão bancários são documentos internos, e quando você abre seu histórico de transações, você só pode ver as transações em que você estiver envolvido. Esse papel de terceiro confiável, mantendo um livro-razão não público, é o papel principal de um banco. Tornar o livro-razão público é o fundamento da segurança da blockchain, mas um livro-razão público significa que a privacidade está comprometida. Esse era um dos problemas fundamentais para transações ponto-a-ponto antes de 2008. Ninguém conseguia descobrir como garantir privacidade usando um livro-razão aberto ao público. Os benefícios de um livro-razão público eram enormes para velocidade, custo e confiabilidade. Porém, os consumidores provavelmente não adotariam um sistema que permitira que suas transações fossem rastreadas.

Criptografia

A primeira camada de segurança e proteção de privacidade na blockchain é a criptografia. A informação sobre transações é armazenada em um mesmo amontoado. Isso inclui ID de transação, tempo, quantia, endereço do destinatário e endereço do remetente. A informação da transação é então passada por uma função de criptografia *hash* antes de ser adicionada ao livro-razão. Quando a informação da transação é criptografada, ela fica dessa forma (exemplo de uma transação de Bitcoin de 20 de outubro de 2017):

aba128d3931e54ce63a69d8c2c1c705ea9f39ca950df13655d

Uma função criptográfica *hash* encurta e padroniza o número de caracteres em uma descrição de transação, significando que mais transações podem ser enviadas pela rede a qualquer momento. Somente olhando para uma lista de transação, é impossível saber qualquer coisa sobre o destinatário, o remetente e a quantia. Porém, como os padrões de encriptação do Bitcoin são disponíveis publicamente, ainda é possível decriptar a transação e descobrir mais detalhes, incluindo a chave pública do destinatário e do remetente e a quantia enviada.

Novos competidores da Bitcoin usam diferentes tipos de criptografia para ofuscar ainda mais as informações da

transação, tornando impossível descobrir qualquer coisa sobre a transação após ela ser adicionada ao livro-razão.

Discutiremos encriptação e *hashing* em maior profundidade em um futuro capítulo.

Livro-Razão Distribuído = Difícil De Modificar

O livro-razão distribuído, um dos maiores desafios para a privacidade, é também a chave da segurança da blockchain. Um livro-razão tradicional mantido por um banco é protegido por várias camadas de segurança para impedir modificações não autorizadas. Porém, se um invasor consegue ter acesso ao livro-razão, ele poderia fazer mudanças instantaneamente. Livros-razão de um só dono também são sujeitos a transações fraudulentas. Se um ladrão de identidade ou vendedor malicioso enviasse ao banco uma requisição de transação em seu nome, é possível que a transação fosse aprovada sem seu conhecimento. Havendo somente um dono do livro-razão significa que os bancos devem gastar bastante energia e dinheiro mediando reclamações e agindo em casos de fraude. O livro-razão distribuído muda esses problemas. Como existem milhares de cópias independentes nos computadores individuais da rede, assim que a transação for adicionada ao livro-razão, é quase impossível mudar isso (discutiremos as razões técnicas disso em um capítulo mais a frente).

Anonimato & Chaves Privadas

Como a tecnologia blockchain usa um livro-razão distribuído, todo mundo tem uma cópia de todas as transações que ocorrem na rede. O livro-razão precisa ser público para funcionar. Porém, sem as devidas medidas de segurança, qualquer um no mundo pode ver o que você comprou e de quem. Implementações da blockchain resolvem esse problema de segurança de formas diferentes, mas a maioria depende de um sistema que desconecta suas informações pessoais de sua conta. Por exemplo, carteiras Bitcoins são anônimas, e você pode ter mais do que uma. A única coisa necessária para acessar sua conta é uma chave privada que só você conhece. Embora qualquer um possa ver o endereço da sua carteira privada, eles não saberão nada sobre quem é o dono da carteira. No artigo original do Bitcoin, é sugerido que você crie uma nova carteira para cada transação que você faça na rede Bitcoin para manter o anonimato. Outras criptomoedas, como a Monera, esperam aumentar o nível de privacidade para transações blockchain. Monera usa endereços *stealth* (discretos), separa IDs de usuários de montantes de transação e ofusca rastros de transação para garantir a privacidade (veja o capítulo sobre a Monero para maiores informações). O resultado é uma criptomoeda totalmente não-rastreável que ainda é sustentada por um livro-razão distribuído e público.

Imaginando Um Futuro Blockchain

Até agora, abordamos os básicos de porque a blockchain foi inventada, o que ela faz, e uma visão geral dos métodos usados pela blockchain. Estamos apenas na superfície, porém, e entraremos nos detalhes técnicos das implementações da blockchain no próximo capítulo. Primeiro, porém, vamos dar uma olhada nos potenciais usos da tecnologia blockchain. É importante entender que a tecnologia blockchain é muito maior do que apenas Bitcoin. Mesmo se o Bitcoin morrer amanhã, a tecnologia blockchain ainda será viável em muitas indústrias. Com novos desenvolvimentos em conexão ponto-a-ponto, programação blockchain e novas formas de criptografia, a tendência por confiança distribuída continuará, devido aos óbvios benefícios em termos de rapidez, custo e segurança. Embora possa não ser o Bitcoin ou o Ethereum que movam o futuro da blockchain, você pode ter certeza que as tecnologias por trás da blockchain serão implementadas durantes as próximas décadas. O efeito geral será a existência de contratos eficientes, transações mais rápidas e menores custos para operadores. A blockchain também tem o potencial de mudar a forma como fazemos compras, viajamos, elegemos líderes, trabalhamos e vivemos.

Finanças

As aplicações financeiras da blockchain recebem a maior atenção da mídia e são normalmente as primeiras plataformas baseadas na blockchain que os consumidores ouvem falar. Muito provavelmente a primeira vez que você ouviu falar "blockchain" foi em uma discussão sobre Bitcoin. Isso tem dois motivos. Primeiro, a blockchain usa livros-razão, e estes são mais presentes no mundo financeiro. A tecnologia é perfeita para aplicações financeiras. Segundo, a primeira aplicação bem sucedida da blockchain, o Bitcoin, foi projetada desde o início para ser uma moeda. Um futuro financeiro baseado na blockchain tem uma aparência radicalmente diferente da do sistema bancário atual. O uso de dinheiro vivo já está em queda, e é muito provável que os países ocidentais façam a transição para sistemas bancários totalmente eletrônicos no futuro próximo. No futuro blockchain, todas as transações poderiam ser pagas de sua carteira de criptomoedas. A existência de tecnologias novas e altamente ampliáveis significa que a sua transação poderia ser processada e verificada em segundos. Vendedores não teriam de pagar pelo processamento de pagamentos, e comprar algo provavelmente seria tão simples quanto autorizar a transação usando seu celular ou outro dispositivo conectado. Embora um futuro sem dinheiro em espécie pareça provável, não está claro quem irá controlar a moeda digital. Se moedas

descentralizadas como o Bitcoin ou grandes bancos irão ganhar no fim é algo ainda incerto. Os bancos já estão considerando formas de inserir a tecnologia blockchain em suas práticas atuais em uma tentativa de manter o papel de intermediário confiável em transações financeiras. A regulação de mercados financeiros também mudará. Governos coletam impostos e combatem lavagem de dinheiro, e ambas práticas ficam mais fáceis e mais difíceis usando blockchain. Como o livro-razão é público, rastrear transações é significantemente mais fácil, mas com transações anônimas e contas-fantasma, é possível que fique mais difícil haver regulação financeira governamental. Essa é uma das razões de porque grandes bancos podem continuar a controlar mercados financeiros, mesmo após implementar as melhores práticas da blockchain.

Contratos

Pagamentos são um dos exemplos de um contrato baseado em blockchain, mas já existem várias aplicações desenvolvidas na blockchain. Esses contratos usam a natureza distribuída da blockchain para criar confiança sem precisar de uma instituição, e eles não podem ser quebrados ou barrados por entidades externas. O Ethereum é a blockchain onde a maioria desses aplicativos estão sendo desenvolvidos, e é a segunda blockchain mais valiosa no mundo, depois do Bitcoin. O Ethereum permite que desenvolvedores trabalhem em cima de sua blockchain, e

os desenvolvedores podem criar programas no Ethereum como eles fariam com qualquer outra linguagem de programação. Isso significa que o Ethereum disponibiliza jogos online, redes sociais e provedores de serviço da mesma forma que a internet. A única diferença é que esses programas são descentralizados. Após serem criados, eles durarão o quanto a blockchain do Ethereum durar. Como usuários ao redor do mundo sustentam a blockchain do Ethereum, o governo não pode derrubar o serviço, e nenhum usuário pode deletar ou alterar os conteúdos do serviço. A melhor parte contratos inteligentes é que eles são ilimitados. Qualquer coisa que você puder programar em um computador pode ser programada na blockchain. No futuro, isso provavelmente incluirá inteligência artificial e outras formas de aprendizado de máquina, tornando a IA prontamente disponível para qualquer um que faça parte da rede ponto-a-ponto da blockchain.

Governança

A tecnologia blockchain não se limita a finanças. Nos últimos anos, emergiram tecnologias que permitem que desenvolvedores criem programas baseados em uma blockchain. Isso significa que aquele código está vinculado à blockchain e mantido pela rede ponto-a-ponto. Um grande exemplo de como isso poderia funcionar é em votações. Atualmente, dependemos de comissões eleitorais, instituições centralizadas, para administrar eleições e contar votos. Esses sistemas não são perfeitos. Eles requerem

que você vá ao local de votação em pessoa em determinado dia, tenha seus dados pessoais verificados, e que vá até uma cabine fazer seu voto em uma urna. Cada um desses passos introduz um problema aos votantes. Se eu não posso ir ao local de votação no dia em questão, eu não posso votar. Se eu não tiver minha identificação comigo, eu não posso votar. Se eu fizer meu voto incorretamente, meu voto não será contado, e em alguns casos, falhas técnicas ou problemas de contagem significam que votos serão excluídos. Ao fim do dia de eleição, eu tenho que confiar que os funcionários da eleição no país todo não vão cometer fraudes e vão contar os votos de forma justa. Em alguns países, onde um ditador está no poder ou as instituições não são fortes, as eleições podem ser aparelhadas sem que os votantes possam fazer algo. Os desenvolvedores da blockchain esperam resolver esses problemas com um contrato de votação inteligente através de um livro-razão distribuído na blockchain. A ideia é simples: criar uma rede ponto-a-ponto onde indivíduos possam submeter seus votos sem precisar confiar nas comissões de eleição ou estar presente em pessoa. Porém, a implementação é difícil. Como você verifica a identidade? Como você impede que pessoas votem mais de uma vez? Se o livro-razão está na blockchain, como você mantém os votos anônimos? Será necessário uma criptografia inteligente antes que tenhamos votações baseadas na blockchain, mas as implicações são enormes. Assim que votar se tornar tão fácil quando entrar em seu celular ou computador e dar seu voto, a democracia direta e referendos públicos frequentes se

tornam mais possíveis. Decisões de políticas poderiam ser feitas pelas massas. Inclusive, você poderia votar em referendos na sua cidade múltiplas vezes por dia.

Embora precisará de mais trabalho para ter certeza de que os especialistas estão escrevendo e revisando as políticas em que o público vota, não é um exagero pensar que a governança poderia ficar mais ágil e responsiva graças à blockchain.

Crowdfunding & ICOs

Um exemplo de serviço que está usando contratos inteligentes é o *crowdfunding* (financiamento coletivo). Estamos acostumados a pensar em campanhas do Kickstarter, e a ideia é bem simples. Pessoas contribuem para uma boa ideia. Quando a ideia atinge seu objetivo de financiamento, os criadores da ideia são pagos para produzir a ideia. Se eles não atingem o objetivo, os apoiadores originais recebem o dinheiro de volta.

Na blockchain, toda a arrecadação de fundos, cálculo e financiamento/retorno do dinheiro é automatizada e tornada imutável em um contrato inteligente. Sendo um aplicativo descentralizado na blockchain, não há mais o Kickstarter como intermediário. Ao invés disso, o contrato inteligente decide quando uma ideia será financiada, e os criadores não pagam quaisquer taxas pelo serviço. Recentemente, o financiamento coletivo via blockchain cresceu em popularidade para financiar novas ideias de startup, ameaçando o modelo

tradicional de capital semente, capital de risco e investidores institucionais. Fundadores de startups agora oferecem um tipo de veículo público de investimento, conhecido como *oferta inicial de moedas* (*initial coin offering – ICO*), onde qualquer um pode investir em uma ideia em troca de uma participação no crescimento da empresa. Embora ICOs tenham ficado incrivelmente populares, e muitas se tornaram muito bem-sucedidas, elas também são amplamente não regulamentadas, tornando-as investimentos de alto risco e sujeitas a práticas questionáveis de investimento, como manipulação de preços por *pump and dump*.

Seguros

Outro exemplo de contrato inteligente em potencial é o seguro de carros. Com a maior presença de pequenos sensores e dispositivos em nossos carros, não estamos longe de uma época em que o seu carro possa sentir quando você sofre um acidente e enviar essa informação a um aplicativo descentralizado na blockchain. Quando integrado com inteligência artificial, visão computacional e sensores inteligentes em seu carro, o aplicativo da blockchain pode decidir se você foi o culpado e pagar os créditos do seguro em segundos, contanto que você tenha pago os prêmios todo mês. Agora, não há mais empresa de seguros para cobrar taxas, e o aplicativo de seguro da blockchain não tenta lucrar com isso, então seus prêmios mensais são somente

o que eles precisam ser.

Identidade & Identidade das Coisas

O livro-razão distribuído da blockchain também pode armazenar informação sobre identidade.

Ao invés de depender de instituições centralizadas para fazerem documentos de identidade, carteiras de motorista, passaportes, certificados, diplomas e contas, a blockchain pode facilitar a existência de uma identidade única e universal. A segurança de blockchain significaria que suas transações permanecem anônimas por padrão. Porém, você poderia escolher compartilhar informações de identidade como parte do cumprimento de um contrato. Com o tempo, poderíamos padronizar uma identidade e cidadania global na blockchain para toda pessoa viva.

Конец ознакомительного фрагмента.