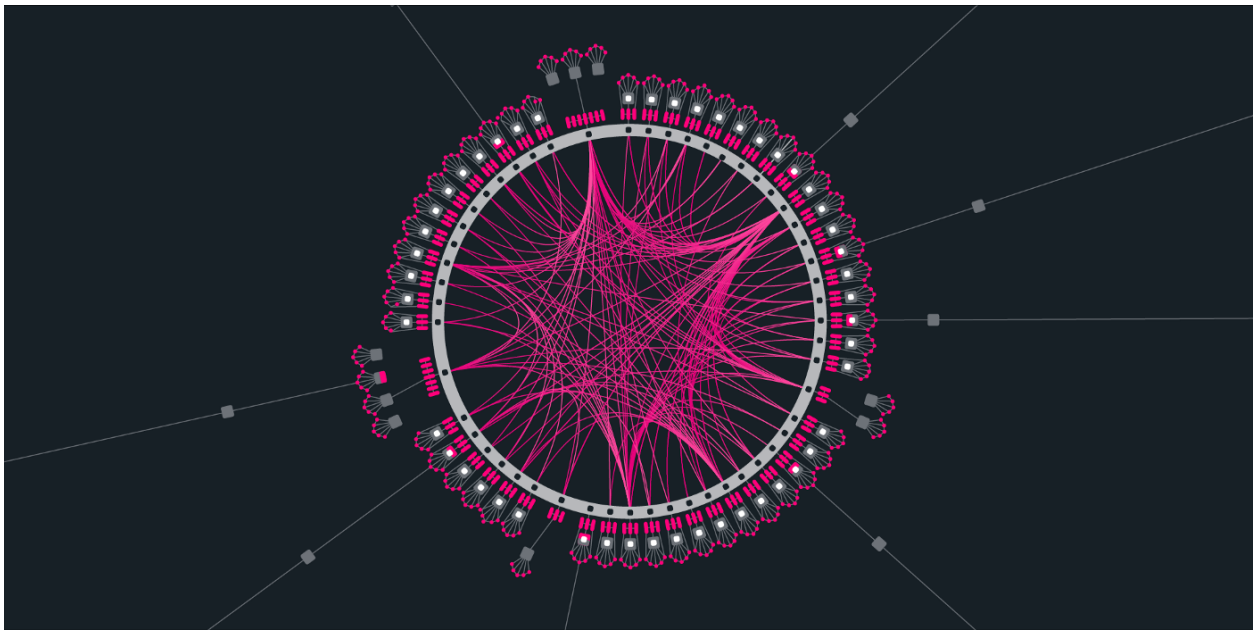
Polkadot
PARA INICIANTES

Um guia não técnico para descentralização, *blockchains* e Polkadot

gbaci

Traduzido por: Panegali e Pitcoin



POLKADOT PARA INICIANTES

Um guia não técnico para descentralização, *blockchains* e Polkadot

Author: Gbaci

Traduzido por: Panegali e Pitcoin

Polkadot para Iniciantes: Um guia não técnico para a descentralização, *blockchains* e Polkadot por gbaci

Publicado por gbaci

Lagos, Nigéria

Editado por AnaelleLTD

Traduzido por: Panegali e Pitcoin

Primeira edição

AGRADECIMENTOS

Este livro foi possível graças à tesouraria de Polkadot, um mecanismo que permite à comunidade do ecossistema financiar projetos e ideias que ajudam a fomentar uma maior adoção das tecnologias de Polkadot.

Primeiramente, gostaria de agradecer a Raul Romanutti por sua ajuda e orientação durante a elaboração de minha proposta à tesouraria.

Agradecimentos também são devidos aos membros do Conselho de Polkadot que têm a ingrata tarefa de supervisionar e orientar a rede para uma estabilidade e crescimento duradouro. Sem sua dedicação, o ecossistema não teria feito o progresso que o ajudou a prosperar nos últimos dois anos.

Gostaria também de estender meu apreço a Emre Surmeli por sua imensamente útil orientação durante a revisão técnica do conteúdo deste livro. Bill Laboon, Chefe de Educação da Fundação Web3, também foi fundamental para que este livro ganhasse vida.

Sinto-me em dívida com Anaelle LTD por suas habilidades de edição especializadas e *insights* sobre tecnologias *blockchain* que tornaram este livro muito mais fácil de ler.

Finalmente, quero agradecer aos membros da comunidade de Polkadot que participaram da elaboração deste livro respondendo a *tweets*, enquetes e pedidos de resenhas preliminares. Uma comunidade é tão forte quanto à dedicação de seus membros e sou grato por fazer parte de um ecossistema repleto de pessoas comprometidas que estão ansiosas para ajudar uns aos outros a prosperar.

Polkadot.

ÍNDICE

PREFÁCIO

Até o século XV, o comércio europeu era dominado pelos venezianos e genoveses que controlavam o comércio mediterrâneo. Estes mercadores compravam mercadorias de comerciantes no porto de Alexandria, no Egito, mercadorias que eram originárias principalmente da Índia e eram então adquiridas por comerciantes árabes que as movimentavam através do Mar Vermelho para o Egito. Estas mercadorias eram então vendidas no Cairo, onde eram fortemente tributadas pelo Sultão antes de chegar aos comerciantes em Alexandria. De lá, os venezianos e os genoveses distribuíam essas mercadorias por toda a Europa a preços muito caros. No entanto, como em qualquer sistema ineficiente onde alguns se beneficiam à custa de outros, haveria alguns para desafiar este *status quo*.

No final do século XV, os portugueses descobriram uma rota direta para a Índia, o que lhes permitiu contornar a tempo todos esses intermediários e transportar seus produtos a uma fração do que os europeus continentais eram obrigados a pagar. Isto levou a uma mudança radical na forma como o velho mundo operava e, em poucos anos, Veneza e Gênova não eram mais atores relevantes no comércio com o Oriente.

Pense na tecnologia *blockchain* como "a descoberta portuguesa da rota direta para a Índia". A ideia principal é que, a fim de perturbar o "velho mundo", certas infraestruturas precisam estar em funcionamento. No exemplo acima, não se podia fazer muito nos primeiros anos da descoberta até que os portos estivessem seguros, os contatos fossem feitos e os fornecedores fossem estabelecidos. A implementação desta infraestrutura foi o golpe final que destruiu os venezianos e estabeleceu uma nova maneira de fazer comércio e negócios.

Hoje, a infraestrutura necessária para a *blockchain* decolar e consolidar a disrupção foi construída. Diferentes indústrias começaram a convergir - jogos e cripto, identidade e cripto, finanças e cripto, só para citar algumas. Quando este entrelaçamento de indústrias ocorre, a magia acontece, e só podemos especular sobre o tipo de inovações que nascerá. O futuro é emocionante e está ficando claro que os projetos de *blockchain* precisarão se comunicar e interoperar com outros projetos, assim como com outros atores fora do mundo criptográfico.

Na situação atual, o mundo não é mais dominado por uma única *blockchain*. Entramos na era *multi-chain* (Múltiplas cadeias), e é aqui que Polkadot desempenha um papel importante, como você aprenderá ao longo deste livro.

Nas finanças tradicionais, tem havido uma atitude um tanto arrogante em relação ao Bitcoin e todas as suas ramificações que impediram muitos (inclusive eu) de ver os benefícios da tecnologia *blockchain* em seus estágios mais iniciais. Felizmente, esta atitude está mudando. As finanças tradicionais têm muitos desafios que ainda não foram

superados, apesar de terem um impacto persistentemente negativo no sistema financeiro e econômico mundial. Bancos, dentro das finanças tradicionais, por exemplo, administram um sistema de incentivos que não está alinhado com outros participantes do mercado. Os banqueiros, têm sido um deles, são míopes, focados em bônus de final de ano, e não são responsáveis por suas ações. Esta configuração levou a práticas bancárias menos aceitáveis, como o mundo viu durante a Grande Crise Financeira, em que a ganância impulsionou a venda de produtos de investimento que tinham preços tão seguros, mas que na verdade eram extremamente arriscados. As recomendações de investimento não são feitas com base no que beneficia os investidores, mas na quantidade de taxas que são geradas e nos dados armazenados dentro de entidades centralizadas.

Quando comecei a estudar a tecnologia *blockchain*, comecei a descobrir que as redes descentralizadas e "permissionless" (sem permissão) tratam dos problemas de confiança e segurança de tal forma que não temos mais que confiar somente nas corporações. Aprendi que os incentivos incorporados aos protocolos da *blockchain* asseguram que os interesses econômicos estejam alinhados e que os participantes possam ser responsabilizados. Aqueles que querem usar uma rede, fazer propostas sobre governança ou ganhar ajudando a proteger uma rede, devem possuir *tokens* (unidades de criptoativos, como criptomoedas e *tokens* não fungíveis - *NFTS*) de tais projetos. Isto, em última análise, leva a um bom comportamento e *compliance*, pois, caso contrário, os participantes correriam o risco de perder seu capital.

Demorei algum tempo para entender o Bitcoin e suas características únicas como novo membro do mundo monetário, e apreciar como seu surgimento complementa a forma como negociamos com dinheiro. Primeiro, tomei conhecimento da *blockchain* Bitcoin, um protocolo cuja função é registrar transações de bitcoins. Depois aprendi sobre o Ethereum, uma *blockchain* "programável" cujo protocolo permite construir aplicações e *smart contracts* (contratos inteligentes) nela para registrar transações na cadeia. Pense no Ethereum como um *smartphone* onde você pode baixar e executar aplicações, enquanto a *blockchain* Bitcoin é um telefone fixo usado exclusivamente para fazer e receber chamadas.

Ethereum abriu a Caixa de Pandora em termos do que poderia ser feito com a tecnologia *blockchain*. Com a explosão do tráfego na *blockchain* Ethereum, seus inconvenientes começaram a surgir. Alguns deles são bem conhecidos: altas taxas de *gas* (a quantidade que alguém está disposto a pagar por uma transação ou por uma interação com um contrato inteligente) e transações lentas; no entanto, alguns não são tão intuitivos. A *blockchain* Ethereum não foi projetada para ser atualizada com muita frequência, portanto, quando são necessárias atualizações, elas são extremamente difíceis e demoradas para implementar. Outro inconveniente é que a *blockchain* Ethereum não foi construída para se comunicar com outras cadeias, pois seu projeto original não considerava a questão da interoperabilidade. Foram esses problemas que deram origem à Polkadot.

Polkadot permite que *blockchains* independentes chamadas "*parachains*" se conectem a ela, essencialmente lidando com a conectividade e segurança para elas. Polkadot pode

mudar seu próprio projeto ao longo do tempo e permite a interoperabilidade entre diferentes cadeias. Polkadot torna todo o espaço da *blockchain* muito mais escalável e melhora os efeitos de rede, é essencialmente como uma ferrovia que conecta cidades e permite que a atividade econômica floresça.

Devido à velocidade da inovação no espaço das *blockchains*, e ao fato de eu mesmo não ser um cientista da computação ou desenvolvedor, tem sido difícil identificar quais projetos de *blockchain* farão a diferença. No exemplo Português que vimos anteriormente, se você estivesse em Lisboa e soubesse da descoberta, poderia ter investido em um único navio e trazido especiarias para seu próprio negócio pessoal. Isso teria sido extremamente arriscado, já que não havia muitos navios que voltassem com segurança naqueles dias. Imagine um investimento melhor, como uma fábrica de navios, onde você se beneficia não apenas da venda dos navios que constrói, mas também através de potenciais royalties de expedições bem sucedidas.

Eu penso em Polkadot exatamente assim. Polkadot requer *blockchains* independentes para ganhar um leilão e alugar um espaço, de modo que elas possam ser conectadas à infraestrutura de Polkadot e se tornarem uma *parachain*. Isso significa que os projetos podem se concentrar em seus casos de uso e deixar Polkadot cuidar da segurança e conectividade. Os apoiadores desses candidatos a *parachain* podem emprestar DOTs - o símbolo nativo de Polkadot - aos projetos e ser recompensados com *tokens* dos próprios projetos caso uma vaga como *parachain* seja assegurada. Esse sistema garante a manutenção da qualidade dos projetos, a relevância para os usuários e o apoio de sua comunidade para continuar a implantação em Polkadot após o término dos aluguéis de *slots*. Esta configuração extraordinária garantirá que o ecossistema Polkadot sempre receba os melhores projetos e permaneça na vanguarda da inovação. É por isso que penso que Polkadot desempenhará um papel essencial no espaço de *blockchains*.

Nunca antes o mundo teve milhões de pessoas incrivelmente inteligentes trabalhando simultaneamente em protocolos de código aberto, o que levou a uma explosão cambriana nos usos da *blockchain*. Estamos apenas começando, e é simplesmente um momento maravilhoso para estarmos vivos. Talvez depois de ler este livro você concorde comigo que investir em Bitcoin é investir no preço, investir em *blockchain* é investir em inovação, e investir em Polkadot é investir no sistema ferroviário que vai levar muito dessa inovação adiante.

Jean Philippe Tissot

Fundador e Gerente de Portfólio da Arauca Capital

UMA BREVE INTRODUÇÃO

Desde seu lançamento em 26 de maio de 2020, Polkadot captou a imaginação de uma grande variedade de pessoas que compartilham valores semelhantes sobre o futuro da organização humana. Polkadot é uma *blockchain* cujo objetivo principal é conectar outras *blockchains*. Dado que são poucas as pessoas que entendem o que é uma *blockchain*, é natural que elas pensem que a ideia objetiva de Polkadot de conectar outras *blockchain* é algo confuso. Assim, tentar entender o que é Polkadot e como ela funciona é um árduo esforço intelectual. Ou pelo menos, costumava ser.

Este livro foi escrito com o único propósito de simplificar a imensa complexidade de Polkadot para que o leitor médio possa entender este ecossistema sem nenhum conhecimento técnico prévio de *blockchains* ou redes de computadores. Para conseguir isso, uma grande quantidade de tecnicidade foi retirada da apresentação de muitos conceitos. E assim, embora este livro seja ideal para o leitor médio, ele pode não ser para uma pessoa tecnicamente experiente. Dito isso, ainda há muito a aprender sobre Polkadot, que não se enquadra no escopo de tecnicidades, governança, *crowdloans* (um mecanismo de financiamento que usuários emprestam seus *tokens* DOT para um determinado projeto concorrer ao leilão), e leilões de *parachain* para citar alguns.

A esperança deste escritor é que o leitor fique tão fascinado e tão inspirado quanto eu estava quando li pela primeira vez o *whitepaper* de Polkadot, um documento que apresentava uma visão arrojada da tecnologia de *blockchains* e a *web* descentralizada (também conhecida como *Web* 3.0), propondo a solução do problema de escalabilidade (para máxima adoção), segurança compartilhada (para máxima diversificação), e interoperabilidade (para máxima inovação e usabilidade). O *whitepaper* de Polkadot deixou claro que seu objetivo era permitir a adoção em massa por meio da propriedade digital e a liberdade para o indivíduo, construindo o maior número possível de tipos diferentes de *blockchains*, cada uma dedicada a uma indústria diferente que necessita de uma revolução.

Mas eu estou colocando o carro à frente dos bois. Uma explicação do que é Polkadot e como ela faz o que faz virá mais tarde. Primeiro, vamos começar com o porquê de tudo isso. Descobri que a maneira mais fácil de entender uma nova tecnologia é compreender a

filosofia que impulsionou sua criação. Assim, vamos começar com a filosofia da descentralização.

A FILOSOFIA DA DESCENTRALIZAÇÃO

Meu objetivo neste capítulo é explicar por que a descentralização é necessária. Por que passar por isso primeiro? Porque parece ter algum mal entendido entre as pessoas que são chamadas para o mundo descentralizado. Muitos vêm em busca de lucros, acreditando que isso é tudo que a indústria tem a oferecer.

É claro que há muitos construtores no espaço, que estão apenas focados no crescimento de seu patrimônio, e isso não é de todo ruim. Quero dizer, todos são livres para fazer o que quiserem. Mas não esqueçamos que o Bitcoin, com uma forte capitalização de mercado de mais de 600 bilhões de dólares, foi uma reação contra a tirania e insensibilidade da elite financeira. Vitalik Buterin, o criador de Ethereum, foi levado a criá-lo por causa da tirania dos conglomerados. Em uma famosa anedota, ele lembrou ir dormir chorando quando o famoso jogo *World of Warcraft* unilateralmente confiscou todos os seus bens no jogo.

Ambas as instâncias eram sobre a liberdade para o indivíduo. Havia dinheiro envolvido? Claro. O lucro financeiro foi o objetivo final? Não. O objetivo sempre foi levar a humanidade para um lugar melhor, para uma liberdade individual maior. Se a descentralização alguma vez perder de vista este objetivo final, então ela ficará fora de controle, algo mais próximo de uma hidra imbatível.

Lições de nossos antepassados: A necessidade de centralização

Os termos centralização e descentralização referem-se a diferentes formas de poder de gestão, propriedade e autoridade. Poder, propriedade, e autoridade estão diretamente relacionadas à segurança porque:

1. Aquele que os possui é responsável pela segurança do que possui.
2. Aquele que é dono tem poder e autoridade sobre o que possui.

Em um sistema centralizado, todos os três atributos (poder, propriedade e autoridade) fluem e são emitidos a partir de um centro - Rei, Conselho, Governo, *CEO*, Gerência, etc. Dessa maneira, o governo é um agente central que organiza os assuntos nacionais, enquanto a empresa é um agente central que organiza os assuntos comerciais. Este modo centralizado de organização tem nos servido bem durante séculos porque foi o método

mais eficaz que tivemos para nos unir e construir civilizações. Mas este nem sempre foi o caso. A centralização, como já a conhecemos, começou com a invenção da agricultura.

Antes da agricultura, nossos ancestrais caçadores/coletores não estavam estacionados em um único lugar, nem possuíam muitas coisas; e por isso, naturalmente, não precisavam se preocupar com a segurança da maneira como fazemos atualmente. Seu modo de governar era mais descentralizado, para que a tribo decidisse coletivamente o que fazer e para onde ir. Mas ao encontrar os benefícios da agricultura, nossos ancestrais caçadores/coletores abandonaram seu estilo de vida nômade por um estilo de vida sedentário.

A partir de então, as pessoas tinham terras agrícolas, casas e vilarejos com fronteiras claras traçadas. Com um abastecimento alimentar mais estável veio a explosão da população, o que trouxe novos problemas à tona.

Por um lado, nossos ancestrais tinham muitas decisões a tomar. Como eles iriam compartilhar a terra? Quem resolveria as disputas? Quem vai liderar em tempos de guerra pela autodefesa e pela conquista? Imagine um bando de soldados de um reino rival chegando para conquistar um reino de 5.000 habitantes. Se o reino invadido dependesse de um modelo descentralizado de organização, então precisaria deliberar longamente antes de chegar a uma conclusão. Até lá, o reino teria certamente sido capturado pelos invasores.

Assim, um novo modo de organização era necessário para corresponder à nossa nova prosperidade e estilo de vida. Então, começou a popularização da centralização como nosso princípio de organização de fato.

A centralização foi amplamente viabilizada graças à especialização, em que todos os membros da tribo não precisavam mais se tornar agricultores. Graças a um fornecimento estável de alimentos, as pessoas podiam se especializar de acordo com seus talentos e com as tarefas disponíveis. Nossos ancestrais descobriram que se algumas pessoas fossem encarregadas de liderar, argumentando sobre o caminho certo e tomando decisões, a comunidade se tornaria mais eficiente na utilização de seus recursos e na resolução de problemas.

Entender o que realmente estava acontecendo aqui. A comunidade decidiu conceder seu poder, propriedade e autoridade a um centro (Rei, Conselho, etc.) em prol de uma maior eficiência. Esta evolução foi descrita por *Thomas Hobbes* em *Leviathan* (1651). Segundo *Hobbes*, uma organização omnipotente ganha vida quando seus membros individuais renunciam ao seu direito de viver de acordo com as leis da natureza (conhecido como "cada um por si"), entregam todos os seus poderes ao soberano (agente central), que é criado como resultado deste ato, e prometem obedecer a partir daí às leis feitas pelo soberano.

Esse modo de organização tem nos servido bem durante séculos: ajudou a dar início às civilizações e as elevou ao seu *status* atual.

Depressões, Censura e Protestos: O lado obscuro da centralização

> *O colapso do mercado imobiliário americano em 2007, que nenhum regulador havia previsto, foi causado por ilusões generalizadas de segurança em investimentos abstratos, que quase ninguém entendia. O sistema continua tão complexo agora como era então e uma crise semelhante pode acontecer novamente. Talvez amanhã.*
>
> *- Hans Rosling, Factfulness*

Como todos sabemos, tudo tem um lado obscuro. No caso da centralização, fomos expostos a seus aspectos mais sombrios, assumindo que as coisas nunca poderiam ficar piores. Mas a realidade nos provou que estamos errados.

Em 2008, a economia global foi arrastada para a "Grande Crise Financeira" pelas ações de alguns banqueiros nos Estados Unidos. Pense nisso por um segundo. O mundo inteiro experimentou dor e tristeza por causa de alguns poucos humanos que, no final, receberam grandes salários por sua ganância e incompetência.

O verdadeiro problema da crise era que os banqueiros não tinham pele em risco (*skin in the game)*. Eles estavam jogando com o dinheiro de outras pessoas, e quando o perderam, não houve grandes consequências para eles, mas o resto do mundo teve que pagar. Isto foi um fracasso do desenho de incentivos no mundo financeiro tradicional, e é também por isso que o novo movimento *Web3* é uma evolução bem vinda. Se os protocolos financeiros descentralizados perdessem dinheiro por qualquer razão, não haveria governo que os socorresse.

Eu, pessoalmente, vivenciei o lado obscuro da centralização durante os protestos do *EndSARS* na Nigéria. O governo nigeriano, abusando de seu poder, forçou os bancos a bloquear as contas das pessoas que estavam ajudando e facilitando os protestos pacíficos (posso testemunhar que estes eram protestos pacíficos porque eu acompanhei tudo isso). Foi preciso Bitcoin e Ethereum para sustentar o movimento por mais uma semana, antes que o governo reprimisse as manifestações da forma mais deprimente imaginável. Ele enviou o exército para o *Lekki Tollgate* em Lagos, onde soldados atiraram contra os manifestantes, ferindo e matando cidadãos que só queriam uma vida melhor. Até hoje, pensar nisso me traz lágrimas aos olhos. Que um governo possa desencadear o exército contra cidadãos inocentes é o maior abuso do poder centralizado. A ironia amarga aqui é que os protestos tinham como objetivo acabar com a brutalidade policial que a unidade de polícia desonesta chamada SARS estava cometendo com jovens nigerianos. Aqui está um relatório da CNN sobre a tragédia.

Eu também poderia tomar o caso do Facebook, Google e outros produtos e serviços da *web*, que usamos como exemplos de centralização que deu errado. A *web* atual está estruturada de forma a incentivar maiores níveis de centralização ao longo do tempo. O Google é tão valioso para os anunciantes devido aos dados que pode acessar mas que na verdade não são de sua propriedade.

O mesmo vale para o Instagram e outros aplicativos de mídia social que utilizamos. Sem os dados dos usuários, eles valeriam muito menos do que valem atualmente. Estas empresas se especializaram em levar nossos dados para crescer impérios de bilhões de dólares sem nunca nos pagar um centavo, os verdadeiros proprietários. Pior ainda, eles podem (e fazem) nos censurar sempre que quiserem. Esta é a realidade em que vivemos e crescemos, porque não tínhamos nenhuma alternativa real até o Bitcoin aparecer. Mas chegaremos ao Bitcoin em um momento.

Para entender melhor o lado obscuro da centralização, precisamos explorar a trindade — propriedade, poder e autoridade.

A propriedade refere-se a quem possui um item. No caso de um país, a terra pertence ao governo, exceto nos casos em que os cidadãos tenham adquirido essas terras. Mas mesmo nesses casos, os governos ainda se reservam o direito de confiscar as terras.

Poder se refere a capacidade de agir. Novamente, em um país, o poder é distribuído pela sociedade, com a maior parte pertencente ao governo (dividida em hierarquias). Assim, o presidente tem mais poder do que o vice-presidente porque tem a capacidade de fazer mais do que o vice-presidente. Os cidadãos têm poder porque podem votar e protestar.

A autoridade se refere a capacidade de controle. Naturalmente, aquele que tem propriedade e poder também tem autoridade por padrão. No espaço atual da mídia social, você não possui nada, nem mesmo sua conta. É por isso que você pode ser bloqueado ou suspenso. Você também não tem muito poder sobre nada além de sair se não gosta de como as coisas estão indo. E finalmente, você não tem autoridade para dizer à empresa o que fazer, exceto no caso em que um grande número de membros da comunidade concorde com você (porque as empresas gostam de se curvar à vontade da maioria). Este é o atual estado das coisas, inclusive com sua conta bancária. Os bancos podem congelar suas contas por qualquer razão, especialmente se o governo pedir.

Isto não quer dizer que seja ruim para o governo ou para os bancos ter tais poderes, pois a verdade é que às vezes este poder é bem utilizado. Mas, na maioria das vezes, há abusos de poder. É apenas a natureza do poder, se for grande demais, ele se corromperá. Este é um dos maiores problemas da centralização. Ela incentiva a acumulação de uma grande quantidade de poder nas mãos de poucas pessoas. Naturalmente, isso cria complexo de deuses em alguns indivíduos, transformando-os em tiranos (onde 'tirano' não é reservado apenas para chefes de estado desonestos).

Assim, o imperativo de abandonar a centralização é múltiplo:

1. A história tem provado, até certo ponto, que poder demais corrompe.
2. A centralização cria pontos únicos de falha, facilitando a tomada de controle de um sistema. Uma perfeita ilustração disto é a história de *Atahuallpa*.

> *Atahuallpa era o monarca absoluto do maior e mais avançado estado do Novo Mundo, enquanto Pizarro representava o Santo Imperador Romano Carlos V (também conhecido como Rei Carlos I da Espanha), monarca do estado mais poderoso da Europa. Pizarro, liderando um grupo de 168 soldados espanhóis, estava em terreno desconhecido, ignorando os habitantes locais, completamente fora de contato com os espanhóis mais próximos (1.600 quilômetros ao norte no Panamá) e muito além do alcance de reforços . Atahuallpa estava no meio de seu próprio império de milhões de súditos e imediatamente cercado por seu exército de 80.000 soldados, recentemente vitorioso em uma guerra com outros índios. No entanto, Pizarro capturou Atahuallpa poucos minutos depois que os dois líderes se viram pela primeira vez. Pizarro continuou a reter seu prisioneiro por oito meses, enquanto extraia o maior resgate da história em troca de uma promessa de libertá-lo. Após a entrega do resgate, ouro suficiente para encher uma sala de 30 m^2 - Pizarro renegou sua promessa e executou Atahuallpa. A captura de Atahuallpa foi decisiva para a conquista europeia do Império Inca. Embora as armas superiores dos espanhóis tivessem garantido uma vitória final em qualquer caso, a captura tornou a conquista mais rápida e infinitamente mais fácil. Atahuallpa foi venerado pelos Incas como um deus sol e exerceu autoridade absoluta sobre seus súditos, que obedeceram até mesmo as ordens que ele emitiu do cativeiro. Os meses até sua morte deram a Pizarro tempo para despachar os grupos de exploração não controlados para outras partes do Império Inca, e para enviar reforços do Panamá. Quando os combates entre espanhóis e incas finalmente começaram após a execução de Atahuallpa, as forças espanholas foram mais formidáveis.*
>
> *— Jared Diamond; Guns, Germs, and Steel.*

3. A centralização incentiva as pessoas a abdicarem de seu poder e responsabilidade, levando inevitavelmente tomada de decisões que marginalizam muitos na comunidade.
4. A centralização cria assimetrias em propriedade, poder e autoridade, colocando o destino de muitos nas mãos de poucos.

A única solução?

Uma solução para as armadilhas da centralização é a descentralização. Talvez não seja a única solução, mas é a melhor opção que temos atualmente. A descentralização, em sua essência, está preocupada com a redistribuição de poder e autoridade de alguns poucos indivíduos no centro para a comunidade em geral. Em tal sistema, nenhuma pessoa ou

grupo governa sobre o sistema: riscos, responsabilidades e recompensas são compartilhados por todos. Portanto, o maior apelo da descentralização é a justiça. É muito melhor saber que caímos por causa de nossa ação coletiva do que por causa das ações de uns poucos. É melhor saber que ninguém pode ser silenciado por falar contra a injustiça, a crueldade, a corrupção, o fanatismo, etc. É melhor saber que todos são financeiramente livres para fazer transações com quem quer que seja, onde quer que seja e quando quer que seja.

A filosofia da descentralização é a ruptura das estruturas de poder centralizadas. A consequência natural de tal filosofia é uma maior liberdade. A natureza e o tipo de liberdade, entretanto, depende de qual sistema descentralizado estamos falando. Bitcoin foi criado com o objetivo de liberdade financeira, para dar às pessoas a opção de se libertarem de uma máquina econômica com a qual estavam profundamente insatisfeitas. O Ethereum queria oferecer aos desenvolvedores a liberdade para construir aplicações que poderiam mudar o mundo - continuando estimular o crescimento das finanças descentralizadas (o que deu a muitas pessoas a liberdade de fazer o que os banqueiros fazem) e *NFTs* (o que deu aos criadores um caminho para a liberdade artística diferente de tudo o que a indústria da arte viu durante décadas). Estes são apenas os dois primeiros casos emblemáticos de uso. Espera-se plenamente que dentro dos próximos dez anos, produtos mais descentralizados cheguem ao mercado, oferecendo alternativas aos sistemas atuais.

Em resumo, as vantagens da descentralização são:

1. Maior segurança porque o sistema não pode ser sequestrado. Por exemplo, se o Google for invadido, o *hacker* terá acesso a todas as informações que o Google possui. Se o presidente de algum país for sequestrado por agentes das trevas (ou alienígenas), a nação não colapsará porque o sistema possui muitos indivíduos.

2. Maior equidade porque mais pessoas estão envolvidas na tomada de decisões. Uma comunidade que atua somente em questões chave quando a maioria aprova tal ação está mais alinhada com o ideal de que todos são iguais. Se apenas algumas poucas pessoas tomarem decisões pela comunidade, não demorará muito para que elas decidam favorecer seus próprios interesses e tirar proveito da comunidade.

3. Melhor distribuição da propriedade. Poucas pessoas não devem ser donas de tudo porque isso vai contra o projeto de vida. O leão não é dono da selva, apesar de poder matar quase todos os animais que nela habitam. Se a propriedade não é compartilhada, então o crescimento e o progresso beneficiam apenas alguns, e isso é um triste estado das coisas que fomenta maior desigualdade.

No próximo capítulo, exploraremos como podemos alcançar a descentralização.

O "COMO" DA DESCENTRALIZAÇÃO

> *Perdemos milhares de células nervosas a cada hora, mas praticamente não tem efeito devido à natureza altamente distribuída de todos os nossos processos. Nenhuma de nossas células cerebrais individuais é tão importante, não há nenhum neurônio Chefe do Executivo.*
>
> *— Ray Kurzweil; The Age of Spiritual Machines.*

Após compreender a necessidade, o propósito e as vantagens da descentralização, vamos agora explorar como podemos alcançá-la na prática.

No passado, era relativamente impossível levar muitos seres humanos a trabalharem em conjunto para um objetivo maior de forma descentralizada. Como previamente explicado, cada tentativa de organização em direção a um grande objetivo foi facilitada pela centralização. Mas por que é assim?

Bem, o maior problema que enfrentamos quando tentamos levar muitas pessoas a trabalharem em conjunto é a questão da confiança. É por isso que a centralização tem sido o modelo organizacional dominante durante os últimos séculos. A centralização contornou a questão da confiança, dando a todos um partido central de confiança. É assim que os bancos trabalham: seu objetivo principal é nos ajudar a saber quem tem o que e quem pode enviar o que. Este é também em parte o motivo da existência dos governos: para nos ajudar a determinar quem pode e deve fazer o que. Confiamos nos bancos para manter nosso dinheiro seguro, governos para nos manter seguros e facilitar a prosperidade, e empresas de mídia social para nos fornecer um serviço. Assim, quando se trata de descentralização, a questão se torna: como você pode fazer o maior número possível de pessoas confiarem umas nas outras?

A resposta curta é: você não pode. Confiança é manter o controle das informações de forma segura para que ninguém possa questionar sua validade. A solução centralizada tem sido delegar a confiança a uma entidade, seja através do poder, da autoridade ou da propriedade. Mas isso representa alguns riscos:

1. A centralização cria uma assimetria de informação que alguns controladores centralizados utilizam em seu benefício às custas de muitas partes interessadas. Este é o caso, por exemplo, quando um empresário ouve falar de uma decisão governamental antes de todos os outros porque ele é amigo de alguns senadores e pode tirar proveito de sua posição. Os banqueiros e as empresas estão sempre em conluio, da mesma forma que os governos e os bancos trabalham juntos. Em resumo, os indivíduos em posições de poder são incentivados a esquematizar e colocar seus próprios interesses à frente do bem coletivo.

2. A coleta e verificação de informações centralizada apresenta um único ponto de falha. Isto pode se manifestar de diferentes maneiras. Por um lado, os servidores centralizados (computadores onde as informações são armazenadas, registros bancários, registros governamentais, dados de usuários, etc.) podem ser hackeados. Como o *hacker* só precisa se concentrar em um vetor de ataque, há um incentivo para invadir e roubar dados. Por outro lado, se alguma coisa acontecesse a esta única fonte de informação, ela seria perdida para sempre.

Então, como podemos superar nossos problemas de confiança e alcançar a descentralização?

Pele em jogo

Primeiro, precisamos reconhecer que o verdadeiro problema está no desalinhamento de riscos e incentivos entre os participantes. Nossos sistemas atuais, incluindo a democracia, permitem que pessoas sem envolvimento, tomem decisões que beneficiam e prejudicam os outros. Assim, quando ocorreu a crise bancária de 2008, não foi porque a elite bancária foi intencionalmente cruel; ao contrário, o sistema permitiu que sua insensibilidade e ganância afetassem a economia global. No entanto, se seus erros tivessem produzido consequências negativas para seu próprio dinheiro, talvez eles tivessem feito sua devida diligência antes de entrar em um mercado imobiliário duvidoso. "*Skin in the Game*" significa responsabilidade por suas próprias ações e suas consequências: se você não tratar bem e perder seu dinheiro, você terá que pagar por essa perda. Além disso, você não deve ter a oportunidade de brincar e eliminar os fundos de outras pessoas por meio de más tomadas de decisão, mas ainda obter apoio de resgates do governo. Isso é injusto de várias maneiras.

Então, como conseguimos alguma aparência de "*skin in the game*" em escala? Entre na *blockchain* e em todas as tecnologias adjacentes.

O que é uma *blockchain*?

Uma *blockchain* é um banco de dados (uma coleção organizada de dados). Mas é diferente das bases de dados a que estamos acostumados com aplicações *Web2* (Facebook, Instagram e Google, para citar algumas), a maioria das quais são bases de dados autorizadas, centralizadas e controladas por uma única autoridade. Os dados na

blockchain têm algumas propriedades únicas que os tornam diferentes daqueles bancos de dados tradicionais:

1. São hospedados por uma rede de computadores pública, descentralizada e *peer-to-peer*.
2. É protegido por criptografia e por um protocolo de consenso que foi projetado para dificultar a tomada de controle, mas facilitar a sincronização dos computadores.
3. É imutável, o que significa que não se pode atualizar ou apagar registros de dados existentes sem obter a aprovação majoritária dos nós da rede. Assim, embora seja possível apagar e manipular dados em uma *blockchain*, isso só é possível quando a maioria concorda em fazê-lo.

Com estas propriedades únicas, o banco de dados da *blockchain* torna-se super útil para aplicações que exigem consenso social para serem válidas, como governança e dinheiro.

Outra maneira de pensar em uma *blockchain* é como uma rede de nós (computadores, servidores, etc.) que trabalham em conjunto sem nenhuma autoridade central de registro e verificação de dados. Esses dados podem ser qualquer coisa, transações, saldos de contas e estados de rede armazenados em um livro razão que cada membro da rede tem livre acesso.

Para construir esta base de dados descentralizada chamada *blockchain*, diferentes partes interessadas pseudomonas devem trabalhar em conjunto. Mas como conseguir que as pessoas que não se conhecem confiem umas nas outras sem a supervisão de uma autoridade central? Bem, você tira a confiança da equação. Em outras palavras, você automatiza a confiança de tal forma que os participantes da rede não precisam confiar uns nos outros, mas sim no protocolo.

O que é um protocolo?

Um protocolo é simplesmente um conjunto de instruções a partir do qual um *software* de computador opera. Pense em *HTTP*, ou *TCP/UDP e IP*. Pense nos Dez Mandamentos ou no código *Hammurabi*.

Um protocolo estabelece as regras de engajamento para todos os participantes de uma rede, de tal forma que os novos participantes podem escolher livremente fazer parte da rede ou sair dela. Mais importante ainda, o protocolo não pode ser alterado por nenhum participante ou grupo de participantes. Quaisquer atualizações só podem ser realizadas quando a maioria dos participantes da rede concordar com essa mudança. Observe que isso é distinto de um país ou empresa onde as mudanças são feitas de cima para baixo.

Assim, as *blockchains* dão a cada participante da rede a liberdade de escolha para entrar ou sair da rede e também a responsabilidade de administrá-la. Propriedade coletiva e liderança é o nome do jogo. No entanto, nem todas as *blockchains* seguem este espírito.

É possível confiar em um protocolo porque suas regras são claras desde o início. No caso do Bitcoin, por exemplo, o protocolo afirma que um bloco (falaremos mais sobre isso daqui a pouco) só será produzido quando um quebra cabeça criptográfico tiver sido resolvido e verificado por uma maioria de nós (computadores) na rede. Em termos mais simples, nenhuma nova transação será adicionada ao livro razão a menos que a maioria dos nós concorde que as transações são válidas. Na criação deste novo bloco, um novo BTC será criado (cunhado) como recompensa. Em resumo, esse é o protocolo Bitcoin.

Então, como funcionam as *blockchains*?

As *blockchains* são constantemente associadas a um livro razão global, e é verdade. Mas dizer que a *blockchain* é um livro razão pode às vezes ser enganoso em um sentido imaginativo porque não há uma tabela semelhante a um livro razão para qualquer pessoa não técnica possa olhar. O termo "livro razão" é usado apenas para estabelecer uma semelhança entre um processo de computador e um processo humano. Assim, a *blockchain* é um registro porque armazena informações, não porque é um verdadeiro livro razão para escrituração contábil. No entanto, é útil manter esta comparação porque ela descreve perfeitamente o que uma *blockchain* faz. De agora em diante, vou me concentrar em propor uma melhor explicação de como este registro é construído.

Para entender uma *blockchain*, precisamos quebrar a palavra *blockchain* em suas possíveis constituintes.

Blockchain = blocos em uma corrente

OU

Blockchain = blocos + corrente

Mas o que é um bloco?

Um bloco é uma coleção de informações verificadas empacotadas juntas e prontas para serem adicionadas ao livro razão global. Um bloco raramente é feito de uma única transação, mas consiste em muitas transações agrupadas. Para criar um bloco, as transações válidas que ocorreram na rede (ou seja, envio de *tokens*, mudança de nomes em um site de mídia social descentralizado, trocas de *tokens* ou publicação de um comentário) são compiladas e trancadas juntas usando criptografia. A criptografia é uma disciplina (assim como a biologia, a química, a física, etc.) que se concentra na criação de uma forte segurança, utilizando quebra cabeças difíceis de quebrar, baseados em matemática comprovada. O objetivo de selar os blocos usando criptografia é evitar futuras adulterações.

Você pode imaginar um bloco como um balde. Cada bloco começa como um balde vazio, depois os usuários finais fazem uso da rede, enchendo o balde com suas transações. Quando o balde está cheio, ele é selado e mantido afastado para referência futura. Agora, é importante perceber que a vedação do bloco só é possível quando muitas pessoas (nós

de rede) concordam que as transações no bloco são válidas. Assim como quando se confirma que ninguém tentou enviar *tokens* que não estão em posse ou outras ações fraudulentas. Uma vez selado, um bloco não pode ser aberto para alterar qualquer transação, mas pode ser usado como referência para verificar os registros de dados.

Então, quando a corrente entra?

Bem, é certo que haverá múltiplos blocos, certo? Já que cada bloco só pode conter um número finito de transações. Assim, o encadeamento dos blocos torna-se necessário para decifrar e rastrear a sequência de transações, ou seja, quais blocos vêm primeiro. O processo de encadeamento não é tão diferente da criação do bloco em si. Eu apenas dividi artificialmente minha explicação para que você pudesse entender melhor o processo. Na realidade, cada novo bloco faz crescer a cadeia e, no caso de uma *blockchain Proof-of-Work*, a torna mais segura.

Mas, num nível mais profundo, como uma *blockchain* atinge esse nível de segurança descentralizada? Diferentes *blockchains* abordam esse tema de forma particular. Mas, apesar de suas diferenças, há realmente duas questões principais a serem consideradas na análise das *blockchains*.

Para que uma *blockchain* faça o que faz, ela precisa de muitos computadores “conversando” uns com os outros constantemente. Isto é chamado de *networking*, ou se preferir o termo mais humano, "fofocando". É assim que os dados são transmitidos através da rede. Em resumo, os dados são copiados de um computador para outro até que todos os computadores da rede tenham esses dados. Sem rede, não haveria *blockchains* como as conhecemos.

O segundo componente principal de uma *blockchain* é seu mecanismo de consenso, conhecido como os diferentes participantes da rede (nós, computadores, servidores) chegam a uma conclusão sobre quais dados são válidos e quais são falsos. Um mecanismo de consenso tem dois aspectos principais:

- Consenso - o processo de cópia e verificação de dados (blocos) de um nó para outro.
- Finalidade - o processo de adicionar novos blocos à cadeia. A diferença entre os dois será muito mais clara a seguir.

Naturalmente, cada *blockchain* tem seu mecanismo único de consenso, a menos que uma nova *blockchain* tenha sido criada usando o código (protocolo) de outra *blockchain*. Entretanto, todos os diferentes sistemas de consenso podem ser classificados em três categorias principais.

***Proof of Work (PoW)* - Prova de Trabalho**

Proof-of-Work é um algoritmo que foi criado para evitar *spam* de *e-mail*, essencialmente dificultando que os computadores sobrecarreguem maliciosamente os servidores de

e-mail. Para conseguir isso, o servidor de *e-mail* daria ao *IP* de envio um pequeno quebra cabeça para resolver, que exigiria algum esforço computacional arbitrário. Quando feito, o computador apresentaria a solução, que era a prova do trabalho que ele fazia, junto com o corpo do *e-mail*. Este processo foi adotado pelo cliente do Bitcoin e foi redirecionado para ser usado como um mecanismo de consenso.

Com o *PoW*, os computadores chegam a um consenso somente quando o trabalho, neste caso, solução de um quebra cabeças criptográfico, for feito. Quem fornece uma solução para o quebra cabeça criptográfico primeiro se torna o produtor do bloco e é recompensado por ele. Este método de consenso tem sido criticado ultimamente por suas operações de uso intensivo de energia. Em tal rede, a segurança de um sistema está de alguma forma ligada ao quão difícil é o quebra cabeça criptográfico, exigindo assim mais horas extras de energia.

Proof of Stake (*PoS*) - Prova de Participação

Este método de consenso foi inventado para superar as deficiências da *PoW* em termos de consumo de energia. Ele troca o trabalho do computador e os quebra-cabeças criptográficos por interesses econômicos, de modo que a segurança de um sistema esteja vinculada a quantos *tokens* estão em *staking* (apostados) na rede. Foi daí que surgiu toda a ideia de *staking* (abordaremos mais sobre isso depois). A lógica é simples, se um sistema for apoiado por um grande poder econômico, então será quase impossível sequestrar esse sistema porque qualquer um que queira fazer isso terá um custo ainda maior... Por exemplo, uma *blockchain PoS* que tem apenas 2 milhões de dólares em jogo é muito mais fácil de sequestrar do que uma rede com 1 bilhão de dólares em *stake*.

Consenso Híbrido

A maioria das *blockchains* modernas utilizam um consenso híbrido que combina o *Proof of Work* e o *Proof of Stake*, levando o melhor de dois mundos para criar uma rede mais segura e eficiente em termos energéticos. Com os sistemas de consenso híbrido, a ligeira diferença entre consenso e finalidade torna-se algo óbvio.

Antes que um bloco seja adicionado à cadeia, ele precisa ser verificado por muitos mineradores (ou validadores). Este processo de verificação contínua, que inclui a cópia dos dados de um nó para outro, é chamado de consenso. Quando verificações suficientes tiverem sido feitas, como especificado pelas regras do protocolo, então o bloco mais "apoiado" é finalizado, ou seja, adicionado à *blockchain*. Ao separar os dois processos, os desenvolvedores podem otimizar a *blockchain* em termos de velocidade, segurança e escalabilidade.

Quem são os participantes das *blockchains*?

Nós completos (*Full Nodes*): Estas são os responsáveis pela segurança da rede. Você pode pensar neles como o "pessoal de segurança". Dependendo da *blockchain*, eles

podem ser chamados de diferentes nomes - mineradores (Bitcoin e Ethereum), validadores (Polkadot, Cosmos), e muito mais. Independentemente de seu nome, seu propósito é o mesmo: proteger a rede. Fazem isso registrando e verificando as transações de forma descentralizada.

Construtores (*Builders)* - aplicativos descentralizados e *blockchains*: Os construtores são similares aos fundadores no mundo atual da *Web 2.0*. São em sua maioria programadores que criam aplicações descentralizadas ou *blockchains* mais novas para trabalhar.

Nós Leves (*Light Nodes)* - Usuários Final, Carteiras e Clientes: Muitas pessoas nesta categoria nunca precisarão saber como as *blockchains* funcionam para poder usá-las. Na verdade, o objetivo da inovação atual das *blockchains* é fazer com que o usuário final interaja com as *blockchains* sem nunca se dar conta disso. Estas são pessoas que utilizam os *dApps* e serviços criados pelos construtores.

Se o conceito de *blockchains* ainda parece ser um conceito, então não se preocupe. Vamos agora explorar a história das *blockchains*, e esperamos que você obtenha mais contexto e, assim, melhor compreensão.

A Evolução das *blockchains*

Primeiro veio o Bitcoin

No sistema antigo, se você precisasse enviar dinheiro para um amigo, você teria que ir ao banco e pedir aos funcionários que enviassem dinheiro em seu nome. Se você vivesse em zonas rurais, a natureza de seus obstáculos não seria apenas financeira, mas também física.

Isso significava algumas coisas importantes: você não tinha controle total sobre seu dinheiro e o banco era livre para emprestar seu dinheiro e ganhar juros sobre ele sem nenhuma recompensa para você. Além disso, eles poderiam perder esse dinheiro através de especulações imprudentes e nunca seriam responsáveis por isso. Loucura, certo? Este foi o caso por um longo tempo até que o Bitcoin mudou o jogo de maneira inesperada.

Com o Bitcoin, pela primeira vez, as pessoas poderiam enviar valores digitalmente para qualquer pessoa em qualquer parte do mundo, sem que nenhum intermediário lhes pedisse documentos ou taxas elevadas.

Com o Bitcoin, tudo o que você tinha que pagar era uma pequena taxa de transação ao protocolo para fazer sua transferência. Se a transferência falhasse, você receberia um reembolso. Não haveria mais necessidade de intermediários. Esta rede poderia crescer e substituir o sistema bancário tradicional.

Há três maneiras de pensar em Bitcoin:

1. Um sistema/protocolo para transferência de valores digital.

2. Ouro digital.
3. Investimento.

Desde que o Bitcoin se tornou um dos ativos de maior desempenho dos últimos tempos, a maioria das pessoas prefere vê-lo como um investimento em vez de "dinheiro digital", como era originalmente pretendido.

Em seguida veio o Ethereum

Em uma tentativa de expandir as funcionalidades da rede ao longo dos anos, a comunidade Bitcoin tentou criar "moedas coloridas", que eram *tokens* construídos em torno, ou como uma cópia do Bitcoin para representar diferentes ativos e ideias. Entretanto, as plataformas não funcionavam como pretendido e não conseguiam superar as limitações do código Bitcoin.

Vitalik Buterin estudou o Bitcoin por alguns anos e pensou: "E se tornássemos essa tecnologia mais generalizada?

Estimulado por esta ideia, Vitalik escreveu o *whitepaper* do Ethereum em 2014, estabelecendo a estrutura para uma *blockchain* de uso geral sobre a qual os desenvolvedores poderiam construir e projetar *tokens* personalizados. Para pagar pelo cálculo que seria necessário para executar seu código, os desenvolvedores usariam um *token* nativo chamado Ether (ETH).

Essencialmente, o Ethereum foi conceituado como um supercomputador global rodando em uma *blockchain* como seu banco de dados. Tomando a estrutura básica de uma *blockchain*, o Ethereum construiu uma plataforma que permitia maior flexibilidade de casos de uso. Pense no Ethereum como uma plataforma de *internet* aberta que permite a criação de qualquer tipo de *website/app*, enquanto Bitcoin é uma plataforma de *internet* aberta inteiramente preenchida com um único *website/app.*

Assim, a partir da ascensão do Ethereum surgiu um novo componente do ecossistema da *blockchain*: aplicações descentralizadas (*dApps*).

Antes de passarmos às cadeias cruzadas (*cross chains*), é crucial que exploremos um pouco os contratos inteligentes.

Um pouco sobre contratos inteligentes

Embora tenham se tornado populares através do Ethereum, os contratos inteligentes foram inventados em 1994 por Nick Szabo. Assim como as *blockchains* dão aos vários participantes da rede as ferramentas necessárias para trabalharem juntos sem a necessidade de confiar uns nos outros, os contratos inteligentes fornecem um mecanismo para facilitar a confiança entre os diferentes atores econômicos. Como isso é diferente de uma *blockchain*? Uma *blockchain* é um conjunto de regras sobre como uma rede irá

operar, enquanto um contrato inteligente é um conjunto de regras sobre como as transações serão executadas.

Para entender melhor os contratos inteligentes, vamos analisar as apólices de seguro. Em uma configuração típica de contrato de seguro, o segurado precisa fornecer prova à seguradora de que seu sinistro é válido, o que pode criar atritos. Digamos que você fez um seguro de carro e seu carro teve sinistro sem ser culpa sua. A companhia de seguros pode pagar o seguro conforme acordado ou atrasar sob o pretexto de investigar o assunto. Às vezes, estas investigações levam meses, durante os quais você tem que recorrer ao transporte público. Isto não quer dizer que as investigações não sejam necessárias; mas para ir ao ponto dos contratos inteligentes, estamos assumindo que a companhia de seguros está agindo de má fé. Com um contrato inteligente, este não será o caso.

Um contrato inteligente é um programa auto executável que funciona sempre que um conjunto de parâmetros pré-definidos é cumprido. Assim, em nosso exemplo de seguro, eis como as coisas poderiam proceder sob um contrato inteligente baseado em um acordo. Primeiro, quando seu carro é sinistrado, um sensor no carro envia esta informação para o contrato inteligente. Assim que o contrato inteligente confirmar os dados, talvez mapeando os dados para relatórios de notícias da área, ele pagará automaticamente sua reivindicação de seguro sem esperar por qualquer outra permissão da companhia de seguros.

Vamos aplicar esse processo às operações financeiras. É possível executar sozinho uma plataforma descentralizada de empréstimos por meio do poder dos contratos inteligentes, porque os participantes podem confiar no contrato sem confiar em outros participantes. Assim, um provedor de liquidez, alguém que fornece dinheiro para outros tomarem emprestado, é encorajado a depositar seus *tokens* para outros usuários emprestarem porque ele tem a garantia de que sempre que ele optar por retirar sua liquidez (*tokens*), o contrato inteligente o liberará junto com todas as recompensas que lhe são devidas. Da mesma forma, o mutuário pode confiar que o contrato inteligente não alterará os termos da transação (taxas de juros e/ou multas) e que sua garantia será devolvida a ele assim que pagar o empréstimo.

Agora há uma grande ressalva. Um contrato inteligente é tão seguro quanto o código que o cria. Muitos *hacks* que levaram à perda de fundos foram realizados no espaço da *Web3.0* devido a contratos inteligentes defeituosos. Assim, antes de interagir com um contrato inteligente, é aconselhável que você revise o código, se tiver conhecimento técnico, ou verifique se o código do contrato inteligente foi auditado.

Mais uma coisa a ter em mente é que um contrato inteligente pode ser usado em uma variedade de indústrias e para uma variedade de propósitos, desde que o objetivo final seja facilitar a confiança entre diferentes atores econômicos por meio de execução ininterrupta. Por exemplo, um contrato inteligente entre um fornecedor e um varejista pagaria fundos ao fornecedor somente quando confirmasse que as mercadorias foram fornecidas ao armazém/loja do varejista

No longo prazo, o desenvolvimento de contratos inteligentes dependerá cada vez mais de códigos bem escritos (desenvolvedores), economia bem incentivada (economistas) e funcionalidades que cumprem a lei (advogados). Portanto, para desenvolver contratos inteligentes e torná-los mais inteligentes, precisaremos adotar uma abordagem multidisciplinar.

Com este assunto examinado, podemos agora voltar nossas atenções para as cadeias cruzadas.

Ascensão das cadeia cruzadas (*cross chain*)

Após o sucesso esmagador do Ethereum, onde o sucesso significa a adoção por mais pessoas, foram criadas múltiplas *blockchains* de primeira camada (l*ayer 1*). Mas o que significa ser um protocolo de primeira camada? Até agora, não era importante deixar esta distinção clara, mas como estamos nos aproximando mais da apresentação de Polkadot, é importante entender o que as camadas representam.

Uma *blockchain* de primeira camada é semelhante a um país com fronteiras seladas. Dentro desse país, as informações podem fluir entre todos os participantes sem a necessidade de confiança. Por quê? Porque ela já opera com uma constituição que não está aberta a interpretações errôneas, mas executada instantaneamente. Com a introdução de contratos inteligentes pelo Ethereum, uma primeira camada (país) pode ter múltiplos sub-protocolos (estados), cada um se comunicando entre si sem problemas. Mas devido a suas fronteiras seladas, esta primeira camada não pode ter conexão direta com o mundo exterior.

Um equívoco comum entre alguns dos primeiros usuários da *blockchain* é que uma única primeira camada será tudo o que é necessário para que a indústria de *blockchain* cumpra sua missão. Esta visão da indústria é frequentemente perpetuada por aqueles que têm uma abordagem maximalista para a adoção da *blockchain*. Portanto, não será raro encontrar pessoas que são da opinião de que qualquer coisa além do Bitcoin é um esquema que não é verdadeiramente descentralizado. Outros cantarão os louvores do Ethereum, afirmando que ele é muito melhor que o Bitcoin, e que outras *blockchains* são redundantes. A maioria dessas pessoas ou estão mal informadas ou estão apenas preocupadas em ganhar dinheiro com os *tokens* que possuem.

A verdade é que a indústria de *blockchains* está preparada para um futuro de múltiplas cadeias, e cada nova *blockchain* trará algo novo à mesa que pode ser alavancado pelas *blockchains* existentes. Assim, se houver uma *blockchain* focada na descentralização das finanças e outra focada na descentralização da identidade, elas serão mais eficazes ao trabalharem juntas do que uma *blockchain* de uso geral. Explicando este conceito em detalhes exigiria mergulhar em explicações técnicas, por isso, por enquanto, vou ignorá-lo. A questão é que não existe uma *blockchain* para governar todas elas, o que seria o mesmo que dizer que existe uma empresa on-line que governa a *internet*.

Se a realidade é um universo de múltiplas cadeias, e os países da primeira camada são países isolados, como conectar esses países isolados? Há muitas soluções possíveis para este problema.

A primeira, perseguida pela Cosmos, é dar a cada primeira camada a mesma constituição de rede, para que a troca de informações entre cadeias seja facilitada através de uma ponte especializada. Neste contexto, uma ponte significa literalmente uma porta de entrada para outro país. Esta abordagem resolve definitivamente o problema de conectar cadeias, mas não é a configuração mais adequada, mesmo quando comparada ao Ethereum.

No Ethereum, contratos inteligentes podem interagir uns com os outros de duas maneiras distintas:

1. Enviar e receber *tokens* - Contratos inteligentes podem trocar *tokens* sem qualquer verificação formal.
2. Dar instruções - Um contrato inteligente pode pedir a outro contrato inteligente para realizar uma transação. Esta é a verdadeira magia da compossibilidade, onde diferentes contratos inteligentes podem ser usados em uma única transação ou aplicação e se comunicar sem intervenção humana.

Dentro do protocolo de comunicação entre cadeias da Cosmos, as únicas informações que podem ser transferidas são os *tokens*. Assim, as *blockchains* não podem instruir um ao outro para tomar certas ações. Como tal, pode-se pensar neste nível de comunicação como algo primitivo (baixo nível de compossibilidade). Para atingir níveis mais altos de compossibilidade, semelhante ao que os contratos inteligentes desfrutam, uma camada mais baixa é necessária. Aí entra Polkadot.

Polkadot é um protocolo de camada zero (*layer 0*) que procura conectar várias primeiras camadas de *blockchain* sem quebrar a compossibilidade de alto nível. Nesta configuração, *blockchains* são capazes de se conectar umas com as outras para enviar *tokens* e mudar o estado um do outro.

Polkadot respeita as funções únicas de transição de estado da primeira camada e não exige que elas sigam a função de mudança de estado da *relay chain* (é o coração do protocolo Polkadot. Ela é responsável pela segurança compartilhada da rede, pelo consenso e interoperabilidade entre as *blockchains*). Ele apenas exige prova de validade da mudança de estado que uma primeira camada pode estar implementando. Dito de forma diferente, Polkadot a camada zero (planeta) leva em conta as leis de qualquer primeira camada (país) que se conecte a ela. Tudo o que exige é a prova de que estas leis ou mudanças são válidas. Esta é a configuração que dá às *parachains* a liberdade de desenvolver seus próprios mecanismos de consenso e de finalidade.

O que significa realmente "mudança de estado"? Vamos dar uma olhada em um exemplo. Uma *blockchain* de primeira camada focada na descentralização financeira pode mudar o

estado de outra primeira camada focada na descentralização da identidade, solicitando para o usuário informações armazenadas na cadeia de identidade. O estado é alterado porque a cadeia de identidade precisa realizar uma nova transação para atender a esta solicitação. Embora nenhum *token* tenha sido trocado, maior valor foi fornecido porque as informações fornecidas pela cadeia de identidade podem potencialmente ser usadas pela cadeia financeira para fazer pagamentos ao usuário. Este é apenas um exemplo entre muitos que estão no centro da perturbação trazida pelas tecnologias de *blockchain*.

Mas antes de abordar a natureza disruptiva das *blockchain*, vamos passar por mais uma camada em nosso mundo multi-cadeia: a segunda camada (*layer 2*). As *blockchains* de segunda camada foram criadas para escalar as *blockchain* de primeira camada, ou seja, aumentar a velocidade ou expandir a capacidade das referidas *blockchains*. O Ethereum, por exemplo, tem pelo menos três protocolos de segunda camada trabalhando para ajudá-lo a escalar - Polygon, Arbitrum e Optimism. O mecanismo através do qual isto é possível não é exatamente relevante para seu entendimento primário das *blockchains*. O importante é saber que as de segunda camada operam na primeira camada.

Uma pequena divagação sobre tokens

Por que os *tokens* são necessários para as *blockchain*, e quantos tipos existem?

Para começar, nem todos os projetos de *blockchain* requerem *tokens*. A maioria das *blockchains* privadas de empresas e corporações não possuem *tokens* e funcionam muito bem. Dito isto, os *tokens* são uma necessidade para as blockchains públicas porque são usados para iniciar transações e pagar taxas de transação *on-chain* (operações/aplicações que acontecem dentro da rede de uma *blockchain*); caso contrário, a cadeia seria interrompida por transações de *spam*. Por estas razões, você paga BTC para usar a *blockchain* Bitcoin, ETH para usar Ethereum e DOT para usar a rede Polkadot. Para redes *Proof of stake*, os *tokens* também são necessários para fins de segurança - mais sobre isso no capítulo 3.

É importante observar que nem todos os *tokens* são *tokens* de utilidade (*tokens* que são usados para transações relacionadas à rede). Alguns *tokens* são de governança que apenas dão a um usuário a capacidade de votar em decisões que terão impacto no futuro do projeto. A maioria dos *dApps* hospedados na primeira camada emitiram *tokens* de governança que não têm utilidade, porém alguns *tokens* de governança podem ser usados para obter dividendos, embora os mecanismos exatos variem de projeto para projeto.

Todos os *tokens* mencionados acima são *tokens* fungíveis. Um grupo de itens é fungível quando cada item deste grupo é idêntico ao outro, de tal forma que nenhum membro possui qualquer individualidade. Isto significa que eles podem sempre ser trocados uns pelos outros sem qualquer conflito. Mas nem todos os *tokens* da tecnologia de *blockchain* são fungíveis. Alguns não são fungíveis.

Se fungibilidade é a qualidade de ser intercambiável com algo de propriedades similares, então a não fungibilidade é a capacidade de ter uma identidade, de ser único. Assim, um *token* não fungível (*NFT*) é um *token* que é único, desde que um único item/objeto tenha sido cunhado (criado) quando foi adicionado à *blockchain*. Portanto, quando você ouve falar de coleções *NFT* hoje, isso geralmente significa que elas são um grupo de *tokens*/peças únicas.

Isto resolvido, vamos nos concentrar na natureza disruptiva da tecnologia da *blockchain*.

Blockchain e *Web* 3.0: A disrupção do cenário da *Web* 2.0

Como a maioria das tecnologias que vieram antes delas, as *blockchains* querem desafiar o *status quo*. Ao contrário das tecnologias anteriores que se desorganizavam de forma dissimulada, as *blockchains* são deliberadas e abertamente revolucionárias, buscando mudar nossa percepção de confiança e automatizá-la. Pergunte-se: qual indústria centrada no ser humano não requer confiança? Em todos os lugares onde há um intermediário, há uma questão de confiança. Assim, muitos campos estão maduros para a ruptura através do uso de *blockchains*. Abaixo estão algumas de nossas indústrias que estão atualmente sendo remodeladas por *blockchains*:

- Finanças
- Governança
- Propriedade
- Identidade
- Dados
- Cadeia de fornecimento de dados

No centro desta ruptura está uma diferença de ética entre o mundo digital existente e o novo mundo digital, entre a *Web 2.0* e a *Web 3.0.* Primeiro, havia a *Web 1.0,* a fase da *Internet* durante a qual os usuários finais **apenas podiam ler dados**. Isto era dominado por *e-mails*, boletins informativos, *sites* estáticos, etc.

Depois veio a *Web 2.0*, a fase durante a qual os usuários finais podiam **ler e escrever dados**. A *Web 2.0* permitiu muita coisa boa no mundo, ampliando nossas redes sociais e permitindo que nos tornássemos mais conectados. No entanto, muita exploração não intencional foi permitida até se tornar um monstro que está produzindo mais desigualdade e abuso dos usuários finais. Ele é marcado por vazamentos de dados, censura de usuários e exploração de dados de usuários, para citar alguns.

Web 3.0 nasceu das deficiências da *Web 2.0* e trouxe uma fase onde os usuários finais **podem ler, escrever e possuir dados**. Com a propriedade digital vem todo um novo paradigma que levará algumas décadas para se definir completamente. Idealmente, a experiência do usuário da *Web 2.0* e da *Web 3.0* permanecerá muito semelhante para o usuário final, enquanto os construtores e fundadores do projeto terão que trabalhar para alcançar as novas tendências. Para o usuário final, o verdadeiro desafio é compreender os

ideais que sustentam a revolução, bem como as vantagens e desvantagens da auto custódia dos ativos digitais. Mais sobre isto mais adiante.

O que é importante notar é a escala de ruptura que é possível. Em teoria, qualquer empresa *Web 2.0* que você possa pensar pode ser reorganizada a partir de uma perspectiva *Web 3.0.* Lembre-se que as principais diferenças entre a *Web 2.0* e a *Web 3.0* são a propriedade real e a liberdade. Pergunte-se: existe alguma indústria que não possa ser remodelada para promover mais justiça e inclusão? Seria quase impossível encontrar uma que seja otimizada como está, e esta é a razão pela qual a interrupção da *blockchain* continuará acelerando. Por enquanto, este movimento de avanço é limitado no escopo porque cada *blockchain* é uma ilha.

Felizmente, Polkadot oferece um caminho para a ruptura máxima, e o resto deste livro é dedicado a explicar o que é e como planeja alcançar seu objetivo final.

Capítulo 1

Por dentro de Polkadot

Polkadot, à primeira vista, pode ser difícil de entender. Algumas pessoas imediatamente desistem pelo conceito desconhecido de uma *blockchain* sem contratos inteligentes conectando outras *blockchains*. Os poucos que vão além da confusão inicial têm de se contentar com outras camadas de complexidade: governança on-chain, atualizações forkless, *parachains*, *crowdloans*, leilões, mensagens em cadeia cruzada e muito mais. Alguns poucos determinados conseguem superar este ponto, auxiliados por vídeos de Gavin Wood explicando o projeto do ecossistema no Youtube, o *whitepaper*, o Wiki Polkadot, e outros recursos úteis. O que todos eles descobrem no fim desta expedição intelectual é que Polkadot é muito mais do que uma simples *blockchain*.

Toda rede de *blockchain* busca intrinsecamente segurança, mas isto não é uma tarefa fácil. Uma vez que segurança se refere tanto à segurança da rede quanto à segurança econômica, espera-se que:

- A *blockchain* seja fortemente descentralizada, com poucos ou nenhum vetor de ataque de alto valor (como computadores centrais que armazenam informação sensível). Isso se traduz em obter muitos mineradores ou validadores para verificar as transações na rede. Se são muito poucos, eles podem conspirar e prejudicar a rede.
- A *blockchain* tem uma capitalização de mercado suficientemente grande para tornar o ataque à rede economicamente difícil. Para exemplo, se uma *blockchain* tem uma capitalização de mercado (o preço por *token* multiplicado pelo número total de *tokens* em circulação) de US$ 15 milhões, qualquer pessoa que possa se dar ao luxo de fazer *stake* de US$ 15 milhões poderia potencialmente assumir o controle da rede. Além disso, se uma pessoa possuir um lote de *tokens*, poderá quebrar o preço do *token* vendendo todas de uma só vez e depois comprá-las de volta quando elas forem baratas. Isto manipula a capitalização do mercado da rede. Em uma rede *PoS* onde o valor total de *tokens* em *stake* na rede é igual ao custo do ataque a essa rede, tal manipulação pode ser difícil. Isto porque, embora você

possa ter US$ 15 milhões, muito provavelmente será muito difícil encontrar pessoas suficientes para vender-lhe US$ 15 milhões em *tokens*.

Em resumo, o lançamento de uma nova *blockchain* não é fácil. Como podemos administrar uma variedade de *blockchains* e ainda ter o mesmo nível de segurança em todas elas? Esse é o primeiro problema que Polkadot pretende resolver. Criando um ambiente heterogêneo de múltiplas cadeias que outras *blockchains* podem ser conectadas e, portanto, se beneficiarem de sua segurança já estabelecida. Em resumo, Polkadot cria um sistema solar onde todos os planetas (*blockchains*) se beneficiam da energia (segurança) do sol (*relay chain* de Polkadot).

O segundo problema diz respeito à interoperabilidade. Como expliquei no capítulo 0.5, o *DeFi* (Finanças Descentralizadas) cresceu exponencialmente (US$ 50 bilhões em valor total trancado em menos de 15 meses) porque o Ethereum possibilitou interações perfeitas entre contratos inteligentes, levando a novos e fascinantes casos de uso e a um "ciclo de mercado de touro". Pense assim: cada contrato inteligente é uma casa que pode ser acessada por todos os servidores de outras casas no país (*blockchain*). Assim, se um padeiro precisa de manteiga, seu funcionário pode correr para a casa do cozinheiro e conseguir a manteiga sem pedir permissão. No mundo real, isto seria chamado de roubo; mas como a própria casa é um dispositivo inteligente e conectado, ela sabe que a manteiga está sendo emprestada para o funcionário do padeiro e que eventualmente será devolvida. Esta é uma ilustração excessivamente simplista do que acontece, mas ela explica os processos básicos.

As coisas e as pessoas trabalham melhor em conjunto, e as redes de *blockchain* não são exceção a essa regra. Se você pensar em cada *blockchain* como um provedor de serviços de *Internet*, então torna-se mais fácil entender por que uma *blockchain* pode querer lidar com identidade, outra com conteúdo e outras com bancos, jogos, privacidade, etc. As possibilidades se tornam infinitas, como costumava ser com a *Web 1.0.* É irresponsável, dado o potencial das *blockchains*, não aproveitar a oportunidade de criar interações mais ricas entre diferentes *blockchain* especializadas, e é aqui que entra Polkadot. Assim como o TCP/IP conectou diferentes nós para criar a *Internet*, Polkadot está conectando redes de *blockchain*, tornando-se essencialmente uma rede de redes de *blockchains*.

Então, o que é Polkadot?

Em sua essência, Polkadot é uma *blockchain* de camada zero (*layer 0*) que conecta outras *blockchains*. O objetivo de Polkadot é otimizar a **escalabilidade**, a **interoperabilidade** e a **segurança compartilhada** para todas as suas redes conectadas.

Consideramos cada recurso para explicar quais são os principais problemas e como Polkadot os resolve por *design*.

Segurança Compartilhada

Para resolver a questão de múltiplas cadeias isoladas e segurança dividida, Polkadot fornece uma estrutura onde várias cadeias podem compartilhar operações de segurança. Em vez de depender de cada *blockchain* de primeira camada para fornecer seu conjunto de validadores para proteger sua rede e um *token* com uma capitalização de mercado suficientemente grande, estas cadeias podem alavancar a segurança de Polkadot, o protocolo de camada zero. Na prática, se Polkadot estiver com um valor de mercado de US$ 10 bilhões, cada nova *blockchain* de primeira camada implantada em Polkadot será economicamente garantida por esses mesmos US$ 10 bilhões. Além da segurança econômica, a cadeia também ganhará segurança de rede com o grande conjunto de validadores de Polkadot. Isso é inédito na tecnologia de *blockchain*, um feito nunca visto antes.

Interoperabilidade

Este é o ponto alto do protocolo de camada zero de Polkadot. Já vimos anteriormente o que os *dApps* podem fazer quando se comunicam livremente entre si, agora estamos falando sobre o que acontecerá quando diferentes *blockchains* se integrarem efetivamente em suas operações diárias. Pode ser difícil de imaginar neste momento, mas certamente se tornará mais fácil quando chegarmos ao capítulo 5 e *parachains*. Por enquanto, basta lembrar que uma grande parte do projeto de Polkadot é sobre garantir a interoperabilidade entre as *blockchains* heterogêneas de primeira camada.

Escalabilidade

As *blockchains* nunca serão capazes de trazer maior justiça e inclusão se não forem escaladas em um nível global. A solução de Polkadot para esta questão é usar "*sharding*" (fragmentação), o que permite que a rede realize diferentes transações em paralelo. Por exemplo, o Ethereum, como existe em 2021, é uma rede de fragmento único onde as transações são processadas uma após a outra e cada nó precisa armazenar dados de toda a *blockchain*. Em uma rede de um único fragmento, todas as transações, embora de natureza muito diferente, serão realizadas no mesmo fragmento. Considerando que, em uma rede *multi-sharded*, as transações serão executadas em paralelo, dentro de seus respectivos shards. Nesse caso, cada shard corresponde a uma *blockchain* diferente, de modo que as transações *DeFi* são realizadas no shard *DeFi*, enquanto as transações *NFT* são realizadas no shard *NFT*. Novamente, essa é uma descrição excessivamente simplista do que acontece, mas deve ajudá-lo a entender os processos de escalabilidade.

Em Polkadot, cada cadeia de primeira camada é capaz de personalizar sua rede para diferentes casos de uso, assim abordando o problema da escalabilidade em um contexto aberto com computação paralela eficiente (onde a rede está processando diferentes tipos de transações em diferentes nós). Desta forma, uma cadeia de primeira camada focada na descentralização da identidade não precisará do mesmo projeto de sistema que uma cadeia focada em finanças descentralizadas. Assim, a rede se torna mais escalável:

1. Garantir que cada rede (*parachain*) seja otimizada para seu caso de uso.
2. Executar diferentes transações em paralelo.

Por exemplo, digamos que você tenha 1.000 nós verificando a validade das transações em sua rede. Em um modelo de uma única seção, todos os 1.000 nós estarão processando as mesmas transações. Em um modelo de 4 nós, os nós serão divididos em quatro grupos de 250 cada um. Cada grupo de nós processaria então diferentes tipos de transações. O grupo A processaria transações da cadeia de identidade, enquanto o grupo B processaria transações da cadeia financeira, o grupo C da cadeia de governança, e o grupo D da cadeia de dados. Desta forma, ainda temos 1.000 computadores, mas estamos fazendo muito mais por causa de como optamos por organizá-los.

Capacidade de atualização sem bifurcação (*forkless*)

Eu menti. A interoperabilidade em cadeia é um ponto alto do projeto de Polkadot, mas não é o único.

Lembra-se do problema entre o Ethereum e o Ethereum *Classic*? Ou a "fratura" entre o Bitcoin e o Bitcoin *Cash*? Eles aconteceram porque a cadeia original/canônica precisava atualizar seus protocolos centrais através de um *hard fork*. Uma bifurcação, como o nome indica, oferece um caminho diferente para as partes interessadas em um ponto específico no tempo. As bifurcações podem parecer uma característica desejável em uma rede, mas considere por um momento um país que se divide toda vez que seus cidadãos têm uma grande discussão sobre o resultado de uma votação. Este país ficaria menor à medida que mais pessoas saíssem, perdendo um pedaço de seu capital humano original a cada vez. É claro que, dado que as *blockchains* são análogas aos Estados-nação digitais, as bifurcações não são muito ideais para o crescimento no longo prazo. Para a prosperidade a longo prazo da rede, é imperativo que a comunidade encontre uma maneira de resolver disputas e atualizar protocolos sem se colocar em risco. Assim, Polkadot permite atualizações sem bifurcação e explicaremos como isso é feito no capítulo 4.

Por enquanto, basta ter uma visão geral de algumas das principais características que tornam Polkadot especial, já que analisaremos o projeto técnico de Polkadot no próximo capítulo. Antes disso, vamos falar um pouco sobre o agente do caos do ecossistema de Polkadot.

Uma breve nota sobre Kusama: O agente do caos

Embora este livro fale exclusivamente de Polkadot sem nenhuma menção a Kusama, é importante entender que as duas *blockchains* estão profundamente conectadas, tanto em tecnologia quanto conceitualmente.

Kusama é frequentemente considerada como uma rede de teste ao vivo para Polkadot, mas não é este o caso. Kusama é uma cadeia independente e *relay chain* de pleno direito, com seus próprios cronogramas de leilões, candidatos a *parachains*, governança e comunidades. Kusama lidera os desenvolvimentos no ecossistema Polkadot: como tal,

todas as funcionalidades implantadas em Polkadot são, antes de tudo, implantadas em Kusama. Kusama é uma versão mais selvagem de Polkadot e existe principalmente para resguardar Polkadot de sofrer interrupções inesperadas e comportamentos da vida real.

E assim, as principais diferenças entre Polkadot e Kusama se resumem à velocidade de implementação e *tokenomics* (economia dos *tokens*), porque o sistema de governança de Kusama funciona quatro vezes mais rápido que o de Polkadot, e também porque o fornecimento gênese do KSM é cem vezes menor que o do DOT. Por esta razão, o slogan de Kusama, que a comunidade adotou rapidamente, é "Espere o Caos" porque não há como dizer o que acontecerá no mundo selvagem e experimental de Kusama.

Embora este livro não mencione explicitamente Kusama pelo nome, deve ser entendido que cada menção a Polkadot inclui Kusama por padrão. A decisão de concentrar o conteúdo deste livro em Polkadot foi principalmente para evitar sobrecarregar o leitor com demasiada informação, mas se você quiser se referir a ambos os ecossistemas Polkadot e Kusama em uma só palavra, o termo DotSama será suficiente.

Capítulo 2

A REDE

Polkadot é frequentemente criticada por ser complicada, e isso é na maioria das vezes verdade. Dito isso, esta complexidade é construída sobre uma simples arquitetura que consiste em apenas duas partes principais – *relay chain* e *parachains*. A *relay chain* é o centro de ligação de todas as *parachains*. Este pequeno capítulo se concentrará exclusivamente na *relay chain*. As *parachains* serão abordadas no capítulo 5.

Imagem: Relay chain de Polkadot

Relay Chain

Para visualizar o propósito da *relay chain*, imagine um tubo circular em que muitos outros tubos se conectem. Estes tubos de ligação podem ser de qualquer forma e fornecer qualquer funcionalidade, desde que usem as mesmas regras que o tubo principal

A principal função da *relay chain* é fornecer segurança compartilhada e interoperabilidade para todas as suas *parachains*. Mas para fazer isso, a relay chain precisa primeiro ser o mais segura possível. Quero dizer, como você pode emprestar suas forças de segurança se sua própria segurança estiver comprometida? Para entender como a *relay chain*

preserva sua própria integridade ao longo do tempo, precisamos considerar dois aspectos chave das redes de *blockchain*.

Uma *blockchain* pública é um ambiente procurado porque ninguém controla o fluxo de informações (seja verificação ou recuperação) que é trocado com ela. Isto significa que a maioria dos nós da rede deve concordar sobre a validade de um novo bloco antes que ele seja criado e conectado à *blockchain*. Mas como é que os nós chegam a um acordo sobre quais transações (dados) são válidas? Isto acontece através de um processo chamado consenso (*consensus*).

Os detalhes completos do mecanismo de consenso da *relay chain* seriam técnicos demais para este livro, então o que é oferecido aqui é uma explicação excessivamente simplificada. A implementação atual da *relay chain* de Polkadot utiliza um mecanismo híbrido de consenso, o que significa que ela combina *proof of stake* com *proof of work* para obter o melhor de ambos os mundos.

Como regra geral, existem dois processos para o consenso da *blockchain*, ou seja, a produção e a finalidade do bloco. A produção de blocos refere-se ao processo de criação de novos blocos, enquanto a finalidade se refere ao processo de verificação e selagem de blocos na cadeia. A *relay chain* de Polkadot, como todas as redes *blockchain* descentralizadas, tenta resolver alguns problemas através de seu consenso:

- Robustez diante da conspiração de maus atores, de tal forma que basta apenas alguns bons atores para preservar a integridade da cadeia. Isso significa que se houver apenas alguns nós honestos, menos de 50%, a integridade da cadeia ainda será preservada, apesar da adulteração por nós corruptos.
- Velocidade de inclusão e verificação da escalabilidade da transação.
- Resiliência da rede de tal forma que ela não caia com frequência ou de forma alguma.
- Maior grau de descentralização, de modo que nenhum grupo de participantes da rede tenha controle total sobre a rede.

Para garantir a implementação bem sucedida dessas soluções em toda a *relay chain*, ela utiliza BABE e GRANDPA. Uma explicação detalhada de ambos os protocolos não é necessária para nossa apresentação sobre Polkadot e foi relegada para o apêndice técnico.

Em seguida, consideramos como a *relay chain* ganha sua segurança dos validadores, nomeadores e coletores.

Capítulo 3

SEGURANÇA DA REDE

Tendo compreendido o projeto técnico que facilita a segurança tecnológica, agora podemos nos voltar para a segurança. Como Polkadot garante sua segurança econômica? Para responder a esta pergunta, vamos mergulhar no assunto *Stake* e nos vários papéis disponíveis dentro da rede.

A filosofia do *staking*

As redes descentralizadas conseguem a colaboração entre muitos indivíduos, utilizando o conceito de teoria dos jogos para projetar um sistema onde há papéis, responsabilidades e incentivos para alinhar as ações de todos os participantes da rede. Este é um dos principais motivos por que os *tokens* são necessários para muitos sistemas descentralizados - as recompensas são o mecanismo de incentivo final. Para o Bitcoin é o BTC e para o Ethereum é ETH. Assim, a força da segurança de uma *blockchain* não é determinada apenas pela qualidade de seu código. Isso é também definido pela qualidade de seu incentivo e *design* de *token* que, no centro, é a teoria dos jogos. Por exemplo, todos os mineradores do Bitcoin criam e verificam blocos para uma recompensa em BTC. Em um sistema de *proof of work* como o do Bitcoin, as funções de rede são poucas e limitadas aos mineradores. Isso é porque a rede precisa apenas de nós, Bitcoins e usuários.

Em um sistema *proof of stake*, além dos nós, a rede precisa de usuários que vão delegar *tokens* para proteger a rede. Lembre-se de que as *blockchains* de *proof of stake* dependem tanto da segurança tecnológica quanto da segurança econômica para que o impacto ambiental seja compensado pela economia. A segurança de uma *blockchain* de *PoW* é tão forte quanto o número de nós que a protegem, enquanto a segurança de uma *blockchain* de *PoS* depende do número de nós e do valor de sua participação, sendo a participação seu valor econômico. Assim, o processo de proteger a rede em uma *blockchain PoS* é chamado de *staking*. Existem duas vantagens principais do *PoS* sobre o *PoW*:

- *PoS* tem muito menos consumo de energia em comparação com *PoW*. Este é um ponto crucial porque nossas tecnologias estão tendo um impacto maior nas mudanças climáticas. Por exemplo, os dados registrados mostram que os sete anos mais quentes do período 1880-2020 ocorreram todos após 2014.
- *PoS* oferece maior envolvimento da comunidade na segurança da rede, alcançando assim uma maior descentralização. Isso ocorre porque o *PoW* transfere a responsabilidade da segurança da rede para pessoas tecnicamente experientes com os meios e as habilidades para executar um nó. Com o tempo, isso inevitavelmente resulta em níveis crescentes de centralização.

Há três tipos de participantes trabalhando na segurança da rede Polkadot, validadores, nomeadores e coletores.

Validadores

Os validadores em Polkadot são como os mineradores no Bitcoin. Eles executam nós que processam e verificam transações, criam blocos e armazenam o histórico da *blockchain*. Sem eles, não haveria rede. Os pontos-chave a serem observados são:

- Eles fornecem a infraestrutura física na qual a rede funciona.
- Eles têm que garantir que estejam sempre online quando precisam estar (particularmente quando são eles que criam um novo bloco).

O processo é tão simples quanto adquirir um computador potente e executar o código de Polkadot. Uma vez implantado um nó, a maioria das operações de rotina podem ser automatizadas, enquanto os validadores podem se concentrar na solução de problemas e na manutenção da conectividade. Por seus esforços, econômicos e físicos, os validadores são recompensados em *tokens* DOT. O número total de validadores na rede é um parâmetro que pode ser ajustado com base na demanda da rede, começando com alguns e agora atingindo 297 (a partir de janeiro de 2022). O objetivo é chegar a 1.000 validadores.

Podemos olhar para este número e nos perguntarmos se ele é suficiente para apoiar a descentralização, especialmente quando consideramos que Bitcoin tem mais de 20.000 mineradores e Ethereum 1.0 tem mais de 10.000 mineradores. Para entender por que 1.000 validadores é suficiente, precisamos ter em mente como funciona o consenso de Polkadot. Ao selecionar os validadores ao acaso através do módulo de produção de blocos BABE e mantendo as informações sobre validação de blocos separadas, Polkadot limita a possibilidade de conspiração entre os validadores. Este procedimento também é assegurado pela premissa de que todos os validadores devem competir de uma só vez para validar blocos individuais.

Quando se diz que Polkadot visa 1.000 validadores, isso não significa que só pode haver 1.000 pessoas qualificadas para se tornarem validadores. Em vez disso, significa que a produção e a verificação dos blocos serão tratadas por 1.000 validadores ao mesmo

tempo, enquanto todos os outros validadores atuarão como candidatos a validadores. No final, um número baixo de validadores é útil não apenas para reduzir nossa pegada de carbono, mas também para alcançar escalabilidade. Se houver 13.000 validadores e 2/3 dos validadores no conjunto ativo (aqueles que atualmente participam do consenso de rede) devem concordar, então cada transação precisará esperar cerca de 7.500 validadores antes de ser processada, o que inevitavelmente desaceleraria a rede.

O objetivo da descentralização não é ter o maior número possível de validadores, mas sim o maior número possível de participantes da rede. É tudo sobre propriedade, poder e autoridade. É por isso que o *PoS* é um sistema muito mais desejável, porque muitas pessoas não têm os meios nem as habilidades para executar nós. Se a segurança da rede for fornecida apenas por validadores ou mineradores, uma grande parte da comunidade ficará de fora. Com *PoS*, o usuário médio, que não sabe nada sobre computadores ou codificação pode desempenhar um papel central na segurança da rede e também ganhar recompensas; por outro lado, *blockchains* de *PoW* tendem a levar à centralização de propriedade, poder e autoridade em torno de técnicos e operadores de equipamentos de mineração. O principal objetivo de um sistema *PoS* é garantir que os mecanismos de participação em vigor promovam uma maior descentralização. Para entender como Polkadot atinge esse objetivo, exploraremos o papel dos nomeadores.

Nomeadores

Se você estiver lendo este livro, então é mais do que provável que você seja ou esteja procurando se tornar um nomeadores. O papel de um nomeadores na segurança da rede é muito menos técnico do que o de um validador. Isso ocorre porque os nomeadores são solicitados apenas para bloquear seus *tokens* em apoio aos validadores que farão o trabalho pesado de executar os nós. Como o vínculo necessário para se tornar um validador é alto (atualmente 1,4 milhão de DOTs), os validadores precisam garantir o suporte contínuo de um grande número de *tokens* de nomeadores para se qualificarem para sua função. Quando as recompensas são pagas ao validador, uma parte dessas recompensas vai para os nomeadores; o valor exato é baseado no número total de *tokens* em *stake* e na porcentagem de comissão definida pelo validador.

Ao contrário de muitos sistemas *PoS* que forçam os nomeadores a vincular todos os seus *tokens* a um único validador, Polkadot usa um mecanismo avançado que permite que cada nomeador escolha até 16 validadores. Destes, apenas alguns validadores conseguirão ser admitidos no conjunto ativo durante as eleições que ocorrem em todas as épocas (que é aproximadamente um dia em Polkadot). Ao escolher 16 validadores, os nomeadores aumentam as chances de obter o máximo de recompensas. Isso ocorre porque a *relay chain* na qual você faz *stake* de seus *tokens*, tem um protocolo que otimiza o processo de *stake* para todos os nomeadores e validadores para garantir segurança máxima. Os detalhes desta ação são muito técnicos, então vou oferecer apenas um resumo básico de suas principais funcionalidades:

Maximizar a participação do nomeador - O algoritmo (protocolo) maximiza a participação de um nomeador no consenso selecionando pelo menos um dos validadores do nomeador para cada era. Uma era é uma medida de tempo em *blockchains*, um pouco como nós humanos temos dias, que é denominado pelo número de blocos produzidos: 6 horas em Kusama e 24 horas em Polkadot. Quando um nomeador seleciona 16 validadores, esse mecanismo garante que pelo menos um desses dezesseis estará no conjunto ativo.

Minimizar risco de centralização - Isso é alcançado através da teoria dos jogos. É natural que os humanos busquem o que é mais certo, que muitas vezes é a mais popular de todas as opções disponíveis. Por exemplo, se muitos nomeadores escolherem um validador, outros nomeadores estarão inclinados a escolher o mesmo validador. E é assim que ocorre a centralização, pois o validador acaba com mais poder sobre a rede do que o inicialmente pretendido. Para mitigar esse risco, o protocolo de *staking* paga recompensas iguais a todos os validadores, independentemente do peso de sua participação ou do número de nomeadores que os apoiam. Mas validadores com muitos nomeadores pagarão menos recompensas por DOT em *staking* no geral. No final, apenas os nomeadores que fazem *stake* da maioria dos DOTs com esses validadores populares receberão a maior parte das recompensas, enquanto os nomeadores que não fazem *stake* de muitos DOTs receberão muito menos (ou não, dependendo de como o validador estiver sobrecarregado). O número de indicados que recebem recompensas em tal situação é dinâmico e varia ao longo do tempo. Isto pretende ser um mecanismo para forçar cada nomeadores a rever constantemente suas nomeações e garantir que eles estejam recebendo a máxima recompensa por sua participação na rede

Como nomear

O primeiro passo para nomear é obter seus *tokens* DOT, para os quais você precisa de uma conta e uma carteira. Você pode usar carteiras como Polkadot-JS, Fearless, Talisman, Nova, Polkawallet e muitas outras carteiras do ecossistema. Uma coisa a lembrar é que, depois de vincular seus fundos para *staking*, você ficará sob um período obrigatório de "desvinculação" de 28 dias. Isso significa que, a partir do momento em que você optar por desmarcar e retirar seus *tokens*, levará 28 dias para recuperá-los.

Para evitar esse inconveniente, você pode fazer *stake* com um terceiro que lhe dará mais liberdade, pois algumas corretoras centralizadas permitem que você retire seu *stake* instantaneamente. Uma solução preferível seria usar plataformas descentralizadas que fornecem um *token* derivado quando você faz *stake* de seu DOT. Por exemplo, você pode fazer *stake* de seu DOT usando Acala (mais sobre eles mais tarde) e receber LDOT que é a abreviação de "*liquid* DOT" (DOT líquido). A diferença entre o DOT e o *token* derivado LDOT é que o LDOT ganha recompensas de *staking* enquanto permanece disponível para uso em protocolos *DeFi* em todo o ecossistema. De tal forma que quando você for trocar seus LDOTs de volta para DOTs, você terá mais DOTs do que antes. O LDOT não é o único *token* que cumpre essa função. Existem outras *parachains* que oferecem o mesmo serviço

de *staking* líquido, mas com nomes diferentes para seus *tokens* (vDOT da Bifrost e xDOT da Parallel Finance, para citar alguns).

O verdadeiro trabalho de nomear se resume a selecionar seus 16 validadores. Se você está fazendo *stake* por meio de uma plataforma de terceiros, não precisa passar por esse processo. No entanto, se você fizer stake por conta própria, precisará aprender a selecionar os validadores certos.

Selecionar os validadores corretos

Selecionar o validador correto é um processo crucial devido à realidade do *slashing* (caso um validador erre na validação fazendo com que o nomeador e o validador percam perder parte de seus *tokens* em *stake*). Se você escolher um validador que age de forma maliciosa, corre o risco de perder seus *tokens* suados, o que seria uma tragédia. Outra razão pela qual você deseja selecionar os validadores certos é maximizar suas recompensas de *stake*. Alguns validadores permitem que você ganhe mais do que outros e é seu trabalho maximizar suas próprias recompensas. Ao selecionar os validadores certos, há algumas coisas que você precisa considerar.

Validador com pele em jogo - É difícil alguém agir de forma maliciosa ou descuidada quando tem algo a perder. Isso também é conhecido como ter “pele em jogo”. Se um validador não tiver nenhum *token* em seu próprio estoque, isso significa que ele não tem nada a perder se for cortado; mas seus nomeadores arcarão com as consequências de suas ações. Se ele for recompensado, no entanto, ele poderá manter algumas recompensas robustas. Assim, não é aconselhável colocar em *stake* em um validador com pouco ou nenhum *stake* próprio, a menos que você confie que ele não agirá de forma maliciosa ou descuidada.

Identidade do validador - É difícil alguém agir maliciosamente quando sua identidade é conhecida por todos na rede. Claro, isso não vai salvá-lo de todos os erros do validador, mas é uma regra prática confiável para usar. As pessoas que exibem sua identidade *on-chain* são mais confiáveis do que aquelas que não exibem porque sua reputação está em jogo. No caso de alguém com uma identidade *on-chain*, você pode entrar em contato para descobrir o que está acontecendo no caso de você ter dúvidas sobre transações. No entanto, alguns validadores maliciosos podem ser cortados e decidirem criar um nova conta de validador com uma nova identidade, que provavelmente seria a mesma da original, apenas com alguns detalhes alterados.

Comissão do validador - Para maior rentabilidade, é mais prudente escolher validadores com as comissões mais baixas. Um validador com uma comissão de 50% receberá 50% de todas as recompensas de *staking*, deixando apenas 50% para ser compartilhado entre os indicados. Um com uma comissão de 10% levará apenas 10% de todas as recompensas, o que certamente o tornará muito mais lucrativo para os nomeadores.

Histórico de corte (*slashing*) do validador - É natural tomar uma decisão sobre uma pessoa ou entidade com base no desempenho passado. No caso de validadores, você não deseja nomear validadores que tiveram vários cortes no passado. No entanto, às vezes os validadores podem estar na extremidade receptora de eventos de corte que não são inteiramente culpa deles. Às vezes, a rede pode ter problemas que fazem com que validadores honestos e diligentes sejam penalizados.

Para obter mais informações sobre a maneira mais segura de nomear validadores, consulte este guia.

Coletores

Enquanto os validadores criam e confirmam blocos para a *relay chain*, os coletores criam e confirmam blocos para as parachains. Tenha em mente que os mesmos mecanismos (BABE e GRANDPA) estão em jogo nas *parachains*. Você pode pensar em coletores como validadores de *parachain*, porque eles precisam executar um nó completo da *parachain*, bem como a *relay chain*. Quando coletores em uma *parachain* concordam com novos blocos de *parachain*, eles encaminham esses blocos para validadores da *relay chain* para inclusão na *relay chain*. Dessa forma, os blocos de transação verificados enviados pelos coletores são verificados pelos validadores e adicionados à *relay chain*; com validadores de *relay chain* atribuídos a *parachains* de forma aleatória.

Por exemplo, na primeira era, que dura um número x de blocos, os validadores V1, V2 e V3 são atribuídos à *parachain* A. Isso significa que os coletores da *parachain* A encaminharão suas transações para V1, V2 e V3, deixando todos os outros validadores livres para verificar transações de outras *parachains*. Quando esses validadores terminam de verificar, eles propõem suas transações verificadas ao restante dos validadores na *relay chain* para verificação adicional antes que as transações sejam adicionadas à *relay chain*. Lembre-se de que a maior parte disso é bastante automática. Os validadores não sabem de antemão em qual *parachain* estarão trabalhando. No final da era, os validadores V1, V2 e V3 serão afastados da *parachain* A, de modo que um novo conjunto de validadores verificará as transações na *parachain* A durante a segunda era.

Esse processo fortalece a segurança da rede, minimizando e contendo o risco de conluio entre coletores e validadores. Por exemplo, se houvesse um ataque durante uma era, esse ataque seria combatido por validadores honestos no início da era seguinte.

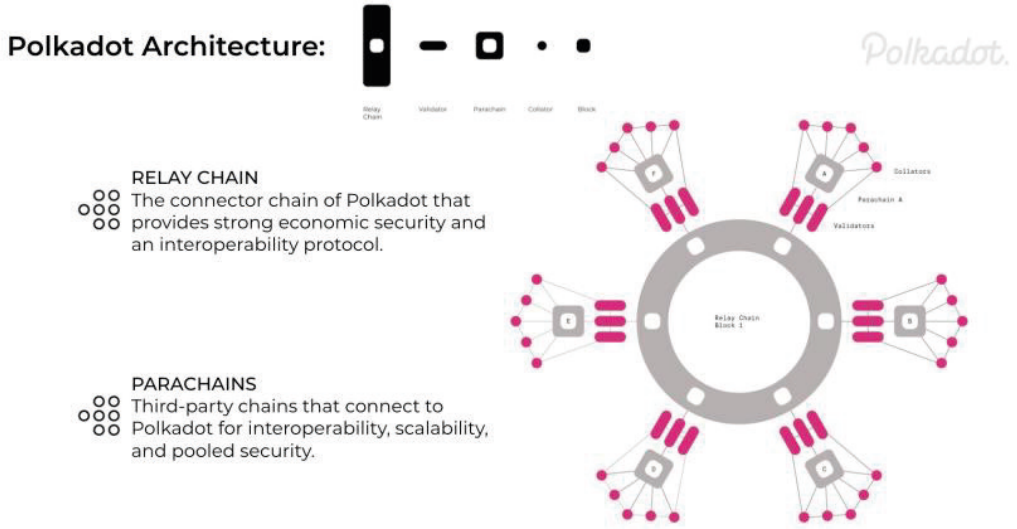


Diagrama de arquitetura de validadores, nomeadores e coletores

1. National Oceanic and Atmospheric Administration. (2021, January). 2020 was Earth's 2nd-hottest year, just behind 2016.

https://www.noaa.gov/news/2020-was-earth-s-2nd-hottest-year-just-behind-2016. Acessado em 31/08/2021.

Capítulo 4

GOVERNANDO A REDE

Quando um clássico saiu com o dinheiro

Em 2016, US$ 60 milhões em ETH foram roubados no que agora é chamado de "*hacker* DAO". Este é um breve resumo de como isso aconteceu.

Em abril de 2016, um grande número de pessoas reuniu seus *tokens* Ethereum em um contrato inteligente para financiar a primeira Organização Autônoma Descentralizada (DAO), do ecossistema de criptomoedas. US$ 150 milhões foram arrecadados durante este financiamento coletivo. No entanto, menos de três meses depois, o contrato inteligente foi hackeado e um mau ator começou a drenar os fundos. A comunidade entrou em pânico. Em pouco tempo, um grupo de *hackers* do bem surgiu, colaborando para tentar parar o infrator. Os detalhes de como o *hack* ocorreu seriam muito técnicos para este livro, mas ficou claro que o *hacker* do mal tirou vantagem de uma falha no código do contrato inteligente. Desde que o atacante só poderia retirar os *tokens* muito lentamente o coletivo de *hackers* do bem finalmente encontraram uma maneira de impedir a exploração. Mas os salvadores cometeram um erro que eventualmente permitiria que o ladrão ficasse impune com o dinheiro: a única solução que restava era reverter a cadeia e cancelar este evento.

Dado que o roubo aconteceu bem debaixo do nariz da comunidade Ethereum, você pensaria que decidir sobre o curso certo de ação seria uma conclusão fácil de alcançar. Mas não foi esse o caso. Primeiro, a comunidade teve que descobrir uma maneira de sondar os usuários da rede Ethereum sobre o que eles achavam que deveria acontecer em seguida. Isto porque, na época, era geralmente aceito que os dados da *blockchain* eram imutáveis, selados por criptografia, e que o que quer que acontecesse na cadeia nunca poderia ser revertido. Mas, neste caso, como US$ 60 milhões haviam sido roubados, os ideais tinham que se confrontar com a realidade. E a realidade da situação era que era possível mudar as informações armazenadas na blockchain do Ethereum.

Dois campos surgiram como resultado dessa descoberta. Por um lado, a maioria queria apagar o histórico do furto, revertendo a corrente para o bloco anterior ao ataque. Por outro lado, os puristas da descentralização eram contra adulterar a imutabilidade da *blockchain* do Ethereum. No final, uma votação foi realizada e 80% da comunidade votou para apagar o *hack* da história do *blockchain* do Ethereum. Para fazer isso, um *fork* teve que ser criado para atualizar o *blockchain* e reescrever o código original. Mas para uma bifurcação seguir em frente, todos os nós da rede precisavam aceitar a atualização para que a rede pudesse entrar em um novo estado e prosseguir em uma nova direção. Assim, quando a atualização foi realizada, apagou todos os vestígios do *hack* e a maioria dos membros da comunidade ficou feliz que a moralidade havia vencido e que o ladrão ficaria sem nada. Ele ficaria mesmo?

Logo ficou claro que, embora a rede Ethereum tivesse se bifurcado em uma nova cadeia e estivesse escrevendo uma nova história, havia alguns nós que não seguiram o caminho da nova atualização. Basicamente, eles escolheram permanecer na antiga cadeia canônica Ethereum, com registros do roubo ainda em vigor. Logo, um novo tipo de pânico se instalou: os operadores de nós estavam fazendo isso intencionalmente? Seria o *hacker*? Tentativas foram feitas para chegar aos mineradores e, no final, ficou claro que foi um ato deliberado, embora os motivos ainda permaneçam desconhecidos. A antiga cadeia que recusou o *fork* ficou conhecida como Ethereum *Classic*. Você pode saber mais sobre essa história em "Out of the Ether", um livro de Matthew Leising lançado em agosto de 2020. Tornou-se necessário aprofundar esse pouco da história para destacar a importância do *design* de governança *on-chain* de Polkadot e das atualizações sem bifurcações.

Você pode então se perguntar: qual é o grande negócio com a bifurcação do Ethereum em Ethereum *Classic*? Do ponto de vista da descentralização, faz sentido dar a cada participante da rede a liberdade de escolher se um *fork* é adequado ou não, preservando assim a integridade da cadeia. Mas também apresenta outros riscos importantes para a comunidade: quando alguns mineradores romperam seu consenso com a rede Ethereum e optaram por permanecer na antiga cadeia, a segurança do Ethereum foi comprometida em três níveis:

1. A rede ficou com menos mineradores para minerar transações.
2. O valor do ETH foi afetado, pois seu preço entrou em queda livre.
3. A fé da comunidade foi abalada pelo *hack* e pela bifurcação inesperada

Infelizmente, este não é o único *fork* controverso que aconteceu na história das redes *blockchain*. Isso também aconteceu com o Bitcoin. Tudo começou quando a comunidade Bitcoin entrou em uma discussão sobre a velocidade da *blockchain* Bitcoin, propondo diferentes maneiras de escalar a rede e aumentar o número de transações que podem caber em um bloco. Um campo queria aumentar o tamanho do bloco em 8x para processar 8x mais transações por segundo. Mas isso também aumentaria o tempo de validação do bloco além de 10 minutos, pois a rede espera que os blocos agora maiores sejam preenchidos. Outros pensaram que adulterar o protocolo Bitcoin era uma heresia.

Não houve votação nem consulta; uma parte da rede Bitcoin foi bifurcada em uma nova rede chamada Bitcoin *Cash*, que os viu atualizar o código existente para permitir um aumento no tamanho do bloco. Ao longo dos anos, o Bitcoin foi bifurcado em muitas outras redes, no entanto, o poder de mineração que protege esses *forks* está cada vez mais concentrado nas mãos de algumas grandes *pools* de mineração.

Portanto, essas redes bifurcadas podem ser facilmente atacadas porque não oferecem o mesmo valor que o Bitcoin e não podem atrair participantes de rede suficientes. Isso ocorre porque o poder de qualquer rede descentralizada está na força, números e níveis de participação de sua comunidade.

Quando olhamos para Bitcoin e Ethereum hoje, parece que esses *forks* não tiveram impacto nas redes, mas isso seria uma visão ingênua da situação. O fato de ambas as redes terem chegado tão longe, apesar desses episódios controversos, não é prova de que seu *design* seja ideal. Em vez disso, aponta para um problema inerente a todas as redes *blockchain*: se o código estiver disponível para que todos vejam e copiem, é fácil bifurcar. E se você bifurcar uma rede o suficiente, poderá danificar sua segurança para sempre. Porque cada bifurcação resulta em perda de valor da rede e poder de consenso, afastando mineradores ou membros da comunidade.

Então, como você pode evitar o enfraquecimento de uma rede e sua comunidade? A resposta de Polkadot é oferecer um processo de governança *on-chain* em que todos os participantes possam confiar. Juntamente com atualizações sem bifurcação, você obtém uma *blockchain* que é facilmente atualizável sem impor alterações importantes. Para entender como, vamos mergulhar no mecanismo de governança de Polkadot. Esta seção seguirá um formato de perguntas e respostas.

Governança de Polkadot

1. Para que serve a governança?

O principal objetivo da governança em qualquer sistema é modificar os parâmetros do sistema. No caso dos países, seriam novos projetos de lei e revisões da constituição. No caso de Polkadot, esses seriam dados *on-chain*. Alguns exemplos incluem:

- Atualizar saldos de usuários (no caso de roubo ou perda de chaves, por exemplo)
- Atualizar o tempo de execução
- Conectar ou desconectar *parachains* e *parathreads*

2. Qual é a estrutura da governança?

A estrutura de governança *on-chain* de Polkadot tem 3 ramificações: o Conselho, o Comitê Técnico e a comunidade (também chamada de “câmara de referendo” ou o número de

detentores de DOT disponíveis para votação). Vamos examinar cada um deles em detalhes.

Conselho - Este é um grupo de 6-24 membros que representam todos os detentores de DOT. Seu objetivo principal é examinar propostas que visam dar novos rumos à rede Polkadot.

O que podem fazer?

- Eleger os membros do comitê técnico
- Votar nas moções do Conselho - Todas as propostas (Referendo, Tesouro, Recompensa, Gorjetas) precisam ser explicitamente aprovadas/rejeitadas pelo Conselho antes de passar para a próxima etapa. As únicas exceções são as propostas lideradas pela comunidade.
- Vetar referendos no caso de uma proposta ser considerada prejudicial ao ecossistema. Dito isso, seu veto pode ser derrubado por meio de outra votação pública.
- Referendos rápidos em caso de emergência técnica.

Quem pode fazer parte do Conselho?

Qualquer *holder* de DOT.

Como são selecionados?

Um *holder* de DOT que deseja ingressar no Conselho precisa apenas se nomear e reunir votos suficientes para entrar no conjunto eleito. Os detentores do DOT podem eleger membros do Conselho para governar a rede em seu nome, vinculando seus *tokens*, da mesma forma que escolheram seus validadores. Como tal, qualquer detentor de DOT disposto a se tornar um membro do Conselho deve estar disposto a fazer campanha para os indicados porque os membros do Conselho são selecionados com base no apoio e na preferência que os eleitores deram a eles.

A cada duas semanas uma eleição é realizada para reorganizar a composição do conselho a fim de evitar o nepotismo. Isso foi projetado para incentivar a participação da comunidade na governança, pois convida os *holders* a delegarem o poder de seus DOTS a outros membros dispostos a governar a rede. Mas este é apenas um cenário ideal. Na realidade, os mesmos membros do Conselho geralmente permanecem em seus cargos por meses porque não há candidatos suficientes no Conselho e porque os eleitores raramente mudam sua lista de candidatos preferidos.

Qual é o mecanismo de votação

A seleção dos membros do Conselho é feita pelo mesmo mecanismo implementado no *staking*. No entanto, como a seleção depende do peso do *token*, existe a chance de, com o tempo, a rede favorecer usuários com um grande número de DOT chamados “baleias”.

Não há solução perfeita para este problema até agora, mas o método *Phragmén* que é usado em Polkadot oferece uma solução interessante. Isso ocorre porque seu algoritmo leva em consideração o peso do *token* por trás de cada candidato, mas não toma decisões apenas com base nessas informações. Em vez disso, o método otimiza os resultados para os seguintes cenários ideais:

1. Maximizar o valor total em jogo para garantir a máxima segurança econômica.
2. Maximizar o *stake* por trás do validador minimamente apostado para que todos os candidatos continuem competindo para obter apoiadores que lhes permitam acessar o conjunto ativo.
3. Minimizar a variação de *stake* no conjunto para que não haja muita diferença entre os validadores com *stake* mais alto e mais baixo.

Em suma, o método *Phragmén* faz um ótimo trabalho ao criar um certo grau de justiça considerando todas as coisas. Para entender seu funcionamento interno, reserve um tempo para ler este artigo da Wiki.

Comitê Técnico - O TC é composto por desenvolvedores que contribuíram para a base de código de Polkadot. Eles são encarregados de garantir que a rede funcione sem problemas.

O que é que eles podem fazer?

1. Fazer propostas ao Conselho
2. Propostas rápidas, geralmente no caso de uma emergência técnica
3. Vetar referendos por meio de uma recomendação ao Conselho, se um referendo representar um risco de segurança para a *relay chain* de Polkadot.

Quem pode participar do Comitê Técnico?

As equipes são adicionadas ou removidas do comitê técnico por maioria simples de votos do Conselho.

Comunidade - É composta por todos os *holders* de DOT que podem e estão dispostos a participar das seguintes atividades:

1. Nomear membros do Conselho
2. Fazer propostas
3. Votar em referendos

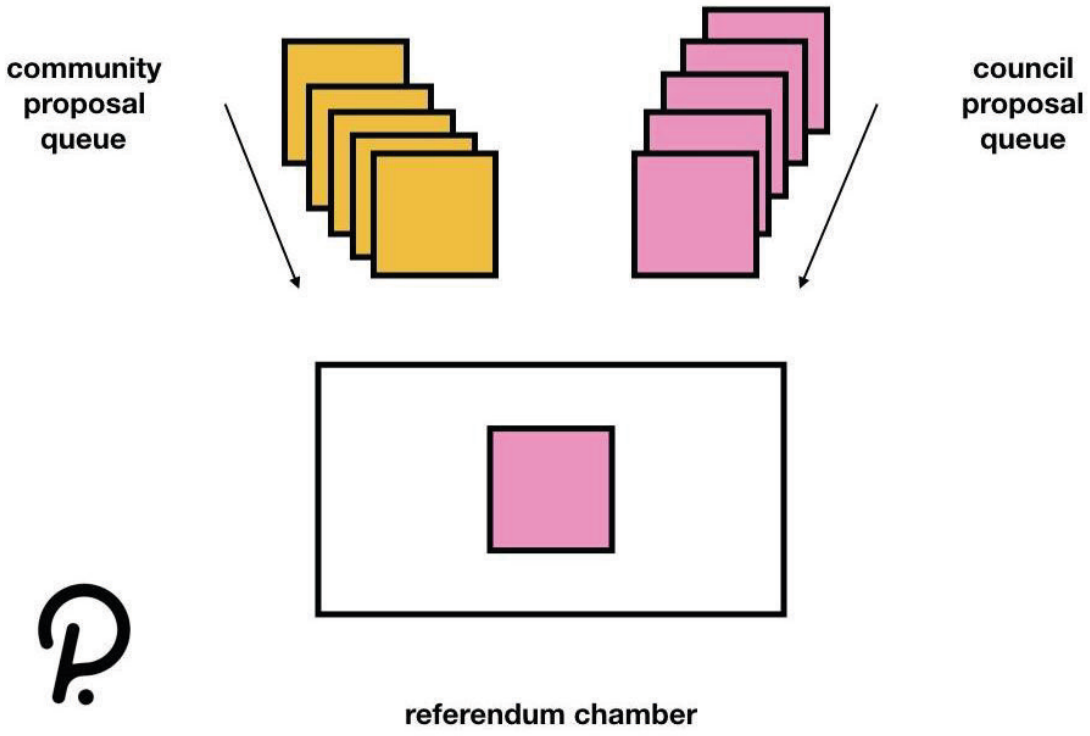
3. Como são tomadas as decisões?

Cada decisão tomada sobre a direção de Polkadot começa com uma proposta. Uma proposta pode ser iniciada por qualquer um dos três braços de governança, embora todas as propostas do Comitê Técnico sejam submetidas ao Conselho, que então a vota. Se a proposta for bem sucedida, então torna-se um referendo público. Como tal, existem duas

filas principais de propostas: uma para propostas lideradas pela comunidade e outra para propostas lideradas pelo Conselho.

A cada “ciclo de votação” (28 dias em Polkadot), a proposta apoiada pelo maior número de tokens se torna um referendo público. Só pode haver uma proposta por referendo, exceto em situações de emergência, quando a comissão técnica precisa acelerar uma ou mais propostas complementares.

Se uma proposta da fila da comunidade foi votada no último ciclo de votação, a principal proposta da fila do Conselho será apresentada no novo ciclo de votação. Essa abordagem de turnos ajuda a garantir que a comunidade, o Conselho e o comitê técnico possam participar ativamente na tomada de decisões oportunas.



O processo do referendo: duas filas.

4. Qual é o ciclo de vida de uma proposta?

Cada proposta submetida via governança *on-chain* pode se enquadrar em qualquer um dos seguintes *status*:

Destacada - Quando um membro da comunidade faz uma proposta, ele ou ela deve vincular alguns DOTs. Se a proposta for valiosa para outros membros da comunidade, eles podem apoiá-la, bloqueando mais DOTs no vínculo original. Quanto mais DOTs forem

vinculados em apoio a uma proposta, mais rápido essa proposta chegará ao topo da fila, e nesse ponto ela mudará de *status*. Um processo semelhante está em vigor para as propostas lideradas pelo Conselho.

Pendente - Quando uma proposta chega ao topo da fila, em breve será convertida em um referendo público oficial. É importante notar que uma vez que a proposta é programada, os DOTs vinculados são devolvidos aos proponentes/apoiadores.

Cancelada - Se uma proposta for considerada perigosa para a *relay chain* de Polkadot, ela poderá ser cancelada pelo Comitê Técnico. Se tal proposta atingir o *status* de referendo antes que a natureza de sua ameaça seja identificada, então uma maioria de dois terços do Conselho pode cancelar o referendo. Se o cancelamento de um referendo for contencioso, a tomada de decisão será passada para a comunidade. Quando uma proposta ou referendo é cancelado, todos os *tokens* depositados como parte de seu vínculo são queimados.

Lista obscura - Uma proposta que representa um risco significativo para o sistema, por exemplo, um erro de codificação, pode ser colocada na lista negra pelo protocolo. Uma proposta na lista negra não pode ser adicionada novamente à fila, a menos que tenha sido alterada.

5. Como são calculados os votos?

Para calcular os resultados de um referendo, existem dois mecanismos principais que valem a pena considerar.

Multiplicador de Convicção - Esta é uma área chave da governança que aproveita ao máximo a teoria dos jogos. Isso ocorre porque um sistema que depende muito de *proof of stake*, precisa ter processos eficazes para nivelar o campo de jogo para os *holders* de *tokens*. Em Polkadot, essa prática é respaldada pelo multiplicador de convicções.

Digamos, por exemplo, que há apenas dois eleitores em um referendo: eleitor G e eleitor B.

> G vota com 20 DOTS
>
> B vota com 90 DOTS

Naturalmente, esperamos que a opinião do eleitor B vença. Este não é o caso quando você introduz o multiplicador de convicção porque tanto o número de *tokens* vinculados quanto a duração do vínculo são considerados no resultado final.

Vamos dar uma olhada mais detalhada na convicção estabelecida pelo eleitor G e pelo eleitor B.

> G vota com 20 DOTS por um período de bloqueio de 6 ciclos de votação

B vota com 90 DOTS por um período de bloqueio de 1 ciclo de votação

De acordo com as especificações da *blockchain* Polkadot, um ciclo de votação é de 4 semanas e cada ciclo aumenta o multiplicador de convicção por um fator de 1. Assim, no exemplo acima, eis como será o resultado.

G = 20 x 6 = 120 PONTOS

B = 90 x 1 = 90 PONTOS

Como você pode ver, a opinião do eleitor G terá maior consequência porque ela teve um multiplicador de convicção maior. Para saber mais sobre esse mecanismo interessante, você pode ler este artigo da Wiki.

Ainda não sabemos até que ponto o multiplicador de convicção reequilibra o poder de voto entre os membros da comunidade com poucos DOTs e aqueles com carteiras muito maiores, portanto, essa solução pode exigir mais ajustes no futuro.

Uma última coisa a notar é que os *tokens* usados para votar em referendos ou nomear membros do Conselho estão temporariamente bloqueados e não podem ser transferidos para outra conta, o que torna dispendiosa qualquer tentativa de burlar o sistema. No entanto, esses DOTs ainda podem ser colocados em *stake* para ganhar recompensas de produção em bloco.

Tendência de Quorum Ajustada - Esta é outra área importante da governança *on-chain* que faz uso extensivo da teoria dos jogos em seu *design*. Existem três maneiras diferentes de determinar o resultado de um referendo público, dependendo de qual órgão de governança iniciou a proposta.

Maioria Simples

Se uma proposta for submetida com a aprovação da maioria do Conselho, então ela precisa de uma maioria simples de “sim” ou “não” para ser aprovada ou reprovada. Independentemente da participação dos eleitores, a maioria determinará o resultado final da votação.

Viés de Participação Positiva

Para referendos originados de propostas lideradas pela comunidade, as coisas são um pouco diferentes. Se poucos eleitores comparecerem, a quantidade de “sim” necessária para prosseguir com as atualizações aumenta consideravelmente. Por exemplo, onde 19% dos membros da comunidade votam, pode levar apenas 20% de 'não' para derrubar 80% de 'sim'.

Essa configuração foi projetada para proteger o ecossistema de maus atores que apresentam propostas controversas na esperança de que uma baixa participação no referendo favoreça os resultados desejados.

Viés de Participação Negativa

Este mecanismo é usado para computar os votos de um referendo originado de uma proposta liderada pelo Conselho. Nesse cenário, o mecanismo se posiciona contra a rejeição da proposta, de modo que, com um número baixo de eleitores, o percentual de 'sim' necessário para aprovar a proposta será baixo. Por exemplo, com uma participação de 30%, apenas 30% dos 'sim' serão necessários para derrubar 70% dos 'não'. O principal objetivo aqui é agilizar as atualizações técnicas na rede. Se o conselho e a comunidade técnica concordarem por unanimidade sobre os méritos de uma proposta, também é seguro assumir que as mudanças propostas agregarão valor ao ecossistema.

6. O que acontece depois do referendo?

Se um referendo falhar, nada acontece na cadeia. Se o referendo for aprovado, as mudanças na cadeia serão implementadas automaticamente pelo sistema após um período de espera de 28 dias. Essa é uma das vantagens da governança *on-chain* conforme codificada em Polkadot, que também destaca por que é importante ter a opção de cancelar ou colocar na lista negra as propostas.

Com todos esses parâmetros principais considerados, sinto a necessidade de adicionar mais uma seção.

Críticas ao mecanismo de governança de Polkadot

Os processos de governança *on-chain* de Polkadot atraíram muitas críticas. Na maioria das vezes, esses comentários negativos nascem da ignorância e não de opiniões fortes sobre questões específicas. Esta seção abordará as críticas mais comuns e proporá um contra argumento.

1. É outra forma de centralização/se tornará centralizada

Algumas pessoas acreditam que um processo de governança visível e ativo é apenas mais uma forma de centralização esperando para acontecer. Sinceramente, eu também tenho esse medo. Dito isso, um processo de governança realmente não instiga a centralização, são os usuários que o fazem. Atualmente, muitas pessoas acreditam que Ethereum é totalmente descentralizado quando se trata de tomada de decisões, o que não é completamente verdade. Mas o que a fundação Ethereum faz com seu orçamento? Como exatamente os gastos são governados ou monitorados pela comunidade? Isso não quer dizer que algo obscuro esteja acontecendo nos bastidores. Longe disso. Meu ponto principal é que ninguém na comunidade Ethereum conhece todos os detalhes de como os

fundos estão sendo gastos e quem está dizendo sim a essas propostas de gastos. Isso não pretende ser uma crítica ao processo de Ethereum, mas sim chamar a atenção para o fato de que as informações sobre alguns de seus trabalhos permanecem bastante vagas. Assim, como alguém pode realmente ter um problema em ter um método mais transparente de fazer a mesma coisa? Estou apenas apontando alguns aspectos que podemos ignorar ou dar como certo.

Quando se trata de desenvolvimentos relacionados à rede, é amplamente aceito que as ideias de Vitalik Buterin estão impulsionando o roteiro do ecossistema Ethereum. Outros participantes frequentemente defendem suas ideias em novos projetos, enquanto uma minoria de críticos aponta falhas antes que as mudanças sejam implementadas pelos mineradores. Este é um bom processo na prática, mas pode ser muito lento e carente de transparência. Embora o mesmo tenha sido dito sobre Polkadot no início, agora podemos verificar todas as mudanças porque tudo está *on-chain.*

Se há um tesouro, então a comunidade precisa saber como ele está sendo gasto. E se não houver, a comunidade não se beneficiaria de ter um? A partir de agora, não há tesouraria oficial Ethereum ou Bitcoin que possa fornecer financiamento aos membros da comunidade de maneira aberta e verificável da mesma forma que uma tesouraria *on-chain* está disponível para apoiar o desenvolvimento do ecossistema. Além do financiamento, é óbvio que os processos de tomada de decisão estão atualmente centralizados nas mãos de uma fundação. Pessoalmente, não vejo culpa nisso, pois é difícil imaginar que as pessoas que construíram um sistema planejariam destruí-lo; é também por isso que confiamos implicitamente nos fundadores dos projetos. Mas ainda sou a favor de processos *on-chain* como forma de tomar decisões sustentáveis relacionadas à rede descentralizada.

Afinal, se queremos uma sociedade melhor, que ainda refletirá a atual, mas com regras mais justas, precisamos de *blockchain*. Isso ocorre porque a *blockchain* é uma ferramenta que podemos usar para corrigir ou melhorar nossos sistemas de governança. Muitos erros serão cometidos e muitas lições serão aprendidas, mas no geral, experimentar é muito melhor do que não fazer nada.

2. Dá aos maus atores (ou novatos) oportunidade de causar danos à rede

Esta é uma preocupação legítima e, felizmente, foi considerada no projeto de governança de Polkadot. Por um lado, qualquer mau ator que deseje destruir a rede via governança deve estar disposto a gastar muito dinheiro denominado em DOT. Isso significa que qualquer pessoa que deseje influenciar os votos para um resultado negativo teria que:

1. Convencer um grande número de detentores de DOT a tomar uma decisão ruim com seu DOT
   OU
2. Financiar sua má decisão por conta própria

Qualquer cenário seria extremamente caro em termos de fundos e recursos. Mas se um novato apresentar uma proposta perigosa por engano, sempre haverá pontos de verificação no sistema de governança que permitem correções ou cancelamentos.

3. É muito complexo para o usuário comum.

Posso simpatizar totalmente com as pessoas sobre isso. A governança tradicional já é tão complicada que existem campos acadêmicos especiais para nos ensinar sobre isso. E, portanto, espera-se que um processo de governança que pretenda se tornar totalmente descentralizado tenha que incorporar muitas lições aprendidas da ciência política, história e teoria dos jogos em seu *design*, tornando-o complexo. Dito isto, você não pode obter uma compreensão sólida da constituição do seu país lendo uma série de postagens no *blog*. Assim como isso requer algum esforço, isso requer muito.

E no caso de Polkadot, tudo o que você precisa saber é que existem funções e processos específicos, cujas informações são muito menos do que um documento de 300 páginas. Como acontece com qualquer tecnologia, entender algo significa simplesmente ser capaz de usar e tirar o máximo proveito disso. Assim como o ser humano médio pode aprender sobre um conselho municipal comum, entender o que um conselho *on-chain* pode fazer não seria muito difícil. É certo que um pouco mais poderia ser feito para tentar simplificar as explicações dos processos de governança e as interfaces atualmente disponíveis.

4. Descentralização significa ausência de governança - Ethereum e Bitcoin estão indo muito bem

Essa crítica está longe de ser válida porque as tecnologias devem evoluir em direções diferentes, da mesma forma que o Ethereum *Classic* e o Bitcoin *Cash* se separaram de suas cadeias originais. Atualmente, a governança *on-chain* oferece uma maneira de resolver conflitos sem ir a extremos e fornecendo meios verificáveis para um fim. Com exceção do Bitcoin, a maioria dos projetos descentralizados tem uma Fundação pai. Mas o que é uma Fundação neste contexto, senão um grupo de pessoas em quem confiamos quando se trata de gerenciar o sucesso a longo prazo da rede? Nós realmente não podemos testemunhar como as decisões são tomadas e os passos que são dados na aplicação dessas decisões. Recebemos uma postagem no *blog* aqui e ali com algumas explicações vagas, mas não vemos uma contagem de votos. Agora, isso não quer dizer que um voto seja necessário para a validade de uma decisão, mas apenas para mostrar que depositamos muita confiança em decisões que são tomadas em nosso nome sem nenhum dado real para atestar sua legitimidade. Considerando que, em sistemas *blockchain* descentralizados, a confiança é tão boa quanto os dados verificáveis registrados na cadeia.

5. Há muita dependência de DOT, portanto, a rede está sempre à mercê dos grandes *holders*.

Essa é outra preocupação legítima sobre a qual tive que pensar muito no passado. Primeiro, há alguns aspectos que precisamos considerar:

1. Quem detém mais DOTs tem muito mais a perder se as decisões de governança impactarem negativamente o ecossistema. Assim, esse detentor é incentivado a apoiar as mudanças que são melhores para o ecossistema.
2. Polkadot reconheceu as limitações da governança baseada em *tokens* e está propondo uma solução para contornar esses problemas. Introduziu o mecanismo do multiplicador de convicções que permite aos pequenos *holders* dar mais peso aos seus votos.
3. Se a rede não estiver evoluindo na direção que você considera desejável, você sempre poderá optar por não participar do ecossistema.

A dependência excessiva de DOT é necessária para garantir o futuro da rede. *Proof of stake* é a **prova de participação**. Se estamos bem em proteger a rede usando mecanismos de prova de participação, por que devemos nos preocupar em adaptá-la à governança? A verdadeira questão é: existe uma maneira melhor de chegar a um consenso sobre as decisões de governança enquanto mantém as operações *on-chain*? Também é possível que nossa dependência de *tokens* acabe mudando se a comunidade considerar essa etapa necessária. E essa é a beleza dos processos de governança de Polkadot.

6. Algo vai dar errado, de uma forma ou de outra

Tendemos a ter um viés negativo em relação a coisas novas ou desconhecidas. Eu mesmo posso imaginar os piores resultados em quase todas as situações, então é natural para mim considerar a possibilidade de algo imprevisto acontecer no curso da governança em Polkadot. No entanto, a presença de um **processo de governança** ainda me dá motivos para permanecer positivo, porque aconteça o que acontecer, os *holders* de DOT podem decidir coletivamente sobre o curso de ação preferível para a rede. E se uma proposta de atualização dividir a comunidade em duas e chegarmos a um impasse, teremos um verdadeiro teste de resiliência da rede.

Em suma, a governança *on-chain* de Polkadot é uma das mais robustas do espaço porque incorpora ciência política, psicologia humana e teoria econômica em seu *design* e implementação. Uma ressalva importante é que tudo o que escrevi até agora está sujeito a alterações porque as coisas se movem muito rápido no ecossistema de Polkadot e praticamente todos os parâmetros do sistema podem ser ajustados pelos participantes. Isso é bom porque se as suposições erradas foram feitas na fase de projeto, elas podem ser corrigidas na próxima versão do sistema. Só o tempo pode revelar quais foram nossos

erros e, portanto, faz sentido dar a nós mesmos a oportunidade de observar e refletir enquanto isso.

Um novo tipo de tesouraria

Uma das vantagens de um processo de governança *on-chain* é que a comunidade pode aproveitar ao máximo a tesouraria do protocolo. Em Polkadot, a tesouraria *on-chain* é administrada pelo Conselho e seu único objetivo é promover a manutenção e o crescimento do ecossistema. Ele atinge esse objetivo por meio de vários componentes:

Recompensas (Bounties)

Existem limites práticos para as capacidades de curadoria dos membros do Conselho quando se trata de propostas de tesouraria. É altamente improvável que os membros do Conselho sempre tenham a experiência necessária para fazer avaliações adequadas das atividades descritas em todas as propostas, portanto, deve haver uma maneira de o Conselho delegar a supervisão das propostas a especialistas.

Um *Bounty* é uma recompensa por um corpo específico de trabalho - ou conjunto especificado de objetivos - que precisa ser executado para um valor de tesouraria predefinido a ser pago. Ele pode ser iniciado por qualquer detentor de DOT, que é chamado de proponente. Uma vez que o proponente tenha proposto uma recompensa, o ônus da execução e verificação do projeto recairá sobre um curador de recompensas. O curador de recompensas pode ser definido como uma pessoa ou grupo de pessoas com agência sobre uma parte limitada do Tesouro a ser usada para um propósito específico. Isso pode ser para corrigir um *bug* ou vulnerabilidade, desenvolver uma estratégia ou monitorar um conjunto de tarefas que beneficiam o ecossistema Polkadot.

Os curadores são selecionados pelo Conselho após a aprovação da proposta de recompensa. Antes de serem aprovados, os curadores precisam fazer um depósito para aceitar sua nova função, para que os fundos possam ser retidos para puni-los se agirem maliciosamente. No entanto, se eles forem bem sucedidos em sua tarefa de conseguir que alguém complete a recompensa, eles receberão seu depósito de volta, bem como a recompensa.

Proposta de gasto

Enquanto as recompensas definem tarefas específicas a serem concluídas, a proposta de gastos é mais aberta. Uma proposta pode ser voltada para construir infraestrutura, educar a comunidade, construir um novo projeto, criar ferramentas ou comercializar o ecossistema. Até o momento, mais de 100 propostas independentes foram financiadas pelo Tesouro de Polkadot, incluindo a criação deste livro. A principal diferença entre uma proposta de gastos e uma recompensa é que a proposta em questão será executada por seu proponente.

Gorjetas (Tips)

Esta é uma forma dos membros da comunidade recompensarem outros membros por seus esforços para manter e aumentar o ecossistema. Qualquer detentor de DOT pode solicitar uma gorjeta para qualquer membro que tenha feito algo digno de ser retransmitido. Por exemplo, uma vez fui indicado por um membro da comunidade para um artigo que escrevi sobre governança Polkadot

Financiando o tesouro

Os fundos do Tesouro vêm de diferentes fontes:

1. ***Slashing***: Quando um validador é cortado por qualquer motivo, o valor cortado é enviado para o Tesouraria como recompensa para a entidade que reportou o validador, muitas vezes outro validador. A recompensa é retirada do valor cortado e varia de acordo com a natureza da ofensa e o número de denunciantes.

2. **Taxas de Transação**: Uma parte das taxas de transação de cada bloco vai para a Tesouraria, sendo o restante para o autor do bloco.

3. **Ineficiência de *staking*:** A inflação é projetada para ser de 10% no primeiro ano, e a taxa de *staking* ideal é fixada em 50% da oferta total. Isso significa que metade de todos os *tokens* existentes deve ser idealmente bloqueado em *staking* para que a inflação vá inteiramente para os validadores como recompensa. Se a taxa de *staking* cair abaixo de 50%, os validadores receberão um valor menor, com o restante indo para o Tesouro.

4. ***Parathreads***: *Parathreads* participam de um leilão por bloco para inclusão em bloco. Parte do valor do seu lance vai para o validador que aceita o bloco e o restante vai para o Tesouro.

Para mais detalhes sobre o Tesouro, você pode ler este artigo no Wiki Polkadot.

Capítulo 5

EXPANDINDO A REDE

Tendo visto como a rede está estruturada, vamos agora ver como a rede está se expandindo por meio de *parachains*, a proposta de valor final de Polkadot. Sem *parachains*, a *relay chain* é apenas uma rede de esqueleto limitada as funcionalidades de *staking* e governança. Por outro lado, as *parachains* podem ser projetadas, no entanto, as equipes de construção desejam: com ou sem taxas de transação, maiores ou menores blocos. Em suma, cada *parachain* é um país próprio. E você pode pensar na *relay chain* como a rede que mantém as estradas e rotas marítimas que ligam cada um desses vários países.

Cada *parachain* também é uma *blockchain* de primeira camada muito personalizável que pode se enquadram nas seguintes categorias:

- Rede Pública de primeira cama
- Rede de primeira camada Privada
- Solução de dimensionamento de segunda camada
- Ponte

Isso é possível porque a *relay chain* não faz suposições sobre as entidades que a ela se conectam. Aceita-as como são, desde que elas sejam construídas usando linguagens de programação compatíveis com o Substrate. O Substrate é um conjunto de códigos (*framework)* para construir *blockchains* modernas, criado pela Parity Technologies, a empresa que foi contratada para construir Polkadot pela W3F. Assim, qualquer *blockchain* ou rede construída com Substrate é compatível com a *relay chain* de Polkadot.

Mas realmente, o que é uma *parachain*? O que significa ser uma? *Parachains* são como filhos de uma *relay chain*, pois são protegidos pelo poder econômico de sua *relay chain* pai e também são capazes de usar os recursos de computação de validadores de *relay chain* para operações de *cross chain*. As vantagens das *parachains* sobre as *blockchains* de primeira camada padrão são duas:

- Segurança compartilhada
- Interoperabilidade

O conceito de segurança compartilhada deve ser entendido agora, para que possamos nos concentrar na interoperabilidade, que é vista como o santo graal da tecnologia *blockchain*.

Interoperabilidade de *parachains*

Acredito que a interoperabilidade é o recurso "matador" de Polkadot. Se você não estiver familiarizado com *blockchain*, isso pode não fazer muito sentido para você, mas tentarei explicar por que a interoperabilidade da *parachain* é a chave para a inovação ilimitada dentro do espaço *blockchain*.

As finanças descentralizadas e a propriedade digital descentralizada (via *NFTs*) tornaram-se as potências que são hoje graças à interoperabilidade, à comunicação livre de confiança entre diferentes sistemas/redes automatizadas. Normalmente, diz-se que as plataformas *blockchain* são interoperáveis, quando os *tokens* de uma plataforma podem ser movidos para outra e vice-versa, por meio de uma ponte.

Por exemplo, se eu quiser enviar Bitcoin para Ethereum, tudo o que preciso fazer é acessar o aplicativo da ponte e fazer a transferência. Esta é agora uma operação bastante simples que pode ser concluída em alguns cliques. O que não vejo é que os *tokens* que mudei do Bitcoin para o Ethereum ainda estão tecnicamente na rede Bitcoin. Isso ocorre porque o método de transferência da ponte é congelar meus *tokens* BTC enviando-os para um endereço de propósito especial na rede Bitcoin, cunhar um novo conjunto de *tokens* derivados chamados "*Wrapped* BTC" (BTC embrulhado) na rede Ethereum e enviar os *tokens* BTC embrulhados para minha conta Ethereum.

Como eu disse, este é um processo direto, mas não é a interoperabilidade implementada na Polkadot. Existem dois aspectos na interoperabilidade:

1. Envio de *tokens* e mensagens
2. Chamada de funções

Hoje em dia, o primeiro aspecto é bastante trivial, mas o segundo é relativamente desconhecido. Para a *blockchain* A chamar uma função do *blockchain* B, precisaríamos automatizar as operações entre o *blockchain* A e o *blockchain* B, eliminando assim a necessidade de intermediários humanos. Em tal configuração, o *blockchain* A chamaria um contrato inteligente no *blockchain* B, que por sua vez responderia à *blockchain* A, fornecendo qualquer informação ou executando qualquer computação solicitada. Interoperabilidade!

Vamos usar outro exemplo prático para entender esse conceito.

Um usuário solicita o uso de seu valioso *NFT* armazenado na cadeia B como garantia na cadeia A, uma cadeia focada em *DeFi*, para obter um empréstimo. Mas antes que a cadeia A possa aceitar este pedido de empréstimo, ela precisa confirmar algumas coisas:

1. O usuário é quem diz ser?
2. O usuário possui o *NFT*?
3. Qual é o verdadeiro valor do *NFT*?

Além dessas questões, a cadeia A também precisa:

1. Cunhar um *NFT* para representar a posição do empréstimo
2. Enviar *tokens* para a cadeia B

Para coletar todos esses dados, a cadeia A precisará conversar com outras cadeias.

- Para saber a real identidade do usuário, a Rede A conversa com a Rede de identidade C, que verifica se o usuário é realmente quem diz ser e se tem direito ao empréstimo.
- Para confirmar que este usuário não possui empréstimos pendentes, a cadeia A faz verificações cruzadas com duas outras redes *DeFi* que são suas parceiras.
- Para verificar se o usuário realmente possui este *NFT*, a cadeia A passa a verificar as informações com a cadeia B.
- Para avaliar o valor dessa *NFT* e confirmar se os índices de colateralização são adequados, a cadeia A inicia um contrato inteligente na cadeia D, uma cadeia de previsão. Essa cadeia de previsão incentiva seu conjunto de previsores e avaliadores a analisar o verdadeiro valor do *NFT*.
- Tendo confirmado que tudo está bem, a cadeia A prossegue para coletar o *NFT* e trancá-lo em seu cofre de *NFT* na cadeia B, enquanto fornece ao usuário os *tokens* solicitados e começa a coletar os pagamentos da taxa de juros.

Observe que adicionei mais etapas do que o necessário para essa transação apenas para fins descritivos.

Assim, vemos que existem dois tipos de interoperabilidade: forte e fraca. Com uma interoperabilidade fraca, o usuário precisa fazer todas essas operações isoladamente, assinando várias transações em diferentes cadeias. Com forte interoperabilidade, uma cadeia pode aproveitar recursos de *cross chain*, identidade, previsão e cofres de outras cadeias para proteger suas operações e fornecer uma melhor experiência ao usuário.

Agora, dadas as fortes vantagens que as *parachains* têm sobre outras *blockchains* de primeira camada, agora podemos começar a entender por que haverá uma competição intensa por *slots* de *parachain*. Como a *relay chain* não pode ter um número infinito de *parachains*, seus recursos são finitos, ela suportará cerca de 100 *parachains* na próxima década, de acordo com o *whitepaper* de Polkadot. Mas isso apresenta um novo desafio: como determinamos quem recebe um *slot* de *parachain*?

Leilões de *slots parachain* e *crowdloans*

Em uma situação em que alguns itens valiosos estão disponíveis para venda, mas há uma grande demanda por parte dos compradores, a maneira mais sensata de distribuí-los é através de leilões, porque isso garante que aqueles que os valorizam mais serão tomadores finais. Para Polkadot, um sistema descentralizado com segurança tecnológica e econômica, encontrar a melhor forma de distribuir seus preciosos recursos de rede é primordial. É aí que entram os leilões de *slot de parachain* (*PSA*). Os *PSAs* são um mecanismo robusto que ajuda a alocar *slots* de *parachain* para o maior lance entre os diferentes projetos. Os detalhes completos de como ele consegue isso estão resumidos abaixo.

Cada leilão de *slot parachain* dura uma semana em Polkadot. Durante esta semana, as equipes de *parachain* fazem seus lances. Ao término do período do leilão, um vencedor é determinado. No entanto, os procedimentos reais são um pouco mais complexos.

Cada semana de leilões de *slot* de *parachain* é dividida em 2 fases: uma fase de abertura e uma fase de fechamento. As duas fases são necessárias porque Polkadot usa um novo mecanismo *on-chain* inspirado nos "leilões de velas". Tradicionalmente, a execução de um leilão envolve definir um cronômetro e permitir que o licitante mais alto surja quando o tempo acabar: isso é semelhante ao que você pode ver no Ebay. No entanto, como Polkadot trabalha para maximizar a segurança econômica de sua própria rede, esse estilo de leilão apresenta um grande problema, pois não incentiva os licitantes a fazerem seus melhores lances antecipadamente, deixando o sistema exposto ao corte do leilão.

Por exemplo, Bob quer fazer um lance para uma pintura com US$ 40.000, mas decide começar com US$ 15.000 para sentir o mercado. Quando seu lance é ultrapassado, ele adiciona US$ 500 extras e licita novamente. Mas seu lance é ultrapassado mais uma vez, então ele tem que continuar apostando, sem parar, até que o cronômetro atinja os últimos 3 segundos, com Bob ganhando a US$ 28.000. Infelizmente, no último segundo, Alice corta o lance de Bob com seu próprio lance de US$ 28.500 e Bob perde o leilão. Mas a verdadeira tragédia é que o artista perde uma avaliação maior para a pintura, já que US$ 28.500 é muito abaixo do orçamento real de Bob de US$ 40.000. Para desencorajar tais ações, o "leilão de velas" foi inventado por volta do século 17-18. Introduziu alguma aleatoriedade e incerteza na fase final de um leilão: os participantes foram encorajados a colocar os seus melhores lances antecipadamente porque, embora pudessem dizer o ponto de partida do leilão, ou seja, quando a vela está acesa, nunca poderiam adivinhar quando a vela morrerá sinalizando o fim do leilão.

Agora, implementar o leilão de velas em uma *blockchain* não é um assunto trivial porque as *blockchains* não são construídas para aleatoriedades. A solução de Polkadot é introduzir leilões de duas fases e um "tempo final aleatório retroativo" que entra em jogo durante a segunda fase dos leilões.

Na fase de abertura, que dura 2 dias, os projetos fazem lances registrados *on-chain* e vão até o final do leilão. Eles são livres para licitar o quanto acharem necessário para ganhar, mas também devem ter cuidado para não quebrar seus próprios tesouros. Na fase final, que dura 5 dias, todos os lances do(s) último(s) dia(s) podem ser potencialmente invalidados porque a *relay chain* usará uma função aleatória verificável para escolher retroativamente o momento em que o leilão terminou. Portanto, é o candidato a *parachain* que tiver o lance mais alto no momento exato em que o leilão termina que será o vencedor. Portanto, é possível que a *relay chain* decida que o leilão terminou no 3º dia no bloco #123456. Isso significa que um candidato a *parachain* que fez o lance mais alto após o bloco #123456 definitivamente perderá o leilão. É por isso que a fase de abertura é importante porque a *relay chain* sempre considerará todos os lances colocados na fase de abertura.

Um *slot de parachain* pode variar de 3 meses a 2 anos na Polkadot (1 ano na Kusama), dependendo do número de períodos de *slot* que a equipe escolher para seu projeto. Isso introduz outra dinâmica interessante para os leilões, porque a *relay chain* agora precisa considerar os seguintes requisitos ao selecionar um vencedor:

- Maximizar a receita econômica (conseguir que as equipes ofereçam o maior número possível de DOTs ou KSM).
- Maximizar a duração dos *slots* (fazer com que as equipes ofereçam o maior número possível de *slots*)

Isso significa que um candidato a *parachain* que tem o lance geral mais alto, mas para a duração de *slot* disponível mais curta, será menos favorável aos olhos da *relay chain* em comparação com o candidato a *parachain* que tem o segundo lance geral mais alto para a duração de *slot* disponíveis mais longas. No entanto, observe que a duração de um *slot* também depende dos períodos de *slot* disponíveis no momento em que o projeto precisa deles; e, portanto, esse cenário ideal nem sempre pode se concretizar.

Conseguir um *slot* de *parachain* pode ser um negócio muito caro. O primeiro *slot* de *parachain* em Kusama custou 500.000 KSM (~$90 milhões), o que não é ideal para a descentralização porque muitas poucas equipes podem, realisticamente, gastar tanto em aluguel digital. Para nivelar o campo de jogo, Polkadot implementou um módulo de *crowdloan* que permite que as equipes de *parachain* obtenham DOTs de suas comunidades. Isso é semelhante a uma rodada de financiamento, com algumas diferenças notáveis:

- Os *tokens* vinculados pela comunidade não são entregues às equipes de *parachain*. Em vez disso, eles são mantidos pela *relay chain*. Pense nisso como fazer *stake* sem ganhar recompensas de *stake*.
- Caso a equipe não ganhe o leilão, os *tokens* são devolvidos aos contribuidores.
- Se a equipe vencer o leilão, os *tokens* são vinculados à *relay chain* pela duração do aluguel. No final deste período de aluguel, os *tokens* são devolvidos aos contribuintes do *crowdloan*.

Para incentivar os membros da comunidade a contribuir com seu *crowdloan* durante os leilões de *slots* de *parachain*, as equipes candidatas a *parachain* geralmente oferecem aos contribuidores uma parte do fornecimento de seu *token* nativo, juntamente com outras vantagens como *NFTs, tokens* derivativos, bônus de taxas de *staking*, e funções especiais da comunidade. Para os membros da comunidade, isso se torna um cenário ganha-ganha, com a única perda incorrida sendo recompensas de *staking*, pois os *tokens* usados para empréstimos em leilões de *parachain* não são elegíveis para recompensas de *staking*.

Quando juntamos o mecanismo de leilão de velas e o módulo *crowdloan*, começamos a ver que Polkadot está pronta para um impulso de inovação e expansão sem precedentes. Digo isso pelos seguintes motivos:

1. As vagas de *parachain* devem ser conquistadas com a ajuda da comunidade, o que garante que as "melhores equipes" cheguem ao topo primeiro. Por "melhores equipes", quero dizer como equipes que podem entregar tecnologia e engajamento da comunidade. Porque é possível que as melhores equipes de tecnologia sejam ofuscadas por equipes de tecnologia mais fracas que tenham uma compreensão mais firme da construção da comunidade.
2. Os *slots* de *parachain* precisam ser renovados eventualmente, o que garante que as equipes se concentrem em fornecer melhores serviços à sua comunidade e aumentar seus tesouros para superar a dependência de *crowdloans*. Naturalmente, alguns projetos não poderão renovar seu *slot* de *parachain*, e isso é bom e ruim. Ruim para a *parachain* que reduz ou interrompe seus serviços; bom para o ecossistema porque garantirá que nenhuma *parachains* tenha um *slot* permanente, a menos que gere o valor necessário para mantê-los funcionando.

Outro aspecto interessante desse *design* é a diversidade de projetos de *parachain*. Por exemplo, se houver 3 redes *DeFi* competindo, é improvável que todas tenham sucesso. Em vez disso, apenas 2 podem obter uma vaga, gerando receita suficiente e boa vontade da comunidade. Nesse caso, a terceira *parachain* será rebaixado para uma *parathread*, enquanto outros projetos não *DeFi* continuam operando na rede. Observe que isso é apenas especulação teórica: o ponto a que me refiro é que esse *design* incentiva a diversificação entre os candidatos à *parachain*.

Uma breve visão sobre *parachains*

Dado que os *slots* de *parachain* são finitos, nem todos os candidatos alcançarão com sucesso o *status* de *parachain*. Além disso, tornar-se uma *parachain* pode não ser necessariamente adequado para alguns projetos. Visto que as *parachains* são desejáveis porque têm acesso ininterrupto à *relay chain* e podem enviar blocos sempre que quiserem, é melhor que projetos que não requeiram esses recursos se tornem *parathreads*. Você pode pensar em *parachains* como um serviço de assinatura, enquanto os *parathreads* são pagos conforme o uso.

No contexto de Polkadot, esse modelo é ideal por dois motivos:

- É fácil para os projetos encerrarem suas operações de *parachain,* pois não precisam perder completamente sua conexão com a *relay chain*.
- É possível que projetos que não consigam adquirir um *slot parachain* ainda se beneficiem da segurança compartilhada de Polkadot.

Como as *parathreads* operarão?

Alguns dos *slots* de *parachain* na *relay chain* serão reservados para execução de *parathreads.* Esses *slots* especiais chamados "*pools* de *parathreads*" hospedarão projetos que desejam se tornar *parathreads.* Para adicionar um bloco na *relay chain*, essas *parathreads* enviarão seu candidato de bloco e uma taxa de transação para um agrupador localizado na *pool* de *parathreads* que, por sua vez, o retransmitirá junto com um lance designado em DOT.

Um validador da *relay chain* revisará os lances e decidirá qual bloco incluir na *relay chain*. O principal incentivo para validadores de *relay chain* é aceitar candidatos de bloco enviados com os lances mais altos, gerando o maior lucro para eles. De acordo com o Wiki Polkadot, "os *tokens* dos lances de *parathread* provavelmente serão divididos em 80-20, o que significa que 80% vão para o tesouro de Polkadot e 20% vão para o autor do bloco. Esta é a mesma divisão que se aplica também às taxas de transação e , como muitos outros parâmetros em Polkadot, podem ser alterados por meio de um mecanismo de governança."

Uma visão geral dos interessantes candidatos à *parachain* (setembro de 2021)

1. Acala - *DeFi*

Acala é o primeiro consórcio financeiro descentralizado de seu tipo com a visão de criar infraestrutura financeira aberta de cross chain para o ecossistema Polkadot. Sua missão é se tornar o *hub DeFi* de Polkadot para facilitar o uso ou a criação de aplicativos financeiros, melhorar a eficiência comercial e economizar tempo valioso. Isso significa que a Acala tem a mesma missão que Ethereum, a única diferença é que ela foi construída especificamente para casos de uso *DeFi*, tornando-a muito mais conveniente para serviços *DeFi*. A plataforma oferece um conjunto de protocolos principais que a tornam um destino digno para qualquer desenvolvedor e usuário de *dApps DeFi*.

a) Protocolo Honzon (aUSD)

Este é o protocolo por trás do aUSD de Acala, que é uma *stablecoin* descentralizada e multi-colateralizada que é apoiada por ativos *cross chain.* Por outro lado, o USDT, a maior *stablecoin* por capitalização de mercado, é uma *stablecoin* centralizada que está sob o controle de um único agente. A DAI amplamente adotada, uma *stablecoin* descentralizada,

atualmente é limitada pelo fato de haver apenas um tipo de garantia que pode ser usada para cunhar, ou seja, ETH. Isso explica por que o DAI tem uma capitalização de mercado muito menor em comparação com o USDT. Assim, o aUSD procura oferecer o melhor dos dois mundos e evitar as limitações das stablecoins populares. Além disso, pode ser cunhado a partir de uma variedade de garantias que incluem DOT, ETH, BTC, KSM e qualquer outro *token* listado na lista de permissões pela governança da Acala.

b) Protocolo Homa (LDOT)

O protocolo Homa é um protocolo de *staking* descentralizado que permite aos usuários obter os benefícios de *staking* de seus DOTs sem perder o acesso à sua liquidez. Então, em vez de fazer *stake* de seus DOTs na *relay chain* de Polkadot, os usuários podem usar o protocolo homa no *dApp* Acala e receber LDOTs em troca,

embora não necessariamente na proporção de um para um. LDOT significa DOT líquido, que os usuários podem usar como garantia para obter empréstimos de *stablecoin*, para transferências ou *swaps*. Quando os usuários desejam resgatar seus DOTs em *stake*, eles podem simplesmente devolver o LDOT ao protocolo e obter seu DOT mais suas recompensas de *staking* reembolsadas em sua carteira imediatamente, evitando assim o período de desvinculação de 28 dias da *relay chain.*

c) Corretoras Descentralizadas

Este é um protocolo semelhante a Uniswap, Sushiswap e outras corretoras descentralizadas que permitem aos usuários trocar *tokens*, fornecer liquidez e ganhar recompensas. O objetivo da Acala é tornar o *DeFi* acessível a todos sem todas as complexidades que acompanham os protocolos descentralizados. Eles já têm uma parceria com a Current, uma *fintech* americana, que ajudará a criar um novo tipo de financiamento chamado "*Hybrid Finance*" (uma mistura de finanças descentralizadas e centralizadas). O que significa que será possível para usuários que não possuem uma carteira de criptomoedas obter rendimentos em *DeFi* de suas contas bancárias tradicionais.

2. HydraDX - *DeFi*

HydraDX, outra *blockchain* de primeira camada focada em *DeFi*, é muito diferente de Acala. Uma parte essencial da oferta de HydraDX é o "*Omnipool*", uma "*pool* de liquidez" profundo e diversificado o suficiente para resistir a qualquer coisa que o mercado jogue nele. Atualmente, a maioria das negociações de *token* é realizada em pares, de modo que, se eu quisesse trocar DOT por KSM, precisaria encontrar uma bolsa que tenha um par DOT/KSM. Só então eu seria capaz de trocar DOT para KSM. Se essa *pool* não existir na corretora, serei forçado a trocar o DOT por um *token* emparelhado com o KSM. Digamos, por exemplo, que eu encontre um par DOT/USDT e um par KSM/USDT, terei que trocar meu DOT por USDT antes de trocar USDT por KSM. Isso não é eficiente em termos de capital nem amigável ao usuário. Mesmo quando corretoras descentralizadas como

Uniswap propõem trocas entre dois *tokens* que não estão emparelhados em uma *pool*, eles fazem isso trocando automaticamente de uma *pool* para outra, o que causa muita *slippage* (oscilação).

Graças ao poder e flexibilidade do Substrate, HydraDX está superando essa limitação construindo uma única *pool* (*Omnipool*) para cada ativo. Os detalhes dessa execução são bastante técnicos, tanto em termos financeiros quanto tecnológicos, mas vou dar um resumo básico aqui. Para criar um *Omnipool*, a HydraDX usa o *token* LRNA como o *token* base contra o qual todos os outros *tokens* serão negociados, para que o *token* LRNA possa atuar como um oráculo de preços. Dado que a HydraDX é uma camada 1, seu *Omnipool* não é tudo o que ele tem a oferecer: em vez disso, é o bloco de construção sobre o qual se empilharão muitos outros aplicativos financeiros.

3. KILT - Identidade

Por muito tempo, nossos dados, principalmente os que nos identificam, têm sido usados para nos prender, manipular e tirar vantagem de nós. A KILT procura desafiar esse estado das coisas, descentralizando o processo de atestar e verificar as credenciais dos usuários.

KILT é um protocolo de identidade *blockchain* de código aberto para emissão de credenciais auto-soberanas, anônimas e verificáveis. A KILT permite modelos de negócios inovadores em torno de identidade e privacidade, atendendo à necessidade de soluções de identidade confiáveis no mundo digital. Ela permite que os usuários reivindiquem atributos pessoais, os confirmem por entidades confiáveis e armazenem as declarações como credenciais auto-soberanas.

No centro de seu modelo está a ideia de que os usuários devem ter total propriedade e direitos sobre suas credenciais, para que somente eles possam usar suas informações de identidade ao interagir com outra parte. Dentro de seu protocolo, há aqueles que precisam de credenciais emitidas (como candidatos a emprego) e aqueles que precisam verificar credenciais (como empresas de contratação).

Assim que a *blockchain* da KILT estiver totalmente configurada e funcionando, será possível provar para uma empresa que deseja contratá-la que você é quem afirma ser. Isso será possível porque a empresa só precisará verificar as informações que você forneceu à *blockchain* KILT. Se eles precisarem de verificação adicional, eles poderão pagar um atestador para verificar suas credenciais. Novamente, esta é a ideia básica. Mas lembre-se de que este é uma *blockchain* de primeira camada e que muitos outros aplicativos de identificação podem ser construídos nela.

4. Robonomics - *IoT*

Na minha opinião, este é o candidato a *parachain* mais interessante da DotSama. Digo isso porque eles estão construindo algo que ninguém mais propôs – a economia dos robôs. O núcleo de sua ideia é a percepção de que, com o surgimento da automação (robôs autônomos), surge a necessidade de uma estrutura para gerenciar as interações

entre robôs. Por exemplo, geralmente há uma *pool* de robôs e máquinas trabalhando juntos para fabricar produtos nas fábricas, mas ainda são necessários humanos para facilitar as operações entre esses robôs.

Por exemplo, quando um item completar um ciclo em uma linha, quase sempre é necessário um ser humano para movê-lo para a próxima linha para continuar o procedimento de fabricação. Nesse caso, um humano só é necessário porque não há como os robôs falarem sozinhos e coordenarem suas ações de forma independente.

Ao adicionar uma linha de comunicação automatizada nas interações dos robôs, um novo mundo de possibilidades se abre para nós: a economia do robô. Com a Robonomics, será possível que um robô de fábrica instrua um veículo automatizado, de modo que, quando os produtos estiverem prontos, o robô da fábrica possa enviar um ping para o veículo automatizado vir buscar. Para evitar *spam* de robôs, o robô de transporte só reagirá à chamada do robô de fábrica se o robô de fábrica tiver pago alguns *tokens* ao robô de transporte.

Para melhor clareza, a palavra “robô” não se refere necessariamente a máquinas humanóides. Qualquer máquina automatizada é um robô: uma impressora, uma máquina de café, um programa de computador em um caminhão, um robô de negociação. Eles são robôs porque são projetados para realizar um certo conjunto de ações automaticamente tendo recebido uma determinada entrada. A Robonomics é muito interessante porque o projeto quer vincular a economia do mundo digital e o mundo real por meio de “robôs”, assim como as finanças fiduciárias e criptográficas são vinculadas por meio de “oráculos”.

5. Phala – Privacidade

Phala aborda a questão da confiança na computação em nuvem. A *blockchain* de primeira camada da Phala é uma plataforma de computação livre de confiança que permite o processamento em nuvem em massa sem sacrificar a confidencialidade dos dados. Em termos leigos, Phala está construindo uma nuvem descentralizada e privada por meio de uma rede de PCs reunidos por meio de consenso de *blockchain*. Phala quer tornar redundantes serviços de nuvem autorizados/*Web2* como Google Drive, One Drive, Adobe Cloud, Azure e AWS. A Phala está comprometida em fornecer uma rede de computação descentralizada universal que pode ser combinada livremente com contratos inteligentes, protocolos de armazenamento descentralizados e serviços de indexação de dados.

Um dos novos produtos da Phala é o *Fat Contract*, uma atualização pretendida no atual modelo de contrato inteligente possibilitado pelo poder e flexibilidade do Substrate, a estrutura usada para construir Polkadot e suas *parachains*. Tradicionalmente, os contratos inteligentes executam seu código *on-chain*, o que significa que a rede *blockchain* é responsável por realizar o cálculo do contrato inteligente junto com o consenso. Mas isso limita o poder dos contratos inteligentes porque eles estão vinculados à capacidade computacional da rede (ou seja, produção de blocos, finalidade etc.). Ao dissociar a

execução de um contrato inteligente do consenso da *blockchain*, um contrato inteligente mais poderoso é criado.

Um Contrato *Fat* é simplesmente um contrato inteligente que lida com sua computação *off-chain*. Isso é combinado com o recurso de preservação de privacidade da Phala, que garante que os dados computacionais não possam ser lidos pelos mineradores. O principal apelo dos Contratos *Fat* é que eles permitem um uso muito mais rico e poderoso de contratos inteligentes para uma ampla gama de serviços, particularmente aqueles que exigem muito poder e velocidade de processamento, como jogos, metaverso e análise de dados, para citar alguns.

6. Crust - Dados

A nuvem foi um ótimo complemento para nossas vidas: não precisamos mais armazenar todos os nossos arquivos digitais em dispositivos pessoais com espaço em disco limitado. No entanto, os dados que você armazena em servidores de nuvem centralizados não pertencem totalmente a você e você não pode ter certeza de que seus dados estarão sempre seguros e acessíveis. Por outro lado, uma nuvem descentralizada tem a vantagem de não depender de uma única nuvem ou serviço de hospedagem.

Crust está fornecendo uma solução de armazenamento em nuvem descentralizada e direta para usuários, profissionais e desenvolvedores comuns. Com Crust, seus dados são armazenados em vários nós em todo o mundo, garantindo que você possa recuperar esses dados em qualquer lugar e a qualquer hora. Além disso, todos os dados armazenados são de propriedade total e só podem ser acessados por você. Isso ocorre porque a Crust faz uso de criptografia avançada de dados antes de enviá-los para seus nós. Em suma, Crust procura desafiar todos os serviços de armazenamento em nuvem centralizados atualmente em operação – Google, Dropbox, Box, etc.

7. Zeitgeist - Futurocracia

Zeitgeist é uma *blockchain* de *primeira camada* que propõe algumas das ideias mais originais do ecossistema Polkadot. A democracia é uma forma ideal de governança, mas tem muitas desvantagens quando se trata de modelos para a tomada de decisões.

Atualmente, existem grandes diferenças de riqueza entre as nações que não podem ser atribuídas a diferenças em recursos naturais ou habilidades humanas. Na verdade, o cerne dessas desigualdades está no fato de que as nações, muitas das quais são democracias, muitas vezes adotam políticas ineficazes. A Futurocracia se apresenta como uma nova forma de governo e quer alterar a forma como as decisões são tomadas utilizando os resultados de um mercado de previsão.

O argumento central da Futurocracia é que os mercados tendem a ser mais racionais e podem ser usados como uma forma autônoma de governança. A Zeitgeist fornece uma *blockchain* de primeira camada que permite que qualquer pessoa crie um mercado de previsão para medir as opiniões das pessoas sobre qualquer tópico, apoiando assim a

formulação de políticas para empresas, governos, comunidades *blockchain*, *DAOs* e outras organizações. Com a Futurocracia, as decisões não serão tomadas com base em opiniões flutuantes, mas em apostas ponderadas em que as pessoas são forçadas a "colocar [seu] dinheiro onde [sua] boca está".

E assim, espera-se que as pessoas sejam mais cuidadosas e honestas com suas opiniões quando houver um custo associado a expressá-las. Pode-se imaginar um futuro em que os parlamentares cheguem a uma decisão com base em como fizeram suas apostas. Vejamos a seguinte pergunta: "A redução de impostos criará mais progresso econômico?" Em uma democracia, todos os membros votariam com base nas opiniões deles ou de outras pessoas; enquanto isso, a Futurocracia exige que todos os membros assumam uma posição financeira sobre se a redução de impostos levará ou não ao progresso econômico. Aqueles com a convicção mais forte provavelmente colocarão mais dinheiro em jogo e influenciarão indiretamente o resultado da votação.

Com quem você iria: as pessoas que têm fé suficiente em sua opinião para correr o risco de fazer uma grande aposta ou aquelas que não são corajosas o suficiente para apoiar sua opinião com fundos suficientes?

Mas nem tudo é sol e arco-íris. Existem algumas desvantagens potenciais no modelo Futurocracia. Algumas pessoas inevitavelmente se distrairão com a parte de jogos / apostas / riscos da Futurocracia para cunhar dinheiro e influência social, ou seja, o fenômeno do *Crypto* Twitter, onde contas 'grandes' usam sua influência para aumentar o preço de *tokens* que não valem seu valor de mercado. Espera-se também que as pessoas acabem seguindo *hypes* e grandes apostas sem nunca formar uma opinião própria, o que seria 100 vezes pior do que a democracia, onde indivíduos apáticos não se preocupam em votar por falta de "incentivo". Assim, a Futurocracia é descentralizada o suficiente para atrair um leque maior de participantes, mas também há um efeito de "jogo" que prejudica a relevância das apostas. Somente na implementação poderemos ver como vai se desenvolver, e é por isso que estou entusiasmado com o futuro do Zeitgeist.

8. Moonbeam - Contratos inteligentes

Moonbeam é uma plataforma de contrato inteligente compatível com que permite aos desenvolvedores implantar contratos inteligentes em Solidity existentes e *DApp frontends* com alterações mínimas no código original. Após o lançamento bem sucedido de sua rede canaria em Kusama (Moonriver), algumas pessoas apelidaram a plataforma de "Ethereum 3.0".

Além da valorização dos *token*s MOVR que, sem dúvida, acompanharão essa denominação, a *tag* não é totalmente desmerecida. Por um lado, a integração suave da Moonbeam com ferramentas nativas do Ethereum o torna um destino fácil para todos os *dApps* do Ethereum; dessa forma, os desenvolvedores podem construir *dApps* mais ricos que não sofrem com as limitações da *blockchain* Ethereum - taxas de *gas* irracionais, falta de modularidade, etc.

Esses são apenas alguns dos muitos candidatos a *parachain* construídos em Polkadot. Abaixo estão os links para alguns recursos úteis sobre projetos do ecossistema:

- https://parachains.info/
- https://dotmarketcap.com/
- https://polkaproject.com/

Um ponto importante a ser observado é que a maioria desses projetos são registrados apenas como *parathreads*. Até que um projeto seja conectado à *relay chain* após vencer um leilão de slot de *parachain*, ele continua sendo um candidato a *parachain*.

No início deste livro, pode ter sido difícil para você imaginar por que precisaríamos de uma variedade de *blockchains*. Espero que esta seção tenha sido bem-sucedida em convencê-lo de que o futuro é verdadeiramente *multi-chain.* De qualquer forma, espero que você tenha apreciado a infinita versatilidade de um protocolo de camada 0 como Polkadot, que visa apoiar a inovação exponencial na qual os futuros desenvolvimentos da primeira camada podem prosperar.

Existem muitos problemas não resolvidos para a humanidade e o planeta como um todo, e o objetivo de toda tecnologia deve ser tornar a vida melhor. Não a vida no sentido estrito da palavra que apenas leva em conta a humanidade – esse é o tipo de pensamento que nos levou à atual crise climática. A vida, como eu a uso aqui, refere-se a plantas, animais, a atmosfera e tudo o que não podemos prescindir. As aspirações das redes e organizações descentralizadas são que as pessoas possam se tornar mais receptivas às questões globais ao longo do tempo: respeitar a vida, promover a liberdade, a paz e a justiça e trazer a prosperidade humana. Se eles não puderem fazer isso a longo prazo, estão condenados a repetir os erros cometidos na *Web* 2.0.

Capítulo 6

PARTICIPANDO DA REDE

Neste ponto do livro, você já aprendeu muito sobre Polkadot. Mas conhecimento por conhecimento não traz qualquer valor: é na aplicação que o conhecimento ganha seu valor. Esse livro foi escrito para apresentar Polkadot de uma forma acessível, para que mais pessoas possam se conscientizar das maravilhas e possibilidades desta rede descentralizada. Mas isso é apenas metade da história. A maior razão pela qual este livro foi escrito foi recrutar novos construtores e embaixadores do ecossistema, porque uma rede é tão boa quanto seus participantes.

Se você está animado ou inspirado pelas oportunidades que estão surgindo no Ecossistema Polkadot, este pequeno capítulo convida você a participar da rede.

Aqui estão algumas razões pelas quais você pode querer participar de Polkadot:

- É verdadeiramente descentralizada.
- É à prova de futuro, graças a atualizações sem bifurcação e governança *on-chain*.
- Tem uma comunidade vibrante e apaixonada.
- Pode acomodar as ideias mais ousadas com sua escalabilidade.
- Alinha-se com valores universais como liberdade de discriminação e censura.
- É um portal para um Paraverso sem limites de primeiras camadas, segundas camadas, contratos inteligentes, *dApps*, pontes e muitos outros novos protocolos.

Assim, ao construir ou participar de Polkadot, você está na vanguarda e no centro da inovação *Web3*. Agora que você está convencido da ideia de participar, vamos considerar como isso funciona na prática.

Como participar da rede

Nesta subseção, veremos quais são suas opções em termos de participação.

Segurança

Uma rede descentralizada só tem valor enquanto permanecer segura e, portanto, a maneira mais óbvia de participar da rede é contribuir para sua segurança. Felizmente, Polkadot é uma rede *Nominated Proof-of-Stake* que dá à pessoa comum a chance de ingressar como mantenedora da rede.

Existem quatro funções distintas disponíveis aqui:

1. **Torne-se um validador** - Isso requer algum equipamento e conhecimento técnico. Ao se tornar um validador, você estará verificando transações e produzindo blocos.
2. **Torne-se um coletor** - Enquanto os validadores protegem a *relay chain*, os *coletores* protegem as *parachains* e as *parathreads*. Você pode se tornar um coletor para sua *parachain* favorita.
3. **Torne-se um nomeador** - Se você tiver *tokens* DOT, você pode simplesmente fazer *staking* com validadores para ganhar recompensas. Existem diferentes carteiras e extensões que você pode usar para esse fim (veja as recomendações abaixo).
4. **Torne-se um mutuário** - Você pode bloquear seu DOT para ajudar uma *parachain* a garantir um *slot* na *relay chain* por um período fixo. Isso permitirá que você obtenha *tokens* nativos da *parachain*, o que é um incentivo adicional para a diversificação do portfólio.

Todas as operações acima podem ser concluídas através da extensão Polkadot-js e *Apps*, as interfaces *web* oficiais da rede. No entanto, a maioria dos usuários não técnicos precisará de alternativas mais amigáveis para iniciantes.

Algumas Recomendações de Carteira para *Staking* e *Crowdloaning*

1. Carteira Talisman e extensão (minha recomendação pessoal)
2. Fearless
3. Nova
4. Polkawallet
5. Mathwallet

Uma breve nota contra corretoras centralizadas

Embora você possa fazer *stake* de seus DOTs e participar de *crowdloans* de Polkadot por meio de corretoras centralizadas como a Binance, Kraken e Coinbase, eu as deixei intencionalmente fora da minha lista de recomendações de carteiras. Isso ocorre porque o uso de corretoras centralizadas para operações *on-chain* vai contra a ideia de descentralização: quando você faz *stake* ou contribui para *crowdloans* por meio dessas corretoras, você efetivamente perde a propriedade de seus *tokens* para a corretora. Isso pode se tornar um problema a longo prazo:

1. Uma corretora centralizada pode usar seus *tokens*, assim como os de outros usuários, para participar da governança e votar em propostas que você não apoia.

2. Uma corretora centralizada pode ser invadida e seus validadores podem ser cortados, o que coloca em risco uma parcela maior dos participantes da rede.

Staking e *crowdloan* através das carteiras que recomendei, garantem que suas ações *on-chain* estejam sempre vinculadas a uma conta que está sob sua custódia, em vez de transferir seus direitos de participação *on-chain* para uma conta controlada por uma empresa terceirizada.

Governança

A governança continua sendo a característica menos popular das redes descentralizadas, com a maioria dos referendos não conseguindo uma participação de 10% dos eleitores. Portanto, sua participação nas atividades de governança estaria dando uma nova vida à rede. Abaixo estão algumas ideias:

1. Concorra ao Conselho
2. Vote nos candidatos e concorrentes do Conselho
3. Faça propostas ou segundas propostas[Y1]
4. Vote em referendos
5. De gorjetas para construtores e embaixadores do ecossistema
6. Participe de discussões no Polkassembly, Element, Discord e Reddit

Você pode encontrar mais detalhes sobre esses processos no Polkadot Wiki.

Crescimento do ecossistema

Se nem a segurança nem a governança da rede lhe agradam, considere tornar-se um construtor ou um embaixador.

Construtor

Um construtor é um indivíduo ou um grupo de indivíduos que está trabalhando na implantação de *parachains*, *pallets*, contratos inteligentes, *dApps* e ferramentas de desenvolvedor. Como construtor, você pode obter financiamento solicitando subsídios da Web3 Foundation ou enviando propostas de gastos para o tesouro *on-chain*. Você também pode entrar no Substrate Builders Program, um programa que identifica, apoia e orienta projetos atuais e potenciais relacionados ao Substrate.

Embaixador

Esta função não deve ser confundida com a posição oferecida como parte do programa de embaixador de Polkadot, ao qual você pode participar preenchendo um formulário de inscrição aqui. A principal responsabilidade/dever de um embaixador é ajudar a impulsionar o crescimento e a adoção da rede. Isso pode ser feito de tantas maneiras quanto a mente puder encontrar, sendo a coisa mais importante o objetivo final. Por exemplo, escrever um livro ou *blog* é uma tarefa digna para esse fim, mas também é

importante gravar um *webinar*, compor uma música, organizar um encontro, criar um audiovisual explicativo, etc. Novamente, sua imaginação é o limite. Se você tiver um projeto do qual acredita que o ecossistema se beneficiará, poderá solicitar financiamento do tesouro *on-chain* através do procedimento descrito aqui. Para contextualizar, este livro foi uma ideia original possibilitada pelos fundos recebidos do tesouro *on-chain* de Polkadot.

Acompanhando o ecossistema

O primeiro passo que você pode dar para participar da rede é manter-se atualizado com os acontecimentos do ecossistema. Abaixo estão os links para alguns recursos importantes que ajudarão você a acompanhar o desenvolvimento do ecossistema.

1. DotLeap

Esta é uma *newsletter* semanal dirigida por Gbaci e Bruno Škvorc. Ele se concentra na publicação das atualizações mais dignas de nota do ecossistema DotSama (Polkadot + Kusama), cobrindo notícias da *relay chain, parachains*, *dApps*, *parathreads*, comunidades e muito mais. É uma visão geral, verdadeiramente abrangente, do ecossistema que é publicada no Substack e no Subsocial todas as semanas. Inscreva-se aqui para atualizações.

2. Parachains.info

Este é o *site* mais limpo e abrangente que encontrei para todas as coisas do DotSama. Ele apresenta informações sobre empréstimos coletivos, leilões e projetos de *parachain*, incluindo oferta e preço de *tokens*, investidores, progresso do roteiro, *status* de concessão da Web3 Foundation e muito mais. Também possui uma aba de notícias que agrega notícias de projetos oficiais das *parachains*. Este é outro projeto liderado pela comunidade que foi financiado pelo tesouro *on-chain*.

3. Dotmarketcap

Este *site* é semelhante ao parachains.info no sentido de que agrega informações sobre projetos do ecossistema Polkadot, candidatos a *parachains* e leilões. Ele fornece uma lista de projetos negociáveis classificados por valor de mercado e algumas ideias valiosas. Sua maior vantagem é que todas as informações sobre preços de *tokens* e *crowdloans* são atualizadas instantaneamente e você pode usar o site para acompanhar uma seleção de projetos que lhe interessam.

4. *NFT* Review

Esta é outra newsletter semanal dirigida por Bbaci e Bruno Škvorc, com um forte foco em *NFTs* e Metaverso. Tem o benefício de cobrir as notícias *NFT* da DotSama e do restante do espaço da *Web3* e está disponível para assinatura aqui.

5. *Blog* Polkadot

Este é o *blog* oficial administrado e mantido pela Web3 Foundation. As atualizações não são frequentes e por isso é aconselhável que assine o *blog*. Naturalmente, se você estiver inscrito no DotLeap, receberá uma atualização sobre os artigos mais recentes do *blog* sempre que eles forem publicados.

6. Polkadot Dayle Digest

O resumo diário é escrito quase todos os dias por Bill Laboon, Diretor de Educação e Comunidade da Web3 Foundation. O resumo inclui atualizações importantes de Polkadot e Kusama sobre a *relay chain,* governança e discussões da comunidade. Você pode encontrá-lo em Polkadot e no Subsocial.

7. DotTreasury

Este é um ótimo *site* para encontrar informações sobre o tesouro Polkadot. Fornece informações sobre reservas de tesouraria, receitas, despesas e outras informações relacionadas à tesouraria.

8. Polkadot A to Z

Esta é uma série educacional de Emre Surmeli, Educador Técnico da Web3 Foundation. Fornece informações técnicas básicas sobre as tecnologias Polkadot e Substrate, um conceito por vez. O conteúdo é apresentado em um formato curto e compreensível. Atualmente está no Reddit.

9. Guia para Polkadot.JS

Esta é uma apresentação muito abrangente das funcionalidades da Polkadot-JS e extensão. Criado por Anaelle LTD, um membro da comunidade. Ele fornece instruções passo a passo para tornar as operações da carteira acessíveis a iniciantes e está disponível neste *site*.

10. Ser, Have ya ‘Herd?

Esta é uma série educacional de vídeos diários de Jay Chrawnna, um membro da comunidade. Ele divide e discute as últimas notícias e desenvolvimentos no ecossistema DotSama em um formato muito divertido para o público em geral. Atualmente está hospedado no Youtube.

E isso é tudo, pessoal! Bem-vindo ao Paraverso.

APÊNDICE TÉCNICO

A BABE e a GRANDPA

(*Observe que, devido ao recurso de atualização sem bifurcação de Polkadot, este mecanismo de consenso está sujeito a alterações no futuro*).

Antes de falar de BABE e GRANDPA, preciso explicar uma coisa sobre protocolos de computador.

Primeiro, lembre-se sempre de que uma *blockchain* é um protocolo. Mas o que é um protocolo? Um protocolo é um conjunto de instruções que um *software* de computador opera. É possível confiar em um protocolo porque suas regras são claras desde o início. Você pode pensar em um protocolo como um conjunto de ações automatizadas que um computador executa.

Agora, a coisa vital que você precisa saber sobre protocolos é que ele pode ter muitos protocolos e sub-protocolos dentro dele. Tal que quando dizemos que uma *blockchain* é um protocolo, realmente queremos dizer que uma *blockchain* é um protocolo de sub-protocolos, com cada sub-protocolo equipado com a capacidade de ter outros sub-sub-protocolos. Cada subprotocolo e sub-sub-protocolo é responsável por uma tarefa específica.

Assim, no caso da *relay chain* de Polkadot, que é em si um protocolo, existem vários sub-protocolos e sub-sub-protocolos. É por isso que temos tanto o BABE quanto o GRANDPA como subprotocolos da *relay chain*

Com isso fora do caminho, agora podemos ser apresentados ao BABE. Para nerds que sabem ler código, ele é bem sexy. Mas para nós novatos, ele é apenas um BABE, embora poderoso.

BABE - Atribuição cega para extensão de bloco

BABE é um subprotocolo na *relay chain* que coordena a produção de blocos. Para fazer isso de maneira segura e descentralizada, ela usa alguns truques legais:

Atribuição às Cegas ou Seleção Aleatória

O primeiro truque na manga é o processo de atribuição às cegas. Existem duas maneiras de determinar qual nó criará o próximo bloco – aleatoriamente ou de forma determinística. Se um nó souber com antecedência que fornecerá um número x de blocos, esse nó terá tempo suficiente para criar transações falsas para inclusão nesses blocos. Assim, BABE escolhe aleatoriamente. Desta forma, os nós não sabem de antemão quais blocos irão produzir. O mecanismo específico é muito técnico para ser explicado neste livro, apenas lembre-se de que nosso BABE seleciona nós aleatoriamente para produzir blocos. Outra razão pela qual não quero entrar em mais detalhes neste livro é que há um boato de que ele está de saída. Seria muito lamentável gastar tanto tempo quebrando sua complexidade apenas para ter que fazer emendas menos de um ano depois.

Múltiplas Atribuições também conhecidas como Criação de Backups

Para garantir um maior nível de descentralização, o BABE fornece a diferentes nós o mesmo bloco para produzir. O objetivo é tornar a produção de blocos competitiva para que, no caso de conflito entre diferentes nós sobre a validade de um bloco, todos os nós possam votar em qual bloco é mais provável que seja válido de acordo com parâmetros predefinidos - lembre-se, é um protocolo.

Outra boa vantagem de várias atribuições é que, às vezes, um nó que foi escolhido para criar um bloco pode ficar offline ou ter outros problemas que o impeçam de criar um bloco. Quando isso acontece, sempre haverá um bloco secundário produzido no qual a rede pode fazer *fall back* (recuar). E assim, para cada bloco esperando para ser criado, existe um produtor de bloco primário conforme determinado pelo BABE e vários produtores de blocos secundários.

Existem outros subprotocolos no BABE, mas os que listei são os mais notáveis. Qualquer informação adicional só nos levará a mergulhar fundo no território técnico. Para isso, recomendo a leitura do seguinte artigo de pesquisa sobre BABE.

GRANDPA - O *gadget* de finalidade

Como o BABE, GRANDPA é outro sub-protocolo. Mas, ele está focado na finalidade – verificando se os bloqueios são válidos e não podem ser revertidos. Em suma, onde o BABE ajuda a rede a criar blocos de forma descentralizada, o GRANDPA ajuda a finalizar blocos de forma descentralizada. Ele faz isso executando eleições em todas as várias opções de bifurcação.

Como o BABE seleciona diferentes nós para produzir o mesmo bloco, sempre há uma dúvida sobre qual sequência de blocos é verdadeira. Isso ocorre porque o BABE cria alguns blocos e suas bifurcações associadas antes que o GRANDPA chegue. Então, o trabalho do GRANDPA é decidir qual bifurcação da cadeia é a mais válida.

Você provavelmente está se perguntando: “Então Polkadot também tem bifurcações?!” Bem, um termo mais adequado para essas bifurcações em nosso contexto seria “*faux-forks*” (bifurcações falsas), porque elas ainda não foram finalizadas. Uma vez que

uma bifurcações é finalizada, todas as outras são abandonadas e todos os nós da rede aceitam a decisão do GRANDPA. Mas como o GRANDPA toma sua decisão e como podemos confiar nele? Bem, por um lado, ele é um protocolo e, portanto, só faz o que foi instruído a fazer. Vou explicar esse ponto, evitando o máximo de detalhes técnicos que puder.

Quando várias bifurcações surgem na cadeia, a decisão do GRANDPA sobre qual bifurcação se tornará a cadeia finalizada é guiada por:

1. Sua conexão com o último bloco finalizado - Qualquer uma das opções de bifurcação provenientes do último bloco finalizado pelo GRANDPA é considerada válida o suficiente para permanecer uma opção.
2. Seu número de blocos primários - Qualquer uma das opções de bifurcação com o maior número de blocos primários recebe um peso maior. O bloco primário é aquele que foi criado pelo nó considerado como nó primário pelo BABE no momento em que o referido bloco estava em produção. Lembre-se que o BABE escolhe diferentes nós para criar o mesmo bloco, e que um nó é sempre primário enquanto os outros são chamados de secundários.

Armado com esses requisitos, o GRANDPA pode escolher o bloco que mais corresponder a esses critérios de finalidade.

Em suma, o objetivo principal do BABE e do GRANDPA é oferecer à *relay chain* uma maneira descentralizada de alcançar consenso e finalidade, ou seja, segurança. Uma maior descentralização é sempre favorecida porque garante que a rede estará operando sobre a verdade compartilhada e não na falsidade centralizada. Se todos os maus atores tentassem manipular dados *on-chain*, eles teriam uma tarefa quase impossível de cumprir.

SOBRE O AUTOR

Gbaci é um escritor, cineasta e músico apaixonado por descentralização e o ecossistema DotSama.

Ele começou seu mergulho profundo nas tecnologias *blockchain* em dezembro de 2020 e desde então se tornou um Embaixador da Polkadot, *Head Content* escritor da RMRK e co-editor da *NFT Review* e DotLeap – um boletim semanal sobre todas as coisas de Polkadot e Kusama.

Gbaci acredita que “RMRK será o único padrão *NFT* usado por todos." Ele produz música profissionalmente sob o apelido de Gillian Baci e lançou sua música na Singular na forma de coleções multimídia combináveis.

Quando não está falando sobre cripto ou compondo música, **Gbaci** escreve romances e roteiros, faz filmes, lê livros e brinca com novas ideias sobre como criar um impacto duradouro.

Como cidadão global, acredita que tudo está conectado e que somos todos um em nossas sociedades e no universo em geral.

Você pode encontrá-lo no Twitter sob o nome **@gbaciX.**