Estar conectado num mundo barulhento

Em qualquer espaço novo e em desenvolvimento, é provável que haja muito ruído. As novas soluções tanto concorrem por um novo mercado contra os monopólios existentes (que atualmente detêm o mercado), como contra outras que as tentam eclipsar.

Difícil de entender

Isto é especialmente verdade em relação às inovações/descobertas que mudam o nosso mundo e nos forçam a usar uma nova lente para o compreender. Os preconceitos anteriores tornam-nos menos propensos a investigar as novas invenções numa base de princípios iniciais. Os dados são um legado dos nossos modelos existentes – não os novos. Estes precisam de ser intuidos para prever o que vai acontecer, em vez de serem previstos com dados históricos. Simplificamos os modelos no nosso cérebro para poupar tempo e, como resultado, a maioria das pessoas cai na armadilha de prever o seu comportamento futuro olhando para o seu passado.

É por isso que ao usar um telemóvel Blackberry quando o iPhone foi lançado, não podíamos prever como as nossas mentes mudariam – e a mudança das mesmas devido ao novo valor criado, mudaria uma indústria. Movemo-nos instantaneamente quando nos é dado algo de maior valor, e é impossível prever esse movimento antes de o "vermos".

É também por isso é que a Kodak foi destruída pela câmera digital que a própria marca criou, e a Blockbuster não conseguiu ver a ameaça da Netflix até ser tarde demais.

E é a mesma razão pela qual todos os monopólios falham quando entendem mal a criação de valor entregue à sociedade pelas novas tecnologias. A adoção de tecnologia é, na maioria das vezes, de baixo para cima, não de cima para baixo. Isto porque as pessoas mais afastadas do poder de monopólio têm mais a ganhar, e as outras mais a perder.

Acrescente-se que há sempre um número muito maior de pessoas mais afastadas do monopólio do que perto dele, e torna-se fácil ver a rapidez com que algo que cria mais valor para essas pessoas pode tomar posse e ficar mais forte — tornando um monopólio impotente na sua luta.

Nota — Este quadro é importante a considerar, independentemente de o monopólio estar dentro de uma indústria, ou se se aplica ao próprio dinheiro.

Mais difícil de entender

É ainda mais difícil compreender tecnologias de propósito geral, como a Inteligência Artificial, que afetam todas as indústrias ou preveem a sua taxa de progresso. Como estas tecnologias de Propósito Geral se aplicam à maioria da **criação de valor** ao longo do tempo, podemos facilmente subestimar o impacto correspondente em cada negócio e, por sua vez, nas nossas vidas. Por exemplo, fingir que uma inteligência artificial estrita ou geral não terá um dia um impacto negativo no nosso

trabalho um dia, é algo em que queremos acreditar, o que garante que as narrativas que suportam essa linha de pensamento sejam populares – mesmo que falsas.

Ainda mais difícil de entender

Mas as inovações que são mais difíceis de entender são tecnologias abertas de nível de protocolo e descentralizado. Estes protocolos criam valor sob a forma de uma nova fundação que emerge lenta e metodicamente. Os protocolos são construídos em camadas, o que significa que geralmente não podemos ver o que é possível na camada seguinte até que esta já esteja construída. O protocolo de tecnologia da camada base (camada 1) que permitiu que os computadores fossem ligados em rede chama-se TCP-IP (Transmission Control Protocol, e o Internet Protocol) e foi desenvolvido pela DARPA no final dos anos 1960. Só em 1989 é que Tim Berners-Lee inventou o HTTP (Hypertext Transfer Protocol) na camada 4, que ligaria esses computadores e páginas *web* e formaria uma rede mundial.

É por isso que se tentasse explicar a camada de protocolo aberto TCP-IP que permitiu que computadores anteriormente isolados comunicassem uns com os outros, ou mesmo HTTP (Hypertext Transfer Protocol) a alguém no início dos anos 1990, ou tentasse dizer-lhes que um dia essa mesma tecnologia (largamente inalterada) daria origem ao iPhone, Google, Zoom, a Amazon, e tudo o mais que hoje damos por garantido, os seus olhos revirar-se-iam em descrença.

Experimentamos valor através de produtos e serviços que nos dão valor, em vez de tentar compreender os intrincados detalhes da canalização que dá origem a esses produtos e serviços.

Vou tentar usar um quadro para considerar como isto se aplica à Bitcoin e ascensão previsível de Altcoins, Finanças Descentralizadas (DeFi) Web 3, Metaverso, e todo o espaço das blockchain.

Mas antes disso, temos de começar a um nível mais alto porque a abstração de nível superior afeta e amplifica tudo o resto.

Temos de começar pelo dinheiro. Temos de começar por aí pela mesma razão acima referida.

Nomeadamente:

1. Experimentamos valor através de produtos e serviços que nos dão valor, em vez de tentarmos compreender os detalhes intrincados da canalização que dá origem a esses produtos e serviços, e
2. O dinheiro é a camada de fundação que dá origem a tudo o resto.

Por conseguinte, quando o dinheiro se avaria, ficar de pé quando o chão ceder, pouco contribuirá para a segurança.

Dinheiro é apenas informação.

Isto pode ser difícil de ver porque o dinheiro é informação importante, mas não desejamos mais pedaços de papel (ou as unidades digitais de representação). Desejamos o sentimento que experimentamos ao ter aqueles pedaços de papel e o que eles nos permitem comprar, sejam segurança, um legado na forma de dar aos nossos filhos, férias, estatuto, uma casa ou apenas liberdade. O dinheiro é apenas a informação (um livro-razão) que nos permite medir o que temos, e o que é necessário (nas nossas mentes) para alcançar o resultado desejado. O medo, a ganância e o desejo humano de querer mais surgem acima desse livro-razão e comparação com outras pessoas.

Faz sentido, então, que 1) se o dinheiro é apenas informação e 2) está a ser manipulado pelos bancos centrais a uma taxa sem precedentes para evitar um colapso de crédito do sistema, então 3) a desinformação DEVE estar a crescer em todo o sistema (uma segunda ordem derivada dessa desinformação é que a confiança DEVE estar em declínio em todo o sistema).

Mas este é o sistema infeliz em que vivemos, e tem consequências muito negativas. Porque medimos um sistema dentro do sistema, para a maioria da população isso torna a verdade virtualmente impossível de ver. Da mesma forma, todas as empresas, organizações e partidos políticos são compostos por pessoas semelhantes entre si que medem o sistema a partir do sistema, enquanto todos os membros da sociedade acreditam que podem ver através desta desinformação melhor do que os outros.

(*Caveat emptor* — Embora eu faça o meu melhor para ir mais fundo em questões para entender ambos os lados e onde eu possa estar errado, isto inclui-me a mim, e as palavras nesta página)

Por consequência, é completamente lógico ver reinar as teorias da conspiração, a confusão, a polarização, parcialidade dentro e fora do grupo, e caos social.

Essa desinformação sob a forma de dinheiro não cria apenas polarização. Uma vez que o dinheiro liga valor entre pessoas e nações, o resultado é uma tremenda má afetação de capitais e recursos, já que os atores individuais do sistema pioraram o mesmo com as suas ações para ganhar dinheiro suficiente para escapar dele. Perseguindo retornos cada vez mais altos, não foi só o público. Mesmo os planos de pensões, que precisam de certos retornos de crescimento para se manterem solventes para pagar as responsabilidades sob a forma de benefícios de reforma, começaram a procurar rendimentos "reais" mais elevados. Todos eles, e também nós, à procura de formas de resolver um problema de crescimento para escapar ao próprio sistema que cria o problema.

Num mundo assim, seria fácil cair numa armadilha de pirâmide e ficar rico em esquemas rápidos para escapar. Com efeito, a própria estrutura de manipulação do dinheiro (informação) e a correspondente estrutura de incentivos asseguraria que um mercado crescesse a abusar dele – tanto no mercado criptográfico como no geral. Todos os que medem e tentam criar valor a partir deste sistema contribuiriam, inconscientemente, para uma maior insegurança. Ninguém ficaria isento. Todos, à procura de um retorno maior para

escapar à degradação existente das moedas, aglomeraram-se em mercados que, por sua vez, prejudicam outros.

Com esta 1) desinformação como pano de fundo e 2) uma nova tecnologia de camada de protocolo emergindo (lembre-se de que os protocolos abertos fornecem mais valor para a sociedade e são os mais difíceis de entender), seria extraordinariamente difícil perceber por que razão a Bitcoin se destaca apenas como uma tecnologia inovadora e para onde se dirige. Por extensão, seria relativamente fácil neste ambiente, para os atores mal informados, ou maus, confundirem Bitcoin com Crypto, Web 3, DeFi, Blockchain, Metaverse, e outras convenções de nomenclatura para obter uma vantagem para a sua oferta. Um mercado público que 1) acreditava que estes eram semelhantes entre si, e que assistia a uma subida meteórica do bitcoin nos últimos 13 anos (enquanto simultaneamente se perdia o poder de compra nas outras moedas), e 2) sem tempo para fazer pesquisas profundas, seriam alvos fáceis para imitadores, burlões e até atores bem intencionados que poderiam estar mal informados, assim promovendo a próxima grande cena.

Isto atuaria para amplificar os ciclos de altos e baixos do Bitcoin e ofuscar a sua verdadeira natureza. Em primeiro lugar, ao trazer mais alavancagem, hipótese e re-hipótese para o espaço global, alavancando o bitcoin (que não tem risco de contraparte) como um ativo portador imaculado e amplificando o preço do mesmo no caminho para cima. E em segundo lugar, tal como cada as outras *altcoins* e esquemas de DeFi a elas associadas, caiu devido a essa mesma alavancagem, criando "corridas bancárias" que ampliariam a queda de preço do bitcoin (em termos de dólares americanos), uma

vez que o ativo do portador imaculado (BTC) foi vendido num mercado em falência para cobrir perdas.

À medida que o mercado de dinheiro muito maior se decompôs (o Balanço Mundial é hoje aproximadamente 4 ordens de magnitude maior do que o limite de mercado do bitcoin) e a Reserva Federal e outros bancos centrais se aliviaram ou apertaram em termos fiduciários, isso só ampliaria todo o processo aqui descrito e criaria confusão adicional.

Com esse pano de fundo, fornecerei um quadro simples para explicar por que razão o bitcoin não é igual na sua conceção, para que outros possam usar o mesmo e decidir por si próprios. Espero que, compreendendo as contrapartidas necessárias para a conceção de qualquer cadeia de blocos, o público e/ou os decisores políticos possam compreender com mais precisão as mesmas e ver o sinal através do ruído. Ao fazê-lo, mostrarei também porque é que a ascensão das cadeias de blocos e *altcoins* concorrentes são previsíveis, as vantagens e desvantagens e porque é que, na minha opinião, cada uma acabará por falhar.

Escolha quaisquer 2 lados do triângulo. Mas escolha apenas 2:

O “trilema” da blockchain

Fonte: ego death capital/escalável/descentralizada/segura

Descentralização, Segurança, Escalabilidade

Bitcoin (na camada 1) resolveu (a) Descentralização e (b) Segurança. Nunca na história a sociedade teve a descentralização e a segurança juntas. Treze anos após a sua descoberta/invenção pelo pseudónimo Satoshi Nakamoto e independentemente da quantidade de estados-nação, desafios económicos, ou FUD (Medo, Dúvida incerteza) que lhe tenham sido lançados, ele permanece descentralizado e completamente seguro. Este é um maior negócio do que parece à primeira vista. Como a sociedade ao longo do tempo nunca pôde contar com a descentralização e a segurança em conjunto, era preciso ter confiança nas instituições e no estado de direito (para manter essas instituições sob controlo) para proteção. A Magna Carta, a Declaração

da Independência e muitos outros documentos deste género ao longo do tempo consagraram direitos aos cidadãos, mas também aos governantes no sentido de os controlar. Num horizonte temporal mais longo, o dinheiro ultrapassa as leis, pelo que estas por si só não podem resolver a confiança. Elas mudam ao longo do tempo, garantindo que aqueles com acesso a dinheiro, ou as reescrevam ou prevaleçam em tribunal. Um reflexo do mundo em que vivemos mostra esta infeliz verdade. Ou seja, onde o dinheiro é mais quebrado, o Estado de Direito quebra!

O Estado de direito não protege os cidadãos da manipulação do dinheiro, mas sim os mais próximos da manipulação.

O bitcoin permanece descentralizado e seguro devido à sua conceção. Dois elementos críticos estão na origem disso. 1) Um tamanho de bloco limitado e 2) e a utilização de energia para proteger a rede através de uma prova de trabalho. ***Elementos adicionais da conceção ligados a estes 2 elementos continuam a ser críticos para a segurança e descentralização da rede. Para o leitor que quiser ir mais ao fundo da questão, estes serão explorados mais adiante nesta publicação com hiperligações para alguns grandes líderes de pensamento e conteúdos**. É importante lembrar que o bitcoin é de código aberto, o que significa que está aberto a todos (para auditar ou usar livremente), não é controlado por ninguém, e está livremente disponível para ser mudado por qualquer pessoa através de um garfo para tentar conceber de uma forma diferente que crie mais valor para os utilizadores.

Ao ser concebido de tal forma, o Bitcoin ao longo dos últimos 13 anos tornou-se uma excelente reserva de valor, mas também permaneceu

em grande parte inviável para ser usado como moeda ou pilha de tecnologia mais ampla devido à sua falta de velocidade de transação a 5-7 transações por segundo (na primeira camada). A velocidade de transação não era a única limitação. Ao manter o tamanho do bloco pequeno para garantir a descentralização contínua, o bitcoin deixou uma abertura para as cadeias de blocos/*altcoins* concorrentes para fazer mais na camada 1. Sendo um capital de risco, empresários e promotores de desenvolvimento correram para este ecossistema porque 1) inventando uma nova moeda que pudesse competir com #Bitcoin, conseguiriam lucros maciços a curto prazo para os seus fundadores e apoiantes de capital de risco, e 2) com um maior tamanho de bloco e uma cadeia de blocos mais permissiva, mais poderia ser feito. Estas cadeias de blocos concorrentes dariam origem a contratos inteligentes, fichas não fungíveis (NFTs) e financiamento "descentralizado".

Seria fácil mostrar a Bitcoin como tecnologia antiga, em vez de uma camada de protocolo a um público que procura escalabilidade e outros casos de utilização. Essa mesma escolha, porém, quer por a sua velocidade de transação quer por fornecer mais capacidade através de contratos inteligentes na camada 1, *exigiu* que essas cadeias de blocos sacrificassem a descentralização ou a segurança, para atingir os seus objetivos.

Poderá ver por uma longa história de cadeias de blocos concorrentes que *todos* se tornam centralizados (através de um conselho ou um pequeno número de pessoas/nós que tomam decisões para todos) ou ficam vulneráveis a ataques/falhas à medida que escalam.

Bitcoin é único na descentralização e segurança.

Porquê? Porque simplesmente não há como contornar a escolha de 2 de 3 para uma cadeia de blocos na camada 1.

A conclusão lógica, porém, é que se se sacrifica a segurança pela escalabilidade, a cadeia de blocos falha porque é insegura, ou se se sacrifica a descentralização pela escalabilidade, uma cadeia deve eventualmente tornar-se inútil por razões económicas. E embora se possa argumentar que do ponto de vista de um ecossistema que parece fornecer valor para uma janela de tempo, as compensações económicas de gerir uma cadeia que é centralizada asseguram que não pode funcionar a longo prazo. Dito de forma simples, se a centralização for uma exigência da conceção, uma base de dados é uma solução muito menos dispendiosa — em termos de economia e utilização de energia. Essa razão económica por si só nega qualquer benefício a longo prazo (para além dos primeiros titulares de fichas) de uma cadeia centralizada para os participantes do sistema porque alguém precisa de pagar por ela.

Isto assegura que todos os projetos construídos paralelamente a estas cadeias alternativas (Web 3, Metaverse, NFTs, etc,), independentemente da intenção dos fundadores dos mesmos, devem sofrer o mesmo destino que a cadeia subjacente.

Erguer algo sobre areia movediça não é uma boa estratégia a longo prazo.

Algumas perguntas rápidas para maior clareza:

1) Como é que pode ocorrer financiamento descentralizado numa cadeia de blocos controlada centralmente?

2) Como é que a promessa da Web 3 seria diferente do poder de monopólio atual em tecnologia se fosse construída sobre uma camada base que fosse mais dispendiosa e controlada por muito poucos?

3) Qual é o valor a longo prazo de uma cópia digital (NFT) de algo ligado a uma cadeia que falha?

4) Se existisse uma alternativa de menor custo (através das camadas 2 e 3) E descentralizada que permitisse às empresas de jogos e realidade virtual controlarem o seu próprio destino em vez de arriscarem o seu futuro numa cadeia controlada centralmente, o que escolheriam estes empreendedores? Não seria mais provável que este novo protocolo, em vez de um centralmente controlado, formasse a base do "metaverso"?

O tempo todo, os empresários que constroem para essas cadeias, o público e os reguladores podem desconhecer a natureza a longo prazo da vulnerabilidade. Pior ainda, o capital e os grandes detentores dos vários esquemas de moedas alternativas podem tornar-se participantes dispostos ou relutantes num regime de incentivos perversos em que enriquecem ou saem mesmo a tempo, às custas do público desconhecedor. A famosa frase de Charlie Mungers "mostra-me um incentivo e eu mostro-te um resultado" aplica-se bem aqui. Se

o capital investido (por capitalistas de risco) e o tempo (por um empresário ou equipa) foram para a conceção de uma destas cadeias ou uma empresa suportada por uma delas, a natureza humana diz-nos que é muito mais fácil ofuscar a verdade para vender a um licitador superior antes de esta colapsar do que admitir uma estratégia errada.

Como sempre, siga o dinheiro.

A linha torna-se particularmente distorcida por trocas que oferecem estas moedas a um público desconhecido. Ao oferecer uma multiplicidade de títulos (*altcoins*) – 20.000 – e contando que todos eventualmente sofrem um destino semelhante, criam uma enorme riqueza às custas da sociedade. Por exemplo, fazendo taxas de transação na entrada e na saída, sempre que alguém negoceia qualquer uma destas 20.000 moedas. Um negócio de baixo risco, possibilitado por um público altamente suscetível. Essa mesma riqueza é então usada para defender/pressionar os governos a políticas favoráveis que lhes permitam operar. Veem-se oportunidades de investimento e emprego das maiores bolsas, ao mesmo tempo que se acredita que o bitcoin e as *altcoins* são de natureza semelhante, garante que os decisores políticos sejam facilmente influenciados. Muito disto contribui para que o público e os meios de comunicação estejam completamente desinformados sobre a Bitcoin e a Prova de Trabalho.

Porquê? Porque confundir Bitcoin, cadeias de blocos e *altcoins* é fundamental para os lucros operacionais.

Um mergulho mais profundo nos 3 lados da pirâmide.

O “trilema” da blockchain

Fonte: ego death capital/escalável/descentralizada/segura

1) Segurança

Através da Prova de Trabalho, a Bitcoin oferece aos mineiros uma forma de competir para resolver quebra-cabeças criptográficos para verificar novas transações na cadeia de blocos. Os mineiros compram o *hardware* mais recente para competir pela Bitcoin sob a forma de prémios de blocos. O prémio segue um calendário de redução para metade, sendo programaticamente reduzido a cada 210.000 blocos. A partir de 2009, a 50 bitcoins por nova transação verificada na cadeia (aproximadamente a cada 10 minutos) para 25 bitcoins em 2013, para 12,5 em 2016, para 6,25 BTC hoje, e a ser reduzida para metade a cada 210.000 blocos até ao ano 2140. Na concorrência natural que surge no mercado livre com outros agentes económicos que tentam "ganhar" o

bitcoin, cria-se um incentivo onde os mineiros ganham bitcoins assegurando a rede. Como os custos primários da mineração são 1) o *hardware* (necessário para resolver os quebra-cabeças criptográficos) e 2) os custos energéticos intensivos para executar o *hardware*, os mineiros são incentivados através da concorrência para obter uma vantagem sobre outros mineiros que adicionam taxa de *hash* à rede (a taxa de *hash* é a potência computacional total que assegura a rede).

Satoshi desenvolveu uma nova forma de proteger a rede e aproveitar a teoria dos jogos à medida que a rede se desviou e fluiu com as mais recentes melhorias de *hardware*, permitindo uma computação mais rápida, e novos nós a serem adicionados ou removidos da rede. Essa solução foi denominada "ajustamento da dificuldade". Nela, a rede ajusta automaticamente a dificuldade a cada bloco de 2016, com base no tempo que demorou a minar os últimos blocos de 2016, para manter o tempo *médio* para encontrar o bloco seguinte em 10 minutos. Isto tira partido da ganância e do medo num mercado livre de agentes económicos que trabalham no seu próprio interesse para obter ganhos, para equilibrar e proteger constantemente a rede. À medida que mais poder de computação é adicionado à rede, o ajuste da dificuldade torna automaticamente mais difícil encontrar os próximos blocos de 2016 e, inversamente, à medida que a potência da computação é removida, a dificuldade ajusta-se automaticamente para facilitar a procura dos próximos blocos de 2016. Este processo cria operações mineiras mais e menos lucrativas que tiram partido do mercado livre. Por exemplo, quando a China instituiu a proibição de toda a mineração de bitcoin em maio de 2021, a taxa de *hash* bitcoin caiu durante um período de dois meses, passando de aproximadamente 185 milhões de *hashes* de terra por segundo para

58 milhões por segundo. A cada 2 semanas, a dificuldade é ajustada para baixo para manter o tempo médio do bloco em 10 minutos. Com menos mineiros a competir por prémios, e um excesso de equipamento mineiro recentemente disponível a atingir o mercado, criando uma pressão no sentido da descida dos preços do equipamento, a mineração tornou-se muito mais rentável. Por sua vez, muitas empresas norte-americanas apressaram-se a preencher o vazio (e a oportunidade económica) que a China criou. Seguiu-se uma "corrida ao ouro" para a mineração. À medida que mais agentes económicos se apressavam a tirar partido de lucros fáceis, e a dificuldade de ajustamento era maior, os lucros racionalizavam-se mais uma vez.

E assim, independentemente de um ataque de um Estado-nação, ou de um ciclo de *boom-bust* impulsionado pela ganância e pelo medo, a rede, globalmente, está sempre protegida através do ajustamento da dificuldade em criar um incentivo natural para ganhar uma parte maior de um prémio económico. À medida que mais entradas no mercado concorrem para aproveitar a maior oportunidade de lucro criada por uma taxa de dificuldade mais fácil, acrescentam segurança adicional à rede — por sua vez, levando a taxa de dificuldade mais alta e os seus lucros mais baixos (a taxa de *hash* bitcoin é atualmente de 212 milhões de *hashes* terra).

Além disso, o processo de pagamento de equipamento adicional, que com o tempo se torna obsoleto, à medida que o novo equipamento se torna superior, é dispendioso. Isto tem o efeito de apoiar novos operadores/ideias no mercado. Ou seja, a sua própria natureza reduz

as tendências monopolistas de um mercado para se consolidar em torno de alguns grandes mineiros e fixar o preço de outros.

Os ciclos ascendentes e descendentes da mineração de bitcoin devem ser encarados como a concorrência do mercado livre para uma vantagem num mercado perfeitamente transparente com cada ator racional, na sua própria mente tentando encontrar uma vantagem (o que leva à inovação energética – ver abaixo), durante todo esse tempo assegurando a rede como um subproduto desta concorrência natural.

Energia (como parte da segurança)

Embora muitas pessoas acreditem falsamente que a Bitcoin e a forma como usa a Prova de Trabalho para validar blocos é má para o planeta devido à energia usada para assegurar a rede, a verdade é que Bitcoin é a *única* coisa que encontrei que permitirá uma transição para um sistema de alinhamento planetário e abundância. Como já disse muitas vezes, a abundância no dinheiro cria escassez em todo o lado, e a sua escassez cria abundância.

Ao mais alto nível, isto deve-se ao facto de o atual sistema económico para o planeta ser incongruente com o local onde a tecnologia nos está a levar e a vida num planeta finito.

Como explicado em *O Preço do Amanhã - Por que a Deflação é a chave para um futuro abundante*, e em *O Maior dos Jogos,*

Um conflito tem de ser resolvido a nível do sistema.

1. O aumento exponencial da eficiência impulsionado pelo progresso tecnológico **requer** *uma moeda que permita a deflação (#Bitcoin).* Obtemos mais, por menos trabalho.

2. O sistema monetário fiduciário existente **requer** *inflação e, por conseguinte, necessita de manipulação para se manter viável.* Recebemos menos, por mais trabalho.

Como o sistema existente é baseado no crédito, não pode permitir uma deflação contínua sem um colapso total (pois o crédito seria eliminado e o crédito é o sistema). A sociedade nunca votaria para ter todo o seu modo de viver em colapso. Isto significa que existe um paradoxo em que a sociedade irá sempre insistir em manipular o "crescimento" com medo das consequências do colapso, e que o crescimento manipulado é a principal fonte dos problemas com que a sociedade está a lidar – incluindo os danos ambientais.

Em última análise, isto porque em vez de permitir que os preços caiam (e a sociedade ganhe tempo e liberdade) com o aumento da produtividade, pressupõe que podemos "crescer" para sempre. E o crescimento em si pressupõe que o dinheiro pode ser criado do nada para alcançá-lo. Este "crescimento", para que mais empregos possam pagar as contas, para pagar preços mais elevados, que são manipulados para cima, em primeiro lugar mantém a sociedade numa roda de hamster incapaz de ver que é o próprio sistema com a sua obrigação de crescimento incorporada para servir dívidas não reempregáveis que é responsável por toda a dor. Pior ainda, a partir do sistema existente, toda a inovação que reduza o preço ou poupe tempo no futuro deve ser compensada com uma maior

manipulação da moeda para manter o atual regime monetário em funcionamento. A própria energia constitui um bom exemplo. Não é como se não tivesse havido uma abundância de tecnologia aplicada na exploração, produção, transporte e desenvolvimento de novas fontes de energia. Quando se percebe que a principal razão (o aumento da procura também é importante) de os preços da energia terem subido face à entrada em linha da nova energia e aos ganhos de eficiência das fontes de energia existentes, é que têm de subir para apoiar o sistema de crédito existente, também se percebe que não há saída do sistema.

Para além de o problema ambiental ser insolúvel do sistema existente, a Bitcoin fornece um caminho para um planeta Kardashev tipo 1 onde aproveitamos toda a energia que pode chegar à Terra a partir do Sol (https://en.wikipedia.org/wiki/Kardashev_scale).

E fá-lo porque proporciona um incentivo económico positivo numa transição para energia abundante. Do ponto de vista da oferta e da procura, o elevado custo energético da Bitcoin para garantir a rede é uma característica porque é criado um incentivo económico que é simultaneamente natural e positivo para construir a abundância energética. A energia é o motor n.º 1 da rentabilidade na mineração bitcoin, o que significa que a energia de baixo custo é necessária para os lucros. Um mineiro de bitcoin não pode continuar a ser rentável pagando a energia a taxas que um cliente retalhista irá fazer, por isso não compete com essa energia.

Em vez disso, desencadeia o mesmo comportamento de mercado livre na produção e utilização de energia. Nomeadamente, a procura de

energia de menor custo ou encalhada. Ao fazê-lo, proporciona um preço mínimo para a energia e uma forma de atribuir capital a investimentos que de outra forma não seriam feitos. Esses novos investimentos energéticos, juntamente com as energias renováveis, permitem que regiões que outrora estiveram isoladas do mundo devido à falta de energia fiável possam construir riqueza e independência energética. A concorrência constante para encontrar custos mais baixos em energia e/ou usar o calor fornecido pela mineração Bitcoin para outros usos comerciais, como aquecimento de estufas ou edifícios comerciais, desencadeia uma onda de talento empresarial para o desafio da utilização energética. Tudo isto através da livre concorrência de mercado livre para garantir uma abundância fiável de energia e utilização.

Já deveria ser óbvio para a maioria dos observadores que a energia é mais importante nas nossas vidas do que o número de notas de papel impressas ou as suas representações digitais. Imprimir mais papel ou unidades digitais só cria escassez de energia adicional. A energia suplanta os dólares porque sem energia não há economia.

A ligação da Bitcoin à energia para a segurança e o seu correspondente efeito positivo no crescimento real e na abundância de energia é então talvez a sua característica mais subestimada (e que a grande imprensa tem completamente ignorado).

Este excerto de Gigi (@dergigi) fornece uma nova forma de entender como a energia protege a rede:

Qualquer coisa que não tenha qualquer custo real – custo que seja imediatamente óbvio e possa ser verificado por qualquer pessoa brevemente – pode ser trivialmente forjado ou simplesmente inventado. Nas palavras de Hugo Nguyen, "Ao ligar energia a um bloco, damos-lhe 'forma', permitindo-lhe ter peso e consequências reais no mundo físico".

Se removermos esta energia, digamos, passando de mineiros para signatários, reintroduzimos terceiros de confiança na equação, o que remove a ligação à realidade física que torna o passado evidente por si mesmo.

É esta energia, este peso*, que protege o livro de registos público. Ao trazerem para a existência esta informação improvável, os mineiros criam um campo de força transparente em torno de transações passadas, garantindo o valor de todos no processo – incluindo o seu próprio – sem qualquer uso de informação privada.*

Aqui vem a parte difícil de entender: o valor que é protegido não é apenas o valor no sentido monetário*, mas o próprio valor* moral *da integridade do sistema. Ao alargar a cadeia honesta com mais trabalho, os mineiros optam por agir* honestamente*, protegendo as próprias regras com as quais todos concordam. Por sua vez, são recompensados monetariamente pelo coletivo que é a rede.*

2)Descentralização

Existem 2 grandes escolhas de conceção que levam à descentralização contínua do bitcoin.

1) Em primeiro lugar, a natureza da Prova de Trabalho na resolução do problema dos generais bizantinos. É importante notar que se trata de uma descoberta que não pode ser resolvida novamente. Pode ser copiada, o que cria os seus próprios desafios, ou pode ser alterada para tentar resolvê-la de outra forma. Mas, por causa da relatividade geral, a sua alteração *não pode* resolver o problema sem introduzir um oráculo e centralização. Vamos mergulhar em cada um deles.

a) Uma cópia por necessidade não é a cadeia mais longa porque deve começar mais tarde do que a Bitcoin, que tem a maior prova de trabalho a proteger a sua história. A cadeia de blocos mais longa, por definição, é a que tem mais confiança. Portanto, uma cópia não pode ter a mesma segurança ou confiança, o que levanta a seguinte questão: que utilidade a nova cópia de Bitcoin forneceria que não seria melhor conseguida através da utilização da cadeia mais confiável e segura? Ou como é que uma nova cadeia sem utilidade ganharia tração suficiente para competir com Bitcoin, enquanto simultaneamente a mesma estava exponencialmente a aumentar a sua segurança e taxa de *hash* por causa da sua confiança?

b) Não existe tal coisa como o tempo universal. A teoria da relatividade geral de Einstein diz que a forma como experimentamos o tempo é do nosso ponto de vista. O tempo é relativo a nós – onde estamos. Dependendo das órbitas, esta diferença de "tempo" do nosso ponto de vista na Terra para Marte é entre 4 minutos e 24 minutos. Esta mesma diferença de tempo ocorre também na Terra, mas em intervalos tão pequenos que não a notamos no nosso dia-a-dia. O facto de não o notarmos não muda o facto de estas pequenas diferenças de tempo existirem. Quando os sistemas informáticos procuram chaves

criptográficas para provar que encontraram o bloco seguinte e ganharam o prémio, estas pequenas diferenças no tempo entre as diferentes regiões tornam-se criticamente importantes. Dois mineiros de Bitcoin de diferentes lados do mundo poderiam resolver a criptografia ao mesmo tempo devido a estas pequenas variações e ambos estarem corretos. Não é apenas teórico; já aconteceu inúmeras vezes no protocolo Bitcoin e a forma como é resolvido, é novamente, a cadeia mais longa, ou a maioria da confiança ganha. Durante um período de 10 minutos então, ou até que o bloco seguinte seja minado, estas 2 cadeias podem ser válidas até que o bloco seguinte seja extraído e os nós confirmem a cadeia mais longa. Os mineiros escolhem qual o bloco que acreditam ser válido e como 51% deles escolhem o correto, os outros mineiros mudam-se para a cadeia mais longa. É um desperdício de energia e recursos minerar sobre um bloco órfão. Mais uma vez, a cadeia mais longa é a que tem mais confiança.

Devido a esta descoberta que une energia e prova de trabalho, existe apenas outra forma de resolver o problema do tempo, que envolve a introdução de um agente ou oráculo "confiável" que define as "regras" e, em seguida, escolhe quais as transações válidas (que transação veio primeiro). Mas uma vez introduzido um oráculo para resolver o problema, a confiança é colocada no mesmo, e as regras podem mudar e a descentralização perder-se.

Bitcoin, através da Prova de Trabalho, é a única forma de resolver o problema. Como aponta Neil Degrasse Tyson, "Depois das leis da física, tudo o resto é uma opinião".

2) A segunda escolha de conceção que mantém a Bitcoin descentralizada é o tamanho do bloco. Sacrificar o tamanho adicional do bloco na camada 1 de bitcoin significa um menor número de transações por bloco de 10 minutos e/ou menos espaço para contratos inteligentes no código subjacente. Mantendo o tamanho do bloco pequeno, as dezenas de milhares de operadores de nós completos em todo o mundo são os verdadeiros aplicadores de regras da rede (Tomer Strolight @tomerStrolight dá um grande relato em primeira mão deste poder nas mãos dos operadores de nós aqui).

Por isso, enquanto os mineiros competem como agentes económicos para garantir a rede, são mantidos sob controlo por nós (abertos a qualquer pessoa para facilmente configurar e executar) que confirmem as transações. Estes nós completos têm cada um o historial da cadeia e confirmam cada uma das suas transações. Como o tamanho do bloco é mantido pequeno, significa que estes nós são muito económicos em termos de *hardware* e custos energéticos, o que, por sua vez, leva a mais nós ou participantes a validar o sistema (descentralização).

Ao adicionar informações adicionais ou espaço à cadeia de blocos na camada 1, o custo em energia e potência de computação para proteger a rede explode, e por sua vez leva apenas aos mais poderosos ou ricos ter dinheiro suficiente para executar nós, e por sua vez controlar as decisões. Também pode resultar em centralização. As guerras de tamanhos dos blocos, iniciadas em 2015-2019, lutam por esta questão-chave, com muitos dos mais poderosos defensores da Bitcoin na altura a favorecerem uma mudança de regras que traria mais funcionalidade à camada 1, mas por sua vez, dar-lhes-ia mais controlo na forma de centralização. Bitcoin viu-se a braços com esta luta com novo código

que representa as novas regras. Ao contrário dos garfos macios que são acordados pelos mineiros e cujos nós são retro compatíveis, os garfos duros criam uma nova cadeia. Por exemplo, se fosse dono de um bitcoin antes de 1 de agosto de 2017, e de um garfo duro para bitcoin em numerário, teria moedas em ambas as cadeias. Poderia então optar por vender um deles a favor do outro ou ficar com os dois. Abaixo está uma imagem do que o mercado determina como valor em ambas as moedas.

Capitalização de mercado do bitcoin a partir de 6 de agosto de 2022, — 443 Mil milhões

Capitalização de mercado do bitcoin em numerário a partir de 6 de agosto de 2022, — 2,7 Mil milhões

A discrepância de preço do garfo demonstra mais uma vez que, embora qualquer pessoa possa alterar as regras para oferecer uma moeda diferente, a cadeia mais longa com mais Prova de Trabalho tem mais confiança e é mais valorizada pelos participantes no mercado como resultado. A descentralização é uma grande parte desta confiança.

3) Escalabilidade

Como reforçado ao longo deste artigo, as escolhas de conceção que levaram à descentralização e à segurança que por si só não era possível antes #bitcoin, levaram também a escolhas que careciam de escalabilidade. É aqui que grande parte do conflito e confusão nas cadeias tem origem. Do ponto de vista da natureza humana, é fácil ver que haveria conflitos. Alguns utilizadores quiseram construir mais em

termos de escala ou diferenciação acima de Bitcoin e sentiram-se bloqueados pelo seu lento e metódico consenso de nós que protegem o ecossistema. Decidiram então criar as suas próprias cadeias com diferenciação e tentaram convencer outros de que as novas eram melhores de alguma forma. Embora muitos tenham sido/são completos burlões que procuram ganhar dinheiro com a ignorância alheia, alguns podem nem sequer ter tido consciência das implicações a longo prazo das suas decisões de conceção na criação de cadeias que devem falhar — seja devido a 1) centralização e falta de incentivos económicos, ou 2) vulnerabilidades de segurança. E uma vez criadas — não havia outra saída senão admitir o fracasso, ou continuar a mudar, prometendo resolver o paradoxo nalgum momento futuro.

Uma forma diferente de escalar.

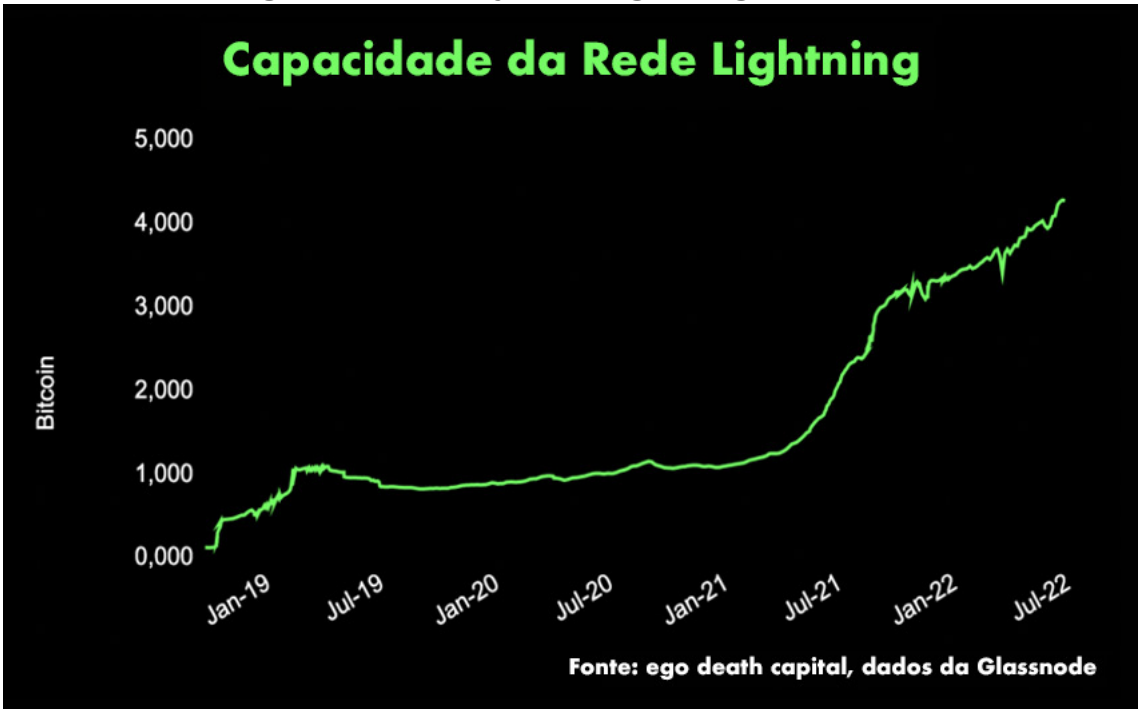
Os protocolos escalam em camadas. Escalar Bitcoin em camadas fornece uma forma de manter a segurança e a descentralização da primeira camada, mas também ganhar escalabilidade na segunda ou terceira camadas, em vez de sacrificar a primeira. À semelhança das camadas que formam os blocos de construção da internet e, em última análise, os produtos que se utilizam todos os dias. Cada um dos diferentes protocolos funciona apenas nessa camada. Esta abstração garante que cada camada é autossuficiente, precisando apenas de saber interagir com as camadas acima e abaixo dela, o que simplifica o *design* e a flexibilidade sem sacrificar o que outra camada fornece. Este curto vídeo no YouTube fornece uma boa visão geral das camadas de protocolo de rede do modelo TCP-IP em camadas:

Devido ao mal-entendido de que os protocolos escalam em camadas e o ruído geral no mercado, inovações como a Lightning, que permitiu o bitcoin escalar, seriam largamente rejeitadas por uma audiência que via a Bitcoin como uma tecnologia antiga em movimento lento, intransigente na sua segurança e descentralização.

Isto proporcionaria uma oportunidade assimétrica para as nações, empresários, capitais e público, que tiveram tempo para entender o que se passava no ecossistema contra aqueles que o rejeitaram.

Creio que estamos naquele ponto de inflexão onde tecnologias como Lightning, Fedimint, Taro e outros irão desencadear uma onda de inovação no espaço. Também acredito que, embora ainda esteja na sua infância, o bitcoin e o protocolo são imparáveis.

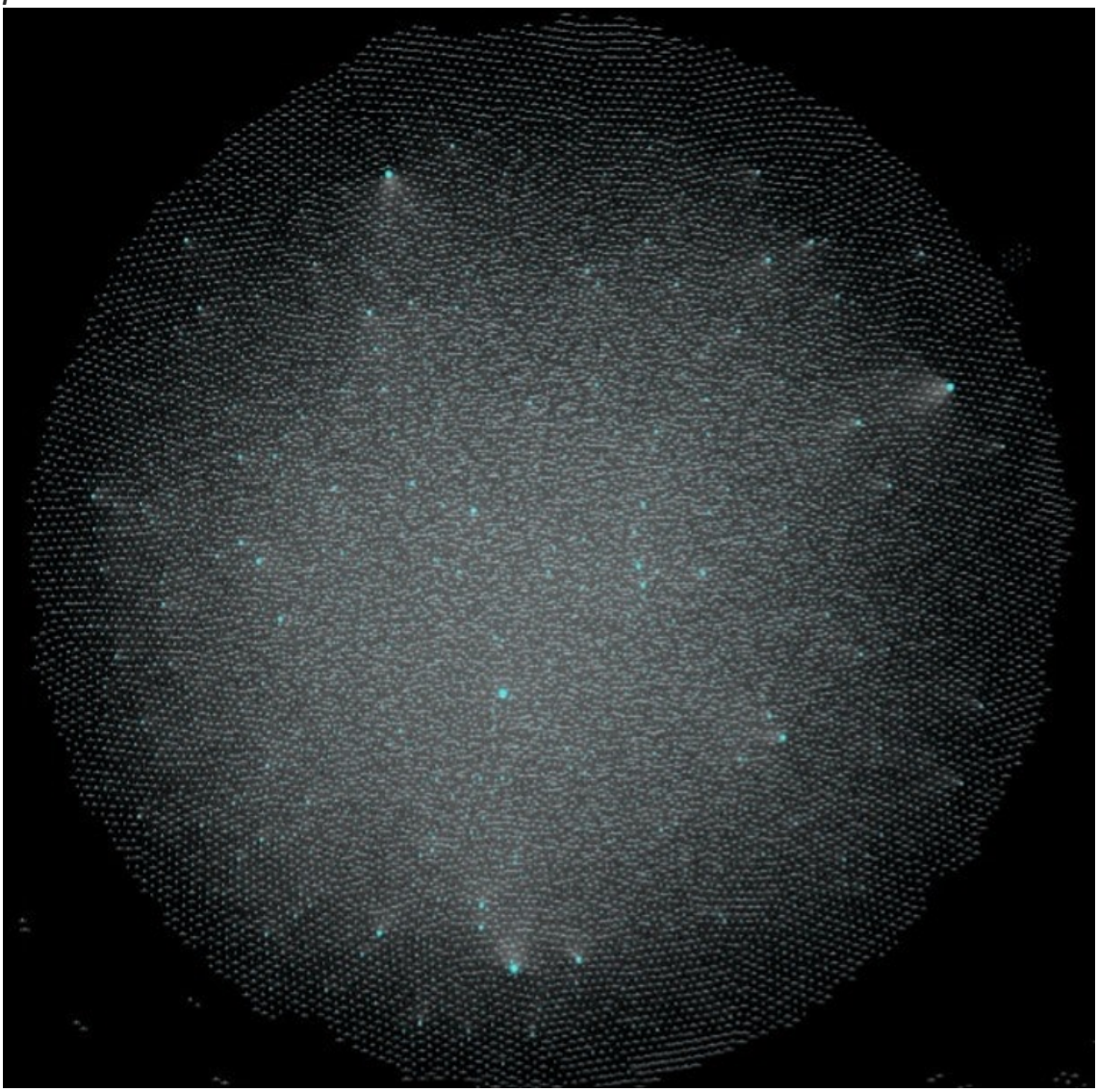
Abaixo está um gráfico de adoção da *Lightning* desde o início.



Da recente obra-prima de Lyn Alden, *A Rede Relâmpago*:

Imagine um sistema global com um grande número de nós interligados. Qualquer pessoa pode entrar na rede com um novo nó e começar a criar canais. Em alternativa, muitos serviços de custódia também dão aos seus titulares de conta acesso à rede através dos seus nós e canais.

Aqui está uma visualização da rede pública Relâmpago atual. É uma rede crescente de nós interligados ligados por canais de pagamento, com os pontos maiores representando nós particularmente bem conectados:



É cedo, e nem tudo vai funcionar como planeado, mas cada sucesso em camadas reforça e traz mais talento e capital para o ecossistema. Algumas destas peças do puzzle (como Lightning, Taro e Fedimint) trabalharão juntas de formas ainda não totalmente compreendidas — acelerando a adoção. Todas elas serão construídas sobre uma fundação de camada 1 que é sólida como rocha. Ao fazê-lo, muitos dos "casos de utilização" a longo prazo de moedas alternativas desaparecerão e, um por um, falharão.

O protocolo Bitcoin, escalando em camadas fornecerá uma camada base que combina uma nova internet ponto a ponto e dinheiro de forma nativa dentro dele. Isto formará uma base completamente segura, aberta a qualquer pessoa, uma fundação integral para a tecnologia de uma forma mais ampla. Como o alvorecer da internet, mas desta vez descentralizada e segura, garantindo com a sua conceção um caminho esperançoso para a humanidade: onde a abundância natural adquirida através da tecnologia é amplamente distribuída pela sociedade em vez de ser consolidada nas mãos de alguns. Os reguladores de certas nações poderiam tentar abrandar ou impedi-lo, mas ao fazê-lo, estariam a cometer um erro grave, como encerrar a internet dos seus cidadãos e bloquear a inovação que a acompanha. Não impediriam a inovação; em vez disso, garantiriam que a inovação e o valor derivados dessa inovação se deslocassem para outras nações. Com o tempo, as pessoas vão perceber que em vez de fixarem o preço do bitcoin "a partir do sistema" em que vivem hoje, ele irá fixar o preço de *tudo* nesse sistema.

Haverá sucessos incríveis, fracassos e aprendizagens Mais importante ainda, porém, haverá um valor duradouro para a sociedade que se

sobrepõe a uma base sólida que é incorruptível por um pequeno grupo de pessoas – descentralizada e segura pela sua conceção. Este sistema emergente, lançado ao mundo por Satoshi em 2009, muda tudo.

Jeff

Agradecimentos Especiais

Gostaria de agradecer a @lynaldencontact, @fossgregfoss, @dergigi, @thetrocro, @lawrenceLepard, @LukeGromen, @Obi, @princeysov, @knutsvanholm, @DarinFeinstein, pelas suas contribuições contínuas para o tema e/ou ajuda no debate através desta peça.

Aqui ficam alguns recursos adicionais:

1. Energia Bitcoin
2. Bitcoin é tempo
3. Resposta RFI: Implicações Climáticas dos Ativos Digitais
4. Instituto de Política de Bitcoin