OCCAM BRASIL

Carta Temática 4.1

CRIPTOATIVOS E PROPRIEDADE NA ERA DIGITAL

Abril 2022

"We cannot solve our problems with the same thinking we used when we created them."

Albert Einstein

Criptoativos e Propriedade na Era Digital

Ao longo desta carta, iremos analisar a utilidade intrínseca e o cenário de possibilidades dos criptoativos, além dos avanços no conceito de propriedade nesta nova era digital. Devido à extensão do tema e suas inúmeras derivações, este documento consiste na Parte 1 de nossa carta. As discussões sobre possíveis aplicações de tecnologias mencionadas serão aprofundadas em um momento posterior, na Parte 2. Faz-se importante ressaltar que esta exposição não deve ser interpretada como recomendação de investimentos e, portanto, não nos debruçaremos sobre aspectos de precificação de ativos.

1. Introdução

O conceito de propriedade suscitou extensos debates filosóficos ao longo da história, tendo sido objeto de análise de grandes pensadores. Na Antiguidade Clássica, Platão postulou que a propriedade coletiva seria essencial para a busca de interesses comuns em uma sociedade. Seu discípulo e dissidente Aristóteles, por sua vez, destacou que a propriedade privada seria capaz de promover virtudes como a prudência e a responsabilidade. No início do período moderno, as teorias de Hobbes afirmaram que a propriedade só poderia existir mediante a criação de um Estado soberano, responsável, portanto, pelo estabelecimento de regras comuns para sua gestão. Na contramão, John Locke, um dos filósofos modernos de maior influência, argumentava que a propriedade poderia existir sem a necessidade de qualquer convenção social ou decisão política.

Todas essas discussões e os entendimentos que dela derivam são relevantes para compreender de que modo se estrutura a "posse" em nossa sociedade, e que conflitos de interesse podem advir deste direito.

Pode-se entender a democracia contemporânea como um conjunto de contratos sociais. Através do voto definimos, direta ou indiretamente, as regras que orientarão a ordem comum. Tomemos como exemplo a Constituição Federal: esse contrato, cujo cumprimento depende de uma instituição centralizadora (Governo), ordena as diretrizes da gestão de propriedade, seja ela pública, coletiva ou privada. O acordo dita, portanto, a forma de interação entre agentes, tornando-se um pilar fundamental para a cooperação, produção e trocas comerciais em uma sociedade, assim como Hobbes acreditava.

Qualquer sociedade que queira evitar conflitos precisa de um sistema de regras comuns – como o que temos atualmente –, o que não quer dizer que esses conflitos

deixem de existir. Embora a propriedade privada seja regida a partir de decisões individuais, ela deve estar inserida em um sistema de regras sociais. Portanto, a propriedade privada tem a contínua necessidade de justificar sua existência também do ponto de vista da coisa pública.

Tal fenômeno é explícito no contrato social dos Estados Unidos, mais especificamente na Quinta Emenda à Constituição, que garante ao Estado a possibilidade de apropriar-se de bens privados para uso público, desde que mediante "compensação justa". A Constituição permite ainda que o Estado imponha restrições quanto ao uso do ativo, a exemplo da proibição de construção civil em zonas transformadas em patrimônio público por meio do tombamento histórico, artístico ou cultural. O direito à propriedade está enredado, portanto, em uma dualidade entre o público e o privado, e seria um equívoco entendê-lo como um sistema de posse absoluta.

A Occam Brasil reitera com esta carta seu foco na busca por conhecimento em inovação e tecnologia, e apresenta um tema que acreditamos ser fundamental para o desenvolvimento tecnológico e social e suas repercussões sobre o conceito de propriedade na era digital.

O objetivo desta exposição é de caráter exclusivamente elucidativo. Recomendamos que o leitor invista nada mais do que seu tempo para conhecer o ecossistema e suas derivadas, ampliando as próprias percepções acerca do tema. Esperamos que, após a leitura desta carta, vocês tenham muito mais dúvidas do que respostas, assim como nós.

Feitas as devidas considerações, e tendo evidenciado o paralelo entre a história e o presente, faremos uma breve retrospectiva a partir da origem do mundo digital.

"Change is the only constant in life.", Heráclito

2. A História da Internet

A internet como a conhecemos hoje teve início nos anos 60, quando o professor J.C.R. Licklider, do MIT, idealizou uma *"Intergalactic Network*" de computadores que, junto ao conceito de *"packet switching"*[1] desenvolvido logo em seguida, formaram dois dos principais pilares da internet. Contudo, o primeiro protótipo viável surge apenas no final daquela década, quando, em outubro de 1969, a ARPANET *(Advanced Research Projects Agency Network)*, uma agência financiada pelo Departamento de Defesa dos Estados Unidos, soltou a primeira mensagem na internet: "*LOGIN*".

[1] *Packet Switching* – ou Computação de Pacotes
Método de agrupamento de dados em pacotes que são transmitidos por uma rede.

A rede mundial de computadores continuou, assim, a se desenvolver nos anos 1970. Um grande passo foi a criação dos protocolos TCP/IP *(Transmission Control Protocol/Internet Protocol)*, que estabeleceram padrões de como os dados deveriam ser transmitidos entre diferentes redes, e que, em 1983, foi adotado pela ARPANET como protocolo base da internet. Vale ressaltar ainda que, nos primórdios da internet, não era óbvio que ela deveria ser aberta e pública – alguns consideravam que as "Intranets" seriam a forma mais segura e confiável de avançar.

O maior marco da internet moderna veio apenas em 1990, quando o pesquisador e cientista da computação Tim Berners-Lee inventou a *World Wide Web,* que, embora muitas vezes confundida com a própria internet, é na verdade uma maneira de acesso comum aos dados de forma online. Em seguida, surgiram diversos protocolos abertos que utilizamos de forma indireta e que devem soar igualmente familiares: HTML *(Hypertext Markup Language)*, HTTP *(Hypertext Transfer Protocol)*, URL *(Uniform Resource Locator)*, entre tantos outros.

Em 1993, Marc Andreessen, na época um estudante de computação de Illinois, ajudou a lançar o primeiro *Web Browser* de fácil uso, o MOSAIC, ajudando a popularizar e difundir a internet. Fundou também em 1994 a Netscape, que chegou a 10 milhões de usuários globais em menos de um ano. Marc, que hoje em dia é co-fundador e *Managing Partner* da notória firma de Venture Capital Andreessen Horowitz ("a16z"), é um grande investidor em projetos de criptoativos.

A internet da atualidade tem grande parte da sua evolução baseada em um modelo de *open-source* e de *open protocols*, em que o desenvolvimento de uma aplicação, empresa ou projeto é pautado em regras claras de difícil modificação e, até hoje, não monetizados. Assim como empreendedores buscam criar empresas em países com transparência e constância regulatória, a internet deve parte da sua explosão de inovação a essas regras claras e imutáveis. Aplicações que um usuário comum utiliza hoje, como Youtube, Twitter, Instagram, WhatsApp – empresas que valem centenas de bilhões de USD – foram construídas com base nesses protocolos.

3. Evolução da Web

A *World Wide Web*, usada por bilhões de usuários, é a principal ferramenta para ler, escrever e compartilhar conteúdos via rede de computadores. Ela evoluiu muito desde as primeiras aplicações, e mudou a maneira como interagimos com outras pessoas pela internet. Dessa forma, a dinâmica do usuário nas redes evoluiu em três estágios: a princípio, ele atuava como mero consumidor de informação; depois, este passa a interagir e a prover conteúdo para a rede – modelo em que as plataformas centralizadoras seguiam sendo as verdadeiras detentoras do conteúdo –; e, finalmente, na terceira fase o usuário tem o poder de ditar as formas de aplicação e passa a ser proprietário do conteúdo que produz.

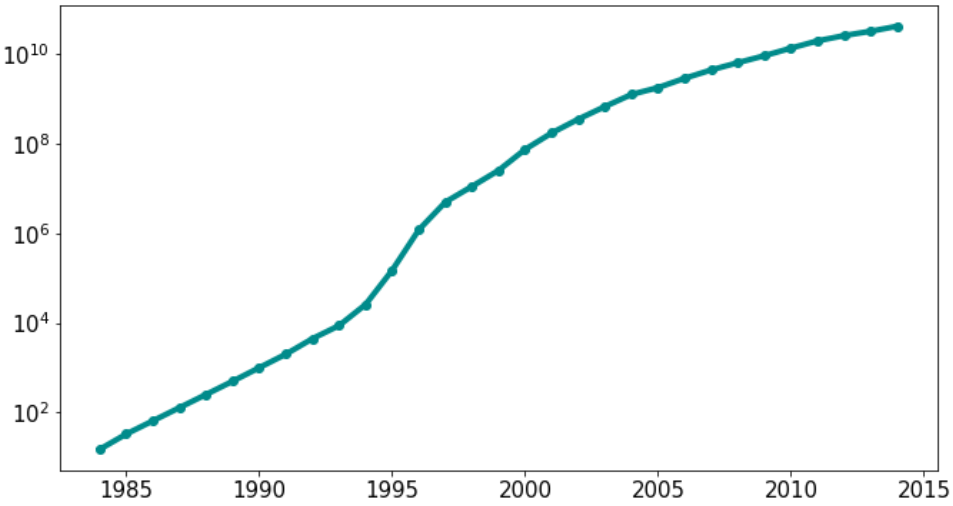
O assunto que vamos tratar nesta carta se situa na terceira fase da internet, na qual os protocolos de criptoativos têm papel fundamental. Portanto, devemos contextualizar a transformação digital da Web para entender que podemos estar diante de um ponto de inflexão na história.

Web 1.0 – (1990 ~ 2005)

Também conhecida como a internet estática, ou "*read-only*", a Web 1.0 foi a primeira fase do desenvolvimento de aplicações online. As primeiras aplicações consistiam basicamente em transposições de experiências offline para o online, como por exemplo a replicação de revistas e jornais. A informação era compartilhada de forma unilateral, tendo como origem sites ou blogs, e destino, o usuário final. Nessa fase, as conexões eram lentas, difíceis de usar e não atraentes para a adoção *mainstream* de usuários. Exemplos clássicos de empresas fundadas nessa fase são Yahoo, Google e Amazon.

Evolução da banda larga da Internet [2]

Tráfego de Internet Global em Gigabytes por Mês



a. Fonte: Cisco Annual Internet Report

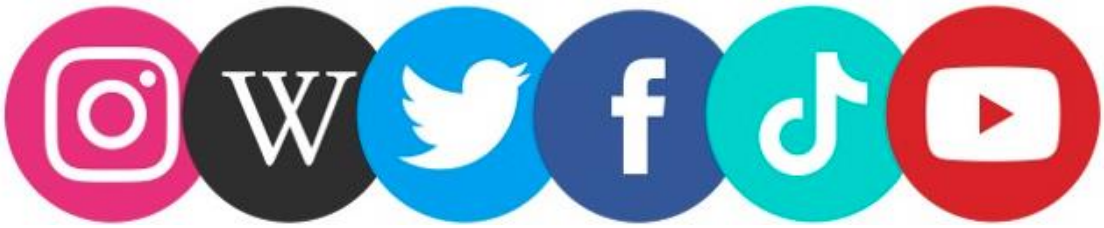
[2] Evolução da banda de dados da Internet
As aplicações mais complexas da Web 2.0 só foram possíveis devido a evolução na infraestrutura de transferência de dados da internet. A banda, no começo, era estreita, passando poucos dados de cada vez. Conforme foi alargando ao longo do tempo, permitiu a passagem de muitos mais dados até chegar ao ponto em que conhecemos como banda larga.

Web 2.0 (Atual?)

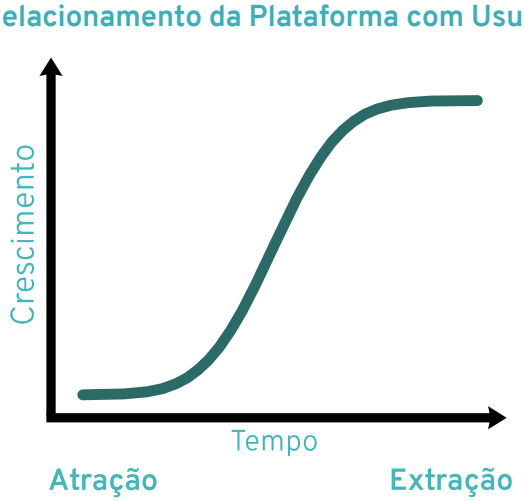
A Web 2.0, também conhecida como *"read-write web"* ou *"social web"*, é marcada pela interação contínua entre plataformas e usuários. Agora a informação flui da plataforma para o usuário e vice-versa, e ambos promovem engajamento para popular a rede. As plataformas são baseadas em conteúdos gerados por usuários e regidas por fortes efeitos de rede. Isso quer dizer que, quanto mais produtores de conteúdo

estão envolvidos, maior é a relevância atribuída à plataforma, que, por consequência, aumenta o valor criado para novos usuários – fomentando o ciclo de crescimento da rede.

Exemplos clássicos desta fase são YouTube, Facebook, Twitter, TikTok, entre tantos outros.



Contudo, não faltam críticas à postura que essas grandes empresas centralizadoras vêm adotando em relação a alguns de seus *stakeholders* – tanto usuários como desenvolvedores. Essas plataformas cresceram de forma meteórica, a ponto de hoje serem consideradas fundamentais para nossa vida. Esse excesso de poder abre espaço para manipulações nas redes que podem ir contra o interesse de usuários. Casos de decisões arbitrárias e controversas corroboram para evidenciar o conflito de interesses entre usuário e rede, e aumentam a desconfiança entre os *stakeholders*.

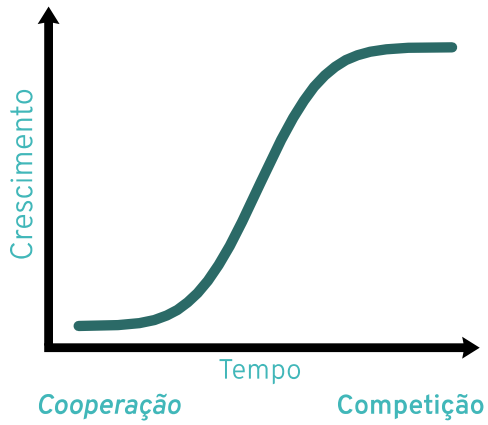


b. Fonte: Chris Dixon Blog

Na fase inicial de desenvolvimento dessas plataformas, a estratégia de crescimento se baseia na captação de usuários para geração de fortes efeitos de rede. Nesse estágio, as empresas não poupam esforços ou recursos para desenvolvê-la e atrair clientes – período ilustrado no gráfico acima pela fase "Atração". No entanto, quando tais plataformas chegam ao estado de saturação de usuários, esse movimento se inverte. A estratégia passa, então, de "atrair" ou "servir ao cliente" para "extrair do cliente". Nessa etapa, representada no gráfico pela fase "Extração", cria-se maneiras cada vez mais elaboradas de monetização da base de usuários.

"If you're not paying for it, you're not the customer; you're the product being sold.", autor desconhecido

Relacionamento da Plataforma com Apoiadores (desenvolvedores e criadores de conteúdo)



c. Fonte: Chris Dixon Blog

O mesmo efeito pode ser visto na relação de cooperação existente entre pequenos empreendedores e grandes plataformas. No início, para fortalecer o ecossistema e atrair novos usuários, os grandes *players* incentivam empreendedores a criar aplicações em suas plataformas. Conforme esses projetos vão ganhando corpo, as companhias entendem as preferências dos usuários por meio da observação de quais aplicações e produtos demonstram estar dando certo. As plataformas incorporam, assim, essas informações e mudam seu comportamento de "Cooperação" para "Competição".

Na posição de competidoras, elas podem então adotar medidas abusivas em relação às pequenas empresas, até mesmo como o corte de seu acesso à rede. Após confiar nas plataformas e desenvolver seus projetos em cima delas, os empreendedores acabam por serem descartados, e as ideias e dados aprimorados por eles são absorvidos pelos grandes *players*.

Existem casos notórios desse comportamento, e que alguns dos leitores talvez possam reconhecer, como: Zynga vs. Facebook, Voxer vs. Facebook, Meerkat vs. Twitter, Amazon 3P vs. 1P, Google vs. Yelp entre inúmeros outros.

Web 3.0

Nesta fase, acreditamos que a internet será pautada por um conceito intrínseco ao mundo offline, mas que até então não havia sido transposto para o mundo online: o conceito de propriedade. Este, por sua vez, é o ponto central para a existência do Metaverso [3]. Não à toa, essa fase é também conhecida como *"read-write-own web"*. Através da propriedade, os usuários e geradores de conteúdo poderão ditar as regras que irão reger seu conteúdo. Gostamos também de denominar a Web 3.0 como a internet descentralizada, uma vez que, ao empoderar o produtor de conteúdo, não será mais necessário depender de instituições centralizadoras para que ditem as regras das aplicações que utilizamos. Nós, usuários, através de comunidades, poderemos influenciar diretamente as aplicações de que fazemos uso.

Algumas *features* que consideramos importantes para o desenvolvimento dessa fase da internet:

[3] Metaverso
Análogo às inovações trazidas pela internet, o Metaverso aqui se refere ao possível futuro imersivo das interações online. Podemos pensar que, se a internet é o 2D, o Metaverso inaugura o 3D.

- *Open:* O desenvolvimento será baseado em *open protocols*, assim como ocorreu nos primórdios da internet. Tal ecossistema aberto incentiva a *composibilidade*[4], uma vez que é possível utilizar códigos já criados por terceiros na criação de novas aplicações, reduzindo assim o retrabalho e fomentando a inovação.

"Composability is to software as compounding interest is to finance.", Chris Dixon

- *Trustless:* Não é necessário que exista confiança entre agentes para que se atinja consenso na rede.

- *Permitionless:* Qualquer pessoa que queira fazer parte da rede pode participar.

- *Interoperability:* Devemos ver aplicações altamente interoperáveis, diferente do modelo atual de plataformas fechadas, ex., Facebook, Google, Twitter... Em que grande parte do "poder" que tais empresas têm é fruto dos altos *switching costs*[5].

Como chegaremos lá? Acreditamos que **blockchain** pode ser o caminho para deslocar o poder do centro para as pontas.

"Web 3 is the Internet owned by users and builders orquestrated by tokens", Packy McCormick

4. Blockchain and DLTs

Em resposta ao cenário de desconfiança no sistema financeiro instaurado após a crise que tomou o globo em 2008, passou-se a questionar paradigmas da época. A busca por uma infraestrutura de pagamentos que não fosse controlada por governos de países específicos e que pudesse funcionar sem a necessidade de confiar em terceiros foi a grande motivação para a criação do Bitcoin. Para atender a estes dois requisitos, propôs-se para a criptomoeda uma estrutura de livro caixa distribuído (*distributed ledger*, ou DLT) baseada no encadeamento de blocos de transações, conhecida como blockchain. Embora a rede do Bitcoin seja regida por um DLT de tipo blockchain, outras criptomoedas podem ter estruturas diferentes de livro caixa.

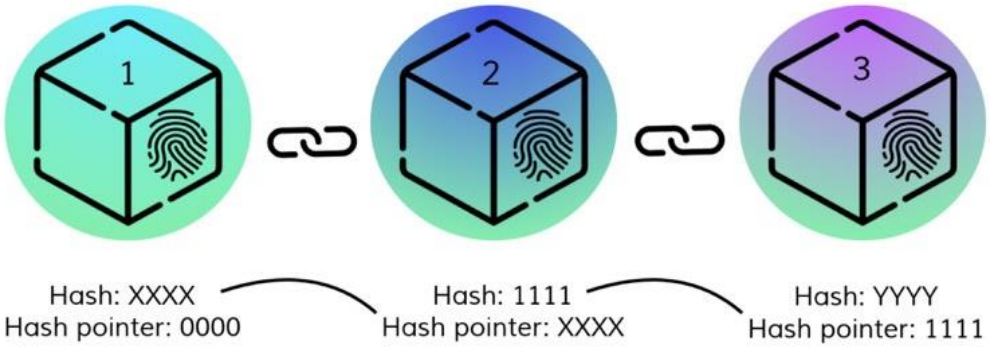
Um DLT funciona como uma grande base de dados em que se registram todas as transações de entrada e saída realizadas em um domínio financeiro, seja este uma empresa, um banco ou um país. Uma blockchain, no caso, registra essas transações

[4] *Composibilidade*
Neste caso, referindo-se à capacidade de qualquer participante de uma rede a usar códigos/programas já existentes e adaptá-los ou usá-los para criação de novas aplicações. Gostamos da comparação com "legos", no qual utiliza-se de diversas peças diferentes para montar uma estrutura

[5] *Switching Costs*
Custos que derivam da migração de usuários de uma plataforma para outra. Podem ser considerados custos relacionados ao esforço ou até financeiros, desde que sejam fruto da troca.

na forma de blocos armazenados, distribuídos nos computadores dos seus integrantes. O que torna esse sistema de registro descentralizado é o fato de que ele pode ser atualizado através de múltiplos servidores, e não existe um agente único responsável por controlar a inclusão de novas transações, sendo assim uma rede compartilhada e distribuída. Esses servidores que incorporam novas informações ao sistema de registro são chamados de *nodes* (nós). Para garantir a integridade e a irreversibilidade das transações, a adição de um novo bloco à cadeia requer uma prova de trabalho (*Proof of Work*), que deve ser validada pelos *nodes* antes de o incorporarem.

A prova de trabalho costuma ser um desafio matemático sem solução analítica possível, isto é, cuja descoberta requer tentativa e erro, em um processo de força bruta, também chamado de mineração. Apesar da elevada dificuldade computacional de minerar um bloco, a verificação de sua legitimidade é extremamente rápida. Dessa forma, ao receber um novo bloco minerado, os *nodes* conseguem validá-lo facilmente antes de incorporá-lo à sua cópia da blockchain. Como o primeiro integrante a realizar uma mineração bem-sucedida costuma receber uma recompensa financeira, muitos computadores são alocados nesta tarefa, numa competição pelo novo bloco a ser integrado à cadeia. A dificuldade do desafio matemático é ajustada automaticamente segundo a velocidade com que novos blocos são criados, visando manter essa taxa constante. No Bitcoin, esta velocidade é definida como um bloco a cada dez minutos.

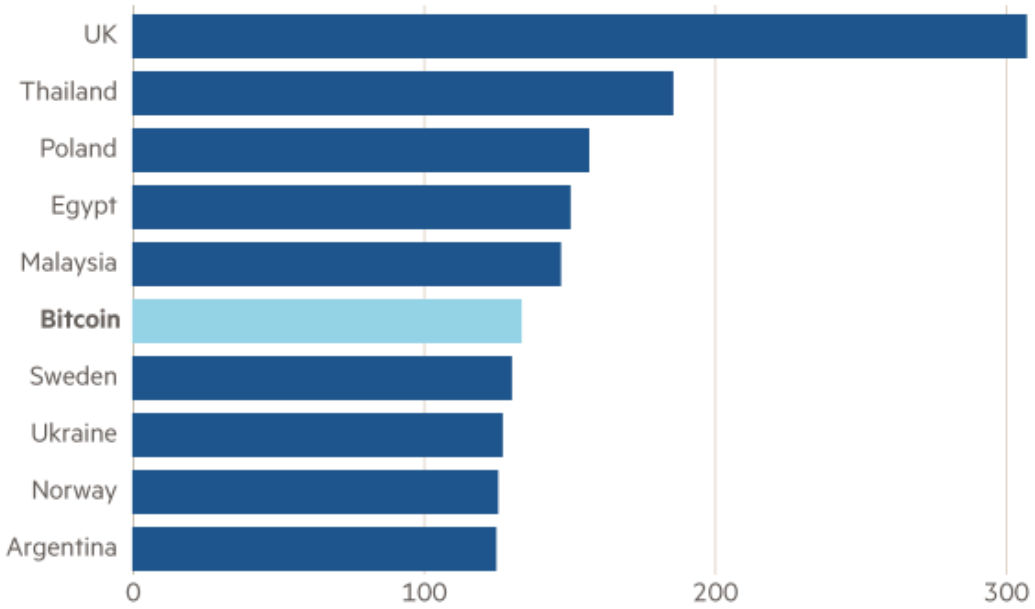


Esse ajuste constante na dificuldade de mineração tem como objetivo assegurar a competitividade entre os participantes, desestimulando tentativas de centralização do controle das blockchains. Este é um ponto central por trás da incorruptibilidade da rede: a dificuldade de solução de um problema matemático determina a capacidade computacional necessária para que um único bloco seja minerado no tempo estipulado. Supostamente, para que um bloco ilegítimo atinja o consenso – isto é, obtenha mais de 50% de validação na rede e seja incluído na série histórica das transações –, o minerador teria que validar um primeiro bloco com transações irregulares e validar um seguinte com transações legítimas dentro desses mesmos dez minutos, no caso do Bitcoin. Dado que o desafio matemático é ajustado para que haja a criação de apenas um novo bloco nesse intervalo de tempo, a fraude sistemática torna-se impossível. Assim, não há incentivos à busca por uma supremacia de mineração, pois o custo computacional para tal seria superior ao valor obtido em retorno. A ideia central é que, ao ser honesto, é possível ser mais bem-

remunerado do que com a fraude à rede, o que conta como um incentivo monetário para que os participantes obedeçam às regras.

A intensa competição pela mineração nas blockchains implicou um gasto de energia elétrica considerável nos últimos anos, chegando a níveis superiores ao consumo total de alguns países. Considerando os impactos ambientais desta que é uma atividade em plena ascensão, novas propostas têm surgido para validar blocos nas blockchains. Uma que chama particular atenção é a prova de participação *(Proof of Stake)*, baseada no volume financeiro da rede associada aos *nodes* que o reconhecem como um bloco válido. Desta forma, a centralização do controle da blockchain exigiria não um poder computacional extraordinário, mas um poder financeiro superior ao benefício obtido em retorno.

Bitcoin consome energia equivalente à Suécia



d. Fonte: Cambridge Bitcoin Eletricity Consuption Index. Energias anualizadas em TWh.

5. Bitcoin

Em agosto de 2008, o domínio "bitcoin.org" foi registrado e, em outubro do mesmo ano, o artigo *"Bitcoin: A Peer-to-Peer Electronic Cash System",* de autoria do pseudônimo Satoshi Nakamoto, foi postado em uma mala direta (*mailling list*) de criptografia. Desde então, a internet, sobretudo o meio de tecnologia, já evoluiu consideravelmente, mas os conceitos que basearam esse artigo sobreviveram firmes à passagem do tempo. A rede descentralizada que serve de livro caixa do bitcoin – neste caso, usa-se letra minúscula para referir-se ao token – vem ganhando adesão como uma forma de propriedade na internet. A identidade de Satoshi continua sendo um enigma até hoje, mistério este que envolve mais de 1.000.000 BTCs (quase USD $45bn em valores atuais), que se acredita estar contidos na carteira digital de Satoshi e nunca terem sido mexidos.

Antes de explicar os principais conceitos por trás desse token, é importante entendermos o que essa rede veio solucionar e por que nunca tivemos o que gostamos de chamar de "verdadeira propriedade" na internet.

Byzantine Generals Problem

O Problema dos Generais Bizantinos é um problema de teoria dos jogos que ilustra a dificuldade que agentes sem confiança mútua (*Trustless*) enfrentam na construção de um consenso. Ele é formulado da seguinte forma: vários generais cercaram uma cidade fortificada, mas devem decidir de forma conjunta quando atacar. Se todos atacarem no mesmo momento, a cidade será tomada, caso contrário, não conseguirão concluir a invasão. Os generais não têm um meio seguro de comunicação, uma vez que as mensagens enviadas podem ser interceptadas, e não há maneira de saber se as mensagens recebidas são verdadeiras ou falsas. Como eles poderiam, assim, coordenar esse ataque?

A "solução" deste problema, até a existência do Bitcoin, foi de confiarmos em instituições centralizadoras que nos garantam que as mensagens contêm a informação verdadeira. A grande inovação do Bitcoin foi justamente a quebra desse paradigma, já que, através de conceitos criptográficos como "*Hashcash*" [6] conseguiu-se criar consenso entre agentes "não-confiáveis" (agentes que não precisam confiar uns nos outros).

[6] Hashcash
Sistema de *"Proof of Work"* proposto em 1997 por Adam Back com a finalidade de limitar *e-mail spams* e a ataques DoS *(Denial-of-Service)*.

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.", Satoshi Nakamoto

O Bitcoin nada mais é que um livro público de transações que faz o acompanhamento das movimentações dos tokens bitcoin, sendo o estado da rede validado de forma descentralizada. Até a existência do Bitcoin, não havia na internet uma maneira consensual de criar uma moeda, ao menos não uma que fosse à prova de transações duplicadas (casos em que a mesma moeda é enviada para duas pessoas ao mesmo tempo). A tecnologia blockchain foi usada para solucionar este problema, assegurando para esse ativo características do papel-moeda como reserva de valor, meio de troca e unidade de conta.

As novas emissões de Bitcoin serão reduzidas pela metade a cada quatro anos por meio do mecanismo de *Halving* [7] e, portanto, haverá um limite para a criação de tokens de bitcoins, estimado em 21 milhões. Dessa forma, criou-se então o primeiro ativo escasso na era digital. Após a inclusão de um novo bloco na rede (ou *ledger*), as transações ali contidas se tornam praticamente imutáveis e, assim como ocorre com protocolos da internet, as regras do jogo ficam bem definidas, sendo o código matemático e criptográfico no qual estas foram escritas o elemento que assegura esse histórico.

[7] Halving
Referência ao mecanismo de incentivos do Bitcoin que, a cada quatro anos, reduz pela metade a remuneração pela prova de trabalho dos mineradores.

O aspecto mais interessante dessa inovação, na nossa visão, não é seu caráter de moeda digital, o fato de poder ser usada como meio de troca, e sim a tecnologia que

há por trás. A disrupção está na dinâmica descentralizada e na criptografia incorruptível em que foi que programada. Esta, por sua vez, permitiu que uma série de outras soluções fossem desenvolvidas e a discussão abordada se tornasse especialmente extensa devido a esta "segunda fase" da evolução da tecnologia blockchain. Temos então o caso da Ethereum, que evidencia o poder de utilização desse meio, em contraponto ao Bitcoin, que até agora é insuficiente em termos de utilidade intrínseca, fora a de reserva de valor.

6. Ethereum

Fundada em 2015, a Ethereum foi criada pelo jovem prodígio Vitalik Buterin, que, nascido em Kolomna, na Rússia, emigrou com os pais para o Canadá quando tinha apenas seis anos. Vitalik, que durante seu tempo no Canadá estudou em turmas para superdotados, é um exímio desenvolvedor, e ajudou a fundar a famosa *Bitcoin Magazine*. Ainda nos primórdios do Bitcoin, atuou como escritor da revista, antes de idealizar e lançar o *whitepaper* do Ethereum, em 2014. Diferentemente de Satoshi, o fundador do Ethereum é uma figura pública, e é considerado uma celebridade dentro e fora da comunidade cripto, ,.

O Ethereum, assim como o Bitcoin, é um *public ledger* que serve para acompanhar o histórico de transações do token ETH ("ether"), e que utiliza o mesmo mecanismo de consenso do Bitcoin, "*Proof of Work*", ao menos até o momento da escrita desta carta. A grande inovação trazida pelo Ethereum é a possibilidade de se criar códigos que sejam executados de forma automática na blockchain, os chamados *smart contracts*. Ethereum é um supercomputador que roda de forma descentralizada e é *"Turing-Complete"*[8], ou seja, pode executar as mesmas funções que o seu computador de casa.

[8] *Turing-Complete*
Referência a um sistema que permite que algoritmos executados em sequência sobre dados arbitrários produzam resultados de qualquer cálculo, desconsiderando memória ou tempo de cálculo. O termo é uma homenagem a Alan Turing.

O "super computador" Ethereum utiliza uma linguagem própria de programação conhecida como *Solidity* e uma plataforma de desenvolvimento chamada *Ethereum Virtual Machine* (EVM), em que é possível imputar códigos a serem executados de forma automática pela rede, criando assim aplicações descentralizadas (DApps). Devido às inovações que o Ethereum trouxe à mesa, muitos desenvolvedores migraram para esse ecossistema com o objetivo de explorar a plataforma e ajudar em seu desenvolvimento. Desta forma, foi criado um ecossistema onde aplicações podem ser desenvolvidas com características impensáveis para as aplicações de Web 2.0.

Até o momento, o Ethereum é a plataforma de criptoativos com a maior comunidade de desenvolvedores e aplicações. Junto com esta rede surgiram outras soluções criadas com o uso de blockchain, dentre as quais destacamos a tokenização, os NFTs e as DAOs.

Layer 1 Alternativas

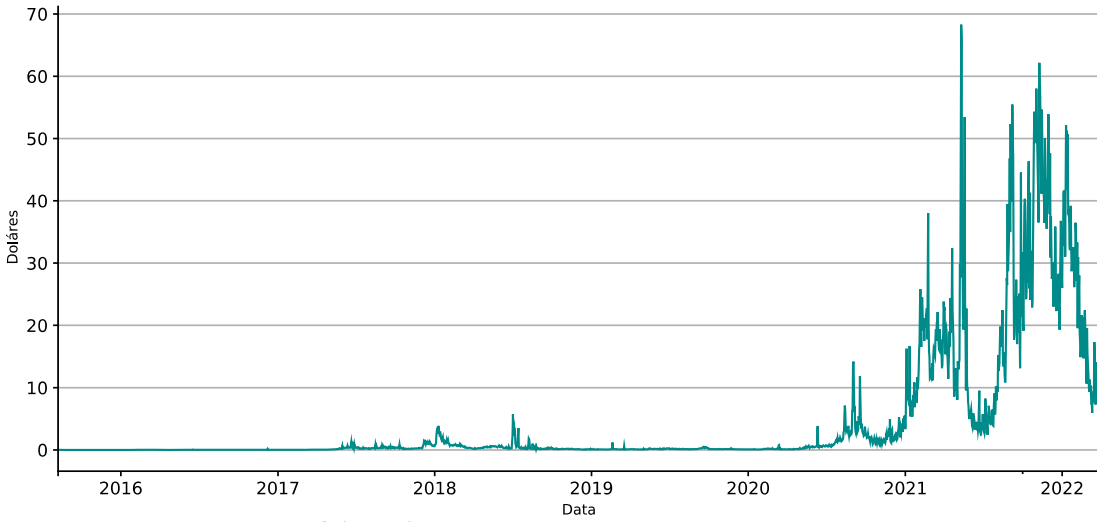
Embora o Ethereum tenha sido a primeira blockchain a incorporar os *smart contracts*, seu desenvolvimento não tem se dado sem percalços. O *"hard fork"*[9], motivado por um roubo de cerca de 5% dos ETHs em circulação em 2016, deu origem a duas redes distintas: uma daqueles que aprovavam a mudança do livro de ordens para impedir o

[9] *Hard Fork*
Referência à mudança drástica no protocolo da rede que demandou que os *nodes* atualizassem seu software, criando assim uma divergência entre estes nodes mais atualizados e nodes que seguem aceitando transações anteriores às novas regras, fato que levou à criação de duas redes distintas.

roubo, e outra daqueles que acreditavam que o livro deveria ser imutável, denominadas *Rede Ethereum* e *Ethereum Classic*, respectivamente.

Outro ponto é a questão da lentidão no desenvolvimento da rede, que até hoje tem capacidade de processar apenas em torno de 13 tps (13 transações por segundo). Essa baixa velocidade de processamento, somada à alta da demanda por aplicações desenvolvidas em cima da rede, leva a um aumento considerável de custo de transação, chegando a mais de $100 por transação em momentos de pico.

Custo Médio de Transação do Ethereum em Dólares



e. Fonte: Coinmetrics

Criou-se assim um efeito de rede perverso, uma vez que, quanto mais aplicações são desenvolvidas, maior a demanda por *"blockspace"*[10] e, consequentemente, maior o custo de transacionar na rede, o que desencoraja o desenvolvimento de novas aplicações. Surgiu então uma oportunidade para que outras redes baseadas nas inovações do Ethereum se formassem e capturassem parte da demanda por capacidade de transações. Essas redes, conhecidas como *Alt Layer 1s*, lidam com diversos *trade-offs* em termos de descentralização, segurança e escalabilidade. O Ethereum prioriza, portanto, a descentralização e a segurança, enquanto outras preferem focar em escalabilidade. O maior exemplo desse trade-off está na rede Solana, que já possui capacidade de processar algo no entorno de 50.000 Tps (aproximadamente a mesma taxa de TPS da Visa) e com *transaction fees* girando perto $0.003. No entanto, em termos de descentralização, a Solana ainda está muito atrás da rede Ethereum, fato em grande parte devido a requerimentos de hardware para validadores.

Não sabemos qual ou quais blockchains serão vencedoras em termos de ser a plataforma base para a criação de DApps, por exemplo. É possível que vejamos aplicações que dependam menos de segurança sendo desenvolvidas em *Layer 1s* mais centralizadas; em contrapartida, as aplicações para as quais descentralização ou segurança sejam fatores-chave tenderão a usar o Ethereum ou seus *rollups*[11] como base. Dada a complexidade do tema, optamos por reservar a discussão conhecida como *"Layer 1 Wars"* para uma futura carta. Daremos ênfase aqui nas inovações que estão sendo criadas com o advento das *Layer 1s*.

[10] *Blockspace*
Referência à limitação de tamanho dos blocos que podem ser validados em determinado período, isto é, à limitação da quantidade de transações que podem ser validadas por bloco.

Blockspace pode ser pensado como uma commodity que alimenta o coração de redes de criptoativos, em que os mineradores teriam o papel de "produtores". Os "leiloeiros" seriam os *Mining Pools* (ex. grandes grupos compostos por diversos mineradores); e os usuários teriam o papel de "compradores".

Porém, diferente de diversos mercados de commodity, neste caso um maior número de produtores (mineradores) não significa um aumento da produção, e sim um aumento da segurança da rede.

"You come to the realization that the blockchain is really a general mechanism for running programs, storing data, and verifiably carrying out transactions. It's a superset of everything that exists in computing. We'll eventually come to look at it as a computer that's distributed and runs a billion times faster than the computer we have on our desktops, because it's the combination of everyone's computer.", Tim Sweeney (Epic Games)

Smart Contracts

Para ilustrar o conceito de contrato inteligente, suponha que João queira fazer uma aposta com Fernanda. João acredita que o Flamengo vai vencer o Fla x Flu, e Fernanda, o contrário. Ambos entram em acordo sobre as condições do contrato e, após o resultado do jogo, ele é automaticamente executado. Isso implica que o dinheiro sairá da conta de um agente para a do outro sem que haja um intermediário. Os *smart contracts* contidos na blockchain são imutáveis, e a execução do contrato é feita de forma confiável e validada por todos os *nodes* da rede.

A criação de *smart contracts* em uma rede descentralizada apresenta oportunidades de desintermediação de agentes que, nas indústrias tradicionais, cobram por garantir que acordos sejam honrados, praticando o famoso *"rent-seeking"*[12]. O potencial de disrupção de indústrias inteiras não deve ser ignorado. Portanto, instigamos os leitores a pensar nos tipos de serviços que utilizam, e para quais deles dependem de intermediários. Será que a aplicabilidade de contratos inteligentes está restrita à indústria financeira? Poderíamos ver alguma utilidade para eles nas comunicações? E no entretenimento? Ou ainda em uma aplicação pouco intuitiva, como no setor de transportes?

Não é necessário ter muita imaginação para elencar a quantidade de serviços de que dependemos e que poderiam ser desintermediados por uma rede descentralizada e aberta. Muitos dos serviços que usamos hoje em dia têm fortes vantagens competitivas, efeitos de rede de difícil descontinuidade, além de apresentar uma experiência e interface de uso extremamente amigável. No entanto, acreditamos mesmo assim que as soluções reveladas através das criptos tragam os incentivos corretos para que haja, a longo prazo, uma quebra do status quo. Estamos animados para acompanhar o desenvolvimento do setor e a possível/provável resposta dos incumbentes.

[11] *Rollups*
Referência às soluções de segunda camada ("*Layers 2's*") para escalabilidade da rede Ethereum.

[12] *Rent-Seeking*
Termo que se refere a agentes que procuram receber vantagens econômicas sem que haja uma contribuição recíproca de valor entre as partes. Pode-se argumentar, por exemplo, que as tarifas bancárias que grandes bancos cobram de seus clientes, em muitos casos sem transparência e recorrentemente indevidas, sejam fruto do mesmo.

7. Conclusão

As narrativas têm um papel fundamental na nossa compreensão de onde viemos e para onde vamos. Por isso, devido à falta de contextualização de muitos, não nos surpreende que grande parte das críticas aos criptoativos sejam baseadas em análises muitas vezes superficiais e focadas no estado atual, sem levar em consideração o cenário de futuras possibilidades.

Se apresentássemos uma tecnologia nova, que fosse implementada sobre uma rede de computadores descentralizada, baseada em protocolos abertos, extremamente lenta, de difícil acesso, cheia de "golpistas" procurando ganhos rápidos, especulação de preços nas máximas e poucas aplicações realmente inovadoras, acreditamos que o leitor ficaria cético a respeito de seu futuro. No entanto, essa é uma definição perfeitamente plausível de como funcionava a internet nos anos 90. Não basta, portanto, abordar o tema unicamente sob a ótica do estado atual de desenvolvimento. Procuramos, por isso, contextualizar o avanço dos criptoativos com a história da internet e suas respectivas evoluções.

Ressaltamos também que, assim como no mundo físico, onde estabelecemos regras comuns para a propriedade, é natural que na era digital também devamos construir consensos. Na realidade offline, as regras variam de acordo com fronteiras geográficas e, na maior parte dos casos, são claras e definidas. No entanto, essas regras continuam sujeitas a intervenções de entes centralizadores com poder maior que o individual.

No mundo digital, existe uma grande dificuldade de assegurar a posse de ativos, pois estes podem ser reproduzidos indefinidamente, com facilidade. Vemos, então, que o surgimento de uma tecnologia que permita um registro imutável e com regras claras viabiliza pela primeira vez na era digital a aplicação da propriedade privada. Protocolos abertos e globais poderão servir como base para a criação da "verdadeira propriedade", com o empoderamento do direito individual.

Nesta primeira carta, abordamos os principais pilares desta nova tecnologia, desde a tecnicidade de blockchains e DLTs, às aplicações reais das tecnologias supracitadas, como Bitcoin e Ethereum. Esperamos que esta carta tenha servido de *"Layer 0"*[13] de conhecimento sobre a infraestrutura que está sendo desenvolvida nessa nova fase da internet. Na próxima carta, abordaremos as aplicações que tais blockchains trazem à mesa e maneiras de interagir com a propriedade na era digital.

[13] *Layer 0*
Termo que usamos aqui para classificar a camada de conhecimento mais fundamental sobre o tema. *Layer 0* pode ter diferentes significados, a depender de seu contexto de uso.

"I am always doing what I cannot do yet, in order to learn how to do it.", Vincent Van Gogh

Atenciosamente,

Equipe Occam Brasil