João Guilherme Lyra

BLOCKCHAIN

E ORGANIZAÇÕES DESCENTRALIZADAS

Conheça a tecnologia por trás do bitcoin

BRASPORT

João Guilherme Lyra

BLOCKCHAIN

E ORGANIZAÇÕES DESCENTRALIZADAS

Conheça a tecnologia por trás do bitcoin

BRASPORT

BLOCKCHAIN

E ORGANIZAÇÕES DESCENTRALIZADAS

João Guilherme Lyra

BLOCKCHAIN
E ORGANIZAÇÕES DESCENTRALIZADAS

Para uma melhor visualização deste e-book sugerimos que mantenha seu software constantemente atualizado.

Editor: Sergio Martins de Oliveira

Gerente de Produção Editorial: Marina dos Anjos Martins de Oliveira

Editoração Eletrônica: SBNigri Artes e Textos Ltda.

Capa: Use Design

Produçao de e-pub: SBNigri Artes e Textos Ltda.

a pessoas ou bens, originados do uso deste livro.

ISBN Digital: 978-85-7452-912-7

BRASPORT Livros e Multimídia Ltda.

Rua Teodoro da Silva, 536 A – Vila Isabel

20560-001 Rio de Janeiro-RJ

Tels. Fax: (21) 2568.1415/2568.1507

e-mails:

marketing@brasport.com.br

vendas@brasport.com.br

editorial@brasport.com.br

site: www.brasport.com.br

Filial

Av. Paulista, 807 – conj. 915

01311-100 – São Paulo-SP

Agradecimentos

Crescemos escutando o provérbio das três metas de uma vida: plantar uma árvore, ter um filho e escrever um livro. Seguramente considerarei as duas primeiras opções antes de me dedicar a escrever um próximo livro. Trata-se de um trabalho complexo, que exige extrema dedicação do autor e a contribuição de muitos. Por isso, gostaria de agradecer:

Aos meus pais, Fernando Lyra e Cristina Lyra, minha fiel revisora, que priorizam ter um filho. Minha irmã, Maria Fernanda Lyra. Minha sobrinha Manuela Lopes e à Peppa Pig, que a hipnotizava e me permitia continuar a desenvolver este material. A Monica Matera e Leonardo Lopes, que são parte dessa linda família. A Bianca Martins, Maísa Rego, Juliana Lyra, Rejane Lyra e a meus padrinhos, tios e primos, que felizmente são muitos, das famílias: Lyra, Rego, Parente e Inoue. Aos meus avós e ao meu tio Francisco Lyra, que seguramente estão felizes com este trabalho. E ao cão Greek.

Meus amigos Bruno Sepúlveda e Vladmir Pires Ferreira, que pacientemente sempre me auxiliaram neste material. Ao meu amigo Pablo Veloso, que acredita nesse novo mundo. À minha amiga Edna Mendes. Ao Carlos Augusto Freitas, que abriu as portas para que este material tenha se concretizado. A meus grandes companheiros de Blockchain Brasil: Evandro Matias e Marcela Gonçalves. A Augusto Sitio, Everton Melo, Liliane Arazawa, Mauro Real, Renan Saisse e Vinicius Oliveira, que sempre contribuíram e compartilharam conteúdos interessantes que fazem parte deste livro. Ao Alex Braz, Pedro Gutierrez e Alexis, da equipe NEM LATAM. A Mario Solis, Ricardo Ruano e Horácio Huerta.

Aos meus professores da Universidade Federal Fluminense: Bianca Feitosa, Dilma Pimentel, Mirian Picinini, que sempre me apoiaram em pesquisas e

estudos. E em especial ao grande professor Marcelo Meiriño, por todo o apoio e pela confiança.

Agradeço à Brasport por acreditar nesse projeto e dar a oportunidade aos brasileiros de explorar novas tecnologias. Um agradecimento em especial para Marina Oliveira, pela paciência e toda a ajuda ofertada. A Christian Sillaber, pela autorização da imagem de sua idealização.

Este trabalho é de vocês também!

“Eu falo de amor à vida, você de medo da morte
Eu falo da força do acaso e você, de azar ou sorte
Eu ando num labirinto e você, numa estrada em linha reta
Te chamo pra festa mas você só quer atingir sua meta

Sua meta é a seta no alvo
Mas o alvo, na certa não te espera

Eu olho pro infinito e você, de óculos escuros
Eu digo: ‘Te amo’ e você só acredita quando eu juro
Eu lanço minha alma no espaço, você pisa os pés na terra.
Eu experimento o futuro e você só lamenta não ser o que era
E o que era? Era a seta no alvo
Mas o alvo, na certa não te espera

Eu grito por liberdade, você deixa a porta se fechar
Eu quero saber a verdade, e você se preocupa em não se machucar
Eu corro todos os riscos, você diz que não tem mais vontade
Eu me ofereço inteiro, e você se satisfaz com metade

É a meta de uma seta no alvo

Mas o alvo, na certa não te espera

Então me diz qual é a graça

De já saber o fim da estrada

Quando se parte rumo ao nada?

Sempre a meta de uma seta no alvo

Mas o alvo, na certa não te espera

Então me diz qual é a graça

De já saber o fim da estrada

Quando se parte rumo ao nada...”

(Paulinho Moska, “A Seta e o Alvo”)

Contexto do Livro

Em meados de 2018, existiam mais de 1.600 projetos de Organizações Descentralizadas (DOs) e criptoativos no mundo, muitos em fase de desenvolvimento de seu protocolo e aplicação e outros já atuantes e oferecendo serviços. Pode-se ainda acrescentar a esses números os mais de 1.000 projetos de DOs que estão em busca de financiamentos coletivos no mundo virtual. Trata-se de um mercado de mais de meio trilhão de dólares que não atrai a atenção de muitos, mas que já é uma realidade.

A tecnologia blockchain ainda possui pouca literatura acadêmica em português. Em relação a organizações descentralizadas e autônomas, não é encontrada nenhuma publicação em busca no portal CAPES até o dia 12 de janeiro de 2018.

Sendo assim, este livro busca estudar os novos modelos de gestão e as variáveis que influenciam essas organizações que surgem com a tecnologia blockchain. Embora citemos diversos casos, projetos e uma tendência de crescimento, este material busca oferecer uma visão mais holística dessas organizações, buscando maior perenidade no conhecimento compartilhado.

As DOs são novas formas de organizações que buscam ofertar serviços e distribuir lucros de forma autônoma, principalmente por modelo de crowdsource. Essas organizações completamente horizontais não possuem espaço físico, podem não estar sediadas em nenhum país e seus níveis de descentralização podem alcançar qualquer localidade onde haja internet. Entender a dinâmica dessas organizações, sua estrutura horizontal e ausência de departamentos clássicos é fundamental para governos, academia, desenvolvedores e mercado.

Sumário

Endereço ou chave pública

Chave privada ou senha

Token

Criptografia

Função hash criptográfica

Timestamp (carimbo de tempo)

Ledger ou nodos completos

Consenso e mineração

Bloco

Blockchain (cadeia de blocos)

Fluxo do blockchain

Capítulo 4. ICOs – Ofertas Iniciais de Moedas

Critérios de análise de ICOs

Equipes

Divulgação e marketing

Ideia de produto

Viabilidade

Legalidade

White paper (descrição do projeto)

Modelos de vendas de token

Pré-vendas privadas

Limites fixos (capped sale)

Introdução

“Compositor de destinos, tambor de todos os ritmos

tempo, tempo, tempo, tempo, entro num acordo contigo”

(Caetano Veloso, “Oração ao Tempo”)

Os avanços tecnológicos das últimas décadas mudarão significativamente a sociedade e sua forma organizacional. Como as primeiras revoluções industriais, que estimularam o êxodo rural e proporcionaram o surgimento de megalópoles ao longo do tempo, o nascimento de tecnologias como inteligência artificial, automação da indústria 4.0, impressoras 3D e a biotecnologia remodelará nossas sociedades futuras e afetará por completo o atual conceito de trabalho.

Durante dois séculos as pessoas dedicaram seus tempos de estudos para atender às necessidades do mercado industrial. Os cursos de engenharia encheram salas de aulas com pessoas que buscavam atender à qualidade exigida pelo mercado corporativo. A sociologia perdeu espaço para os cursos de economia. As visões holísticas dos filósofos foram supridas pelas visões corporativas dos administradores e suas formulações de conceitos de missão, valores e metas organizacionais. Mas o momento atual é de completa incerteza das profissões que existirão no futuro. A Foundation for Young Australians (FYA, 2015) prognostica que 60% dos australianos dedicam seus estudos a postos de trabalhos que serão afetados drasticamente pela automação. O professor Yuval Noah Harari (2016) acredita que, com auxílio da biotecnologia num futuro próximo, poderão surgir uma elite de super-humanos cyborgs e uma massa de inúteis.

Diversos outros estudos sobre impactos das tecnologias e o futuro do trabalho alimentam relatórios intrigantes. O relatório do Fórum Econômico Mundial (WEF, 2016) estima que 7,1 milhões de empregos desaparecerão no mundo até 2020. A pesquisa de 2017 do IFTP (Institute for the Future) prevê que, até 2030, aproximadamente 85% do mercado de trabalho será composto por profissões que nem foram inventadas. Esses dados estimulam mudanças urgentes na sociedade. Os cidadãos que estão sendo formados para o mercado de trabalho não atenderão aos requisitos necessários para sua manutenção econômica futura.

O acrônimo VUCA (Volatility, Uncertainty, Complexity, Ambiguity) surge a partir de palavras que foram encontradas em diversas entrevistas por executivos para descrever um ambiente que desafia as previsões empresariais sobre seus negócios. Os líderes são incapazes de prever suas estratégias com segurança. Torcem mais por acertar suas apostas de negócios, pois realmente é impossível traçar estratégias que enxerguem os inúmeros cenários possíveis (BENNET; LEMOINE, 2014). Este livro não é um exercício de futurologia, então vamos refletir sobre acontecimentos passados.

A cidade de Detroit, exemplar da prosperidade da indústria americana no século passado, atualmente se encontra em ruínas. Mais da metade de sua população se mudou da cidade em busca de oportunidade de empregos em outros locais. A cidade que declarou falência em 2013 faz de tudo para se reinventar economicamente até hoje. Já do outro lado dos Estados Unidos, o estado da Califórnia é exemplo de prosperidade econômica. O Vale do Silício se tornou um grande cluster das maiores empresas de tecnologia do mundo. Com a presença de Google, Apple, Facebook, a Califórnia, se fosse um país, hoje seria a quinta maior economia do mundo, superando os PIBs de Inglaterra ou Brasil.

A Alemanha é a maior economia da Europa e possui uma das menores médias anuais de horas trabalhadas pelos alemães. Já a Grécia, uma das economias mais fracas da Europa, possui uma das maiores médias de horas de trabalho no continente europeu. A Coreia do Sul, que há mais de uma década reduz a média de horas anual do trabalhador, se tornou um país exemplo de prosperidade

econômica para o mundo.

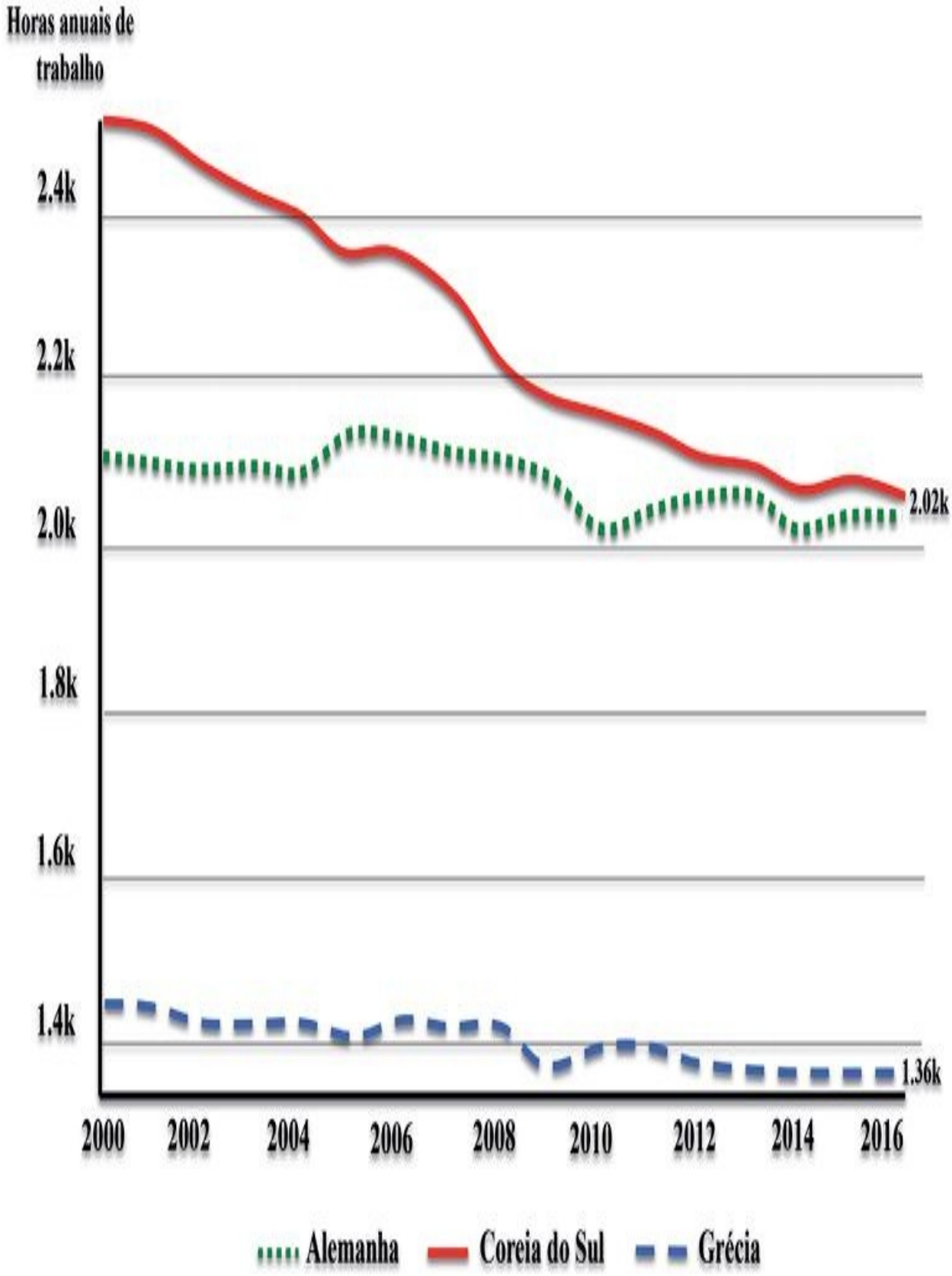

Horas anuais de trabalho
2.4k
2.2k
2.0k
1.8k
1.6k
1.4k
2.02k
1.36k
2000
2002
2004
2006
2008
2010
2012
2014
2016
Alemanha
Coreia do Sul
Grécia

Figura 1. Média de horas anuais de trabalho: Alemanha, Coreia do Sul e Grécia.

Fonte: adaptada de OCDE, 2018.

A Coreia do Sul, com os investimentos educacionais e avanços tecnológicos das últimas décadas, conseguiu um crescimento econômico mesmo reduzindo a jornada de trabalho. Assim, é possível levantarmos a hipótese de que o trabalho não representa mais progresso econômico. Para Pistono (2017), a tecnologia criará um futuro com menos horas de trabalho e mais tempo livre a todos. Claro que isso não é um problema, o problema é como essas pessoas serão economicamente ativas.

Na maior parte do mundo a participação dos salários no PIB (Produto Interno Bruto) dos países sofreu queda. Na Coreia do Sul o percentual de representatividade dos salários no PIB do país era de 57% em 1996 e hoje é de 52%. Na Alemanha a contribuição dos salários no PIB nacional era de 66% no ano 2000 e hoje representa 62%. A diferença seria pouca se nesses países o PIB não estivesse aumentando. Na Grécia, onde a média de horas trabalhadas não sofreu mudanças drásticas, a participação do salário no PIB caiu próximo de 5%. Então se a produtividade está aumentando, as horas médias de trabalho diminuindo e a participação do salário caindo, como explicar essa diferença?

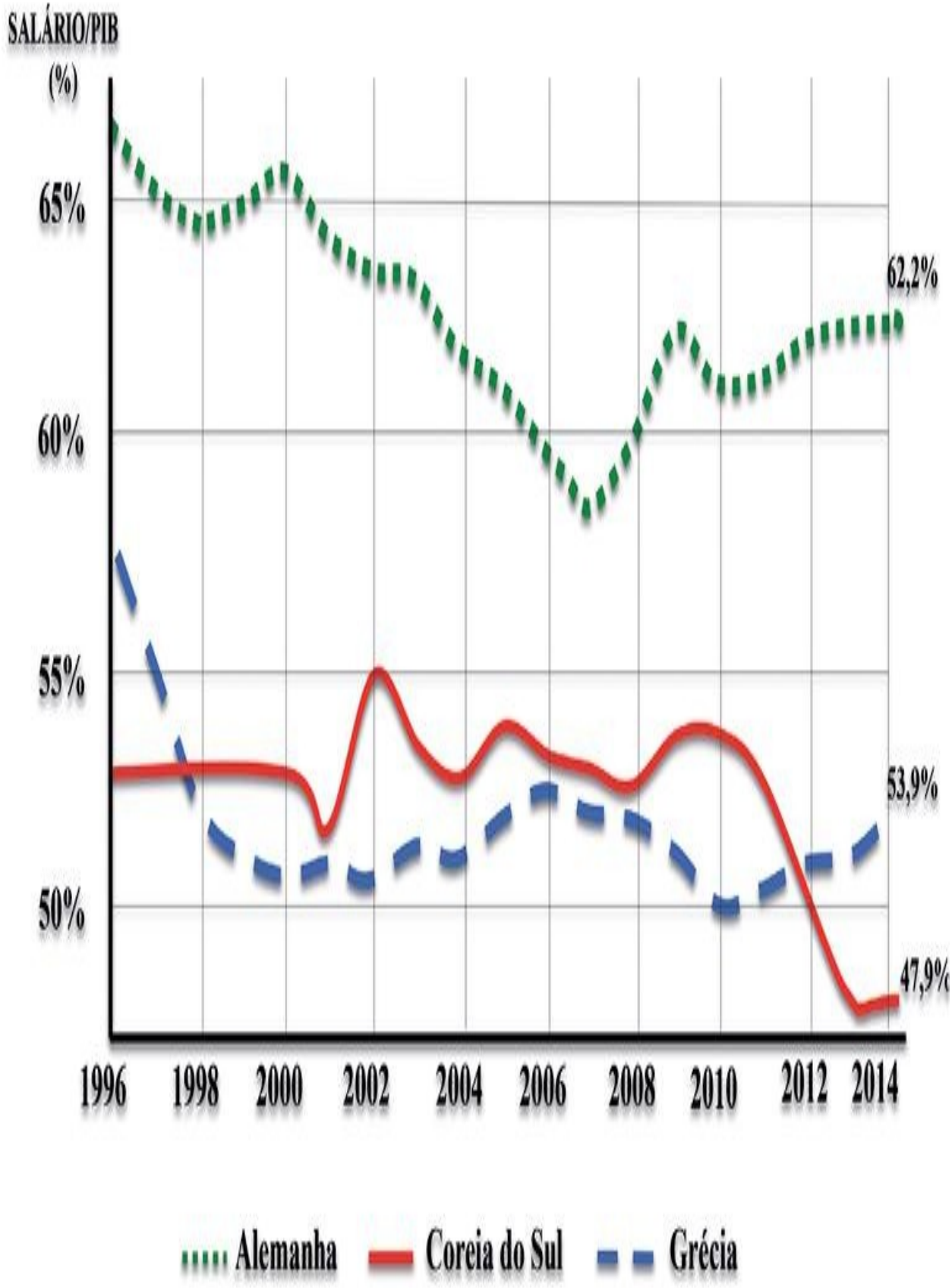

SALÁRIO/PIB
(%)
65%
60%
55%
50%
62,2%
53,9%
47,9%
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014
Alemanha
Coreia do Sul
Grécia

Figura 2. Participação dos salários no PIB: Alemanha, Coreia do Sul, Grécia.

Fonte: Universidade de Groningen. Adaptada de FRED, 2014.

Em 2016 a Suíça realizou um plebiscito sobre uma proposta de renda básica de 4 mil francos suíços mensais, e os principais argumentos dos defensores da renda básica universal era que a automação e a tecnologia irão desaparecer com os empregos, e a Suíça deveria já se preparar para esse futuro, tornando todos os seus cidadãos economicamente ativos. Embora a população suíça tenha rejeitado a proposta, vemos que a preocupação com a economytech já ocupa as agendas governamentais.

Além disso, para Chomsky (2017), houve uma "financeirização" da economia. As grandes empresas hoje não focam mais na produção, e sim no sistema - financeiro. Metade dos lucros da General Electric Group vem de aplicações financeiras. A General Electric possui em seu conglomerado a GE Capital, que busca financiar seus produtos.

Um case famoso de sucesso de financeirização no Brasil foi o da Casas Bahia. A rede varejista de eletroeletrônicos chegou a possuir 14 milhões de cadastros de usuários de crediários. Em seu auge, se a Casas Bahia fosse um banco, seria o quarto maior do Brasil. Mais de 60% das vendas da varejista eram financiadas (BLECHER, 2004).

Com uma economia mundial voltada para o setor financeiro, em 2016 os governos mundiais atingiram um recorde de endividamento superior aos anteriores à crise de subprime de 2008. O total da dívida dos países foi de 225% do PIB mundial (IMF, 2018). Se forem incluídas as dívidas de empresas e famílias nesse patamar, estas representariam, em 2018, 316% do PIB mundial. Esses dados indicaram novos recordes. Se o mundo quisesse pagar sua dívida,

teria que produzir, por mais de três anos, exclusivamente para isso (IIF, 2018). Quando se juntam esses dados à financeirização da economia, pode-se compreender melhor por que a participação do salário no PIB cai na maioria dos países. O empresário, atualmente, busca financiamentos para comprar máquinas mais modernas, o que reduz emprego, aumenta sua dependência do sistema financeiro e diminui a participação do trabalhador na economia.

Esses fatores não têm inibido o crescimento do PIB mundial, bem como os lucros empresariais e muito menos a desigualdade mundial. Inúmeras pesquisas afirmam que apenas 1% da população teria 82% da riqueza mundial.

Faixa de renda	Perdas/Ganhos anuais da faixa	Média de perda/ganho familiar da faixa
Top 1%	+ 673 bilhões	+ 597.241
96-99	+ 140 bilhões	+ 29.895
91-95	+ 29 bilhões	+ 4.912
81-90	- 43 bilhões	- 3.733
61-80	- 194 bilhões	-8.598
41-60	- 224 bilhões	- 10.100
21-40	- 189 bilhões	- 8.582
Base dos 20%	- 136 bilhões	- 5.623

Valores em Dólares. Comparação entre os anos de 1979-2005. Pesquisa de Jacob Hacker, Yale University; Paul Pierson, UC- Berkeley.

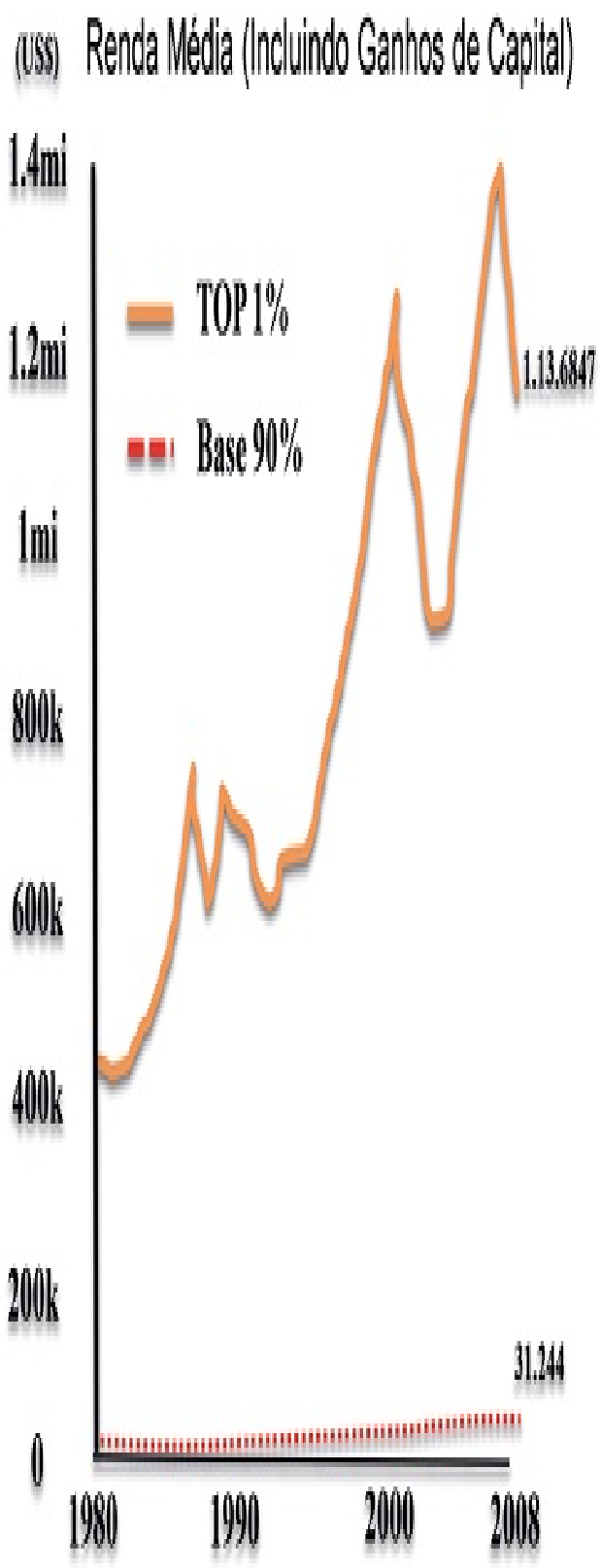


Figura 3. Aumento da desigualdade. Fonte: adaptada de GILSON; PEROT, 2011.

Quando há discrepância na estrutura de uma sociedade, ela sempre se mobiliza para ajustá-la (REICH, 2016). Pistono (2017) não tem ilusões: sem empregos, ou se adota um novo contrato social ou o sistema todo vai entrar em colapso.

Movimentos socioeconômicos hodiernos, apoiados por tecnologias e ideologias cyberpunks e criptoanárquicas, têm criado novos arranjos organizacionais. Com o suporte da confiança oferecida pela tecnologia blockchain, às margens do sistema financeiro e corporativo tradicional, nascem as organizações descentralizadas (DOs) em grande escala. Sem hierarquia, com financiamento coletivo, com ecossistema de valia própria, abertas e participativas, as organizações descentralizadas já nascem com alcance global. E estas, muitas vezes, não podem ser consideradas multinacionais, pois estão fora de qualquer jurisdição. Habitam um novo mundo digital.

Em 2008, distante dos holofotes dos noticiários econômicos, que se voltavam para a crise do subprime e os resgates dos governos a bancos privados, foi publicado um artigo assinado por Satoshi Nakamoto propondo uma nova forma de transferências de valor pela internet. No paper “Bitcoin: A Peer-to-Peer Electronic Cash System”, Nakamoto propôs a solução de gastos duplos para uma rede ponto a ponto, sem a necessidade de um terceiro confiável para validação das operações.

Antonopoulos (2014) afirma que o bitcoin representa o auge das pesquisas em criptografia e sistemas distribuídos e inclui quatro inovações-chave reunidas em uma combinação perfeita. O bitcoin consiste em:

• Uma rede peer-to-peer descentralizada (o protocolo bitcoin).

• Um registro público de transações (a blockchain ou cadeia de blocos).

• Uma emissão de moeda descentralizada, matemática e determinística (a mineração distribuída).

• Um sistema descentralizado de verificação de transações (o script de transação).

A grande revolução do modelo de transferência de valor do bitcoin é a sua plataforma, o blockchain. Blockchain é um conjunto de registros contábeis públicos distribuídos, transparentes, imutáveis e sincronizados. Características que fizeram a conceituada revista “The Economist” classificar a tecnologia como “a máquina da confiança” (2015).

As possibilidades de aplicações do blockchain vão além de aplicações financeiras e baseiam as estimativas de crescimento exponencial desse mercado. Em 2016 apenas 0,025% do PIB mundial circulava nas plataformas blockchain, mas, segundo estimativas do Fórum Mundial Econômico (WORLD ECONOMIC FORUM, 2016), em 2022 o valor que circulará nesse mercado representará 10% do PIB mundial. Já a consultoria Gartner (2017) estima que em 2022 negócios baseados em blockchain valerão 10 bilhões de dólares – valores alcançados bem antes do previsto, pois já em 2018 mais de cinco organizações descentralizadas superaram esses valores de mercado.

Criadas dentro de plataformas blockchain, as organizações descentralizadas (DOs) representam uma inovação nas estruturas organizacionais e possuem

ênfase em regras e contratos computadorizados, estruturas verticalizadas, descentralizadas e criptoanárquicas (CHOHAN, 2017). Entende-se o conceito de anárquica em relação à ausência de hierarquia e centralizadores, junto ao conceito de Anarquia Ordenada de Buchanan (MONTARROYOS, 2006), não o uso pejorativo da ideologia de desordem e caos. No entanto, as estruturas e funções das DOs também levantam questões de governança que exigem atenção e práticas urgentes, particularmente porque DOs ainda são consideradas entidades um pouco difíceis de serem descritas, e o status legal exato do tipo organizacional da DO é ainda indeterminado (CHOHAN, 2017b).

Capítulo 1. Precedentes Históricos

“Só há amor quando não existe autoridade”

(Raul Seixas)

Até hoje, em uma minúscula ilha do Pacífico chamada Yap, está localizado um dos sistemas monetários mais sólidos do mundo. Sua moeda é tão sólida como uma rocha. De fato, as moedas do povo Yap são rochas, rochas calcárias. Há mais de 1.500 anos os yapeses usam grandes discos de pedras para compras de casas, canoas e licenças para casamento. Comprar uma casa com pedras, em Yap, é mais fácil que com dólares. Produtos de menor valor, como cerveja, hoje já são adquiridas com dólares.

As moedas de Yap são redondas, forma inspirada pela lua, e possuem um grande círculo no centro, para facilitar o transporte da pedra. A maioria das pedras tem entre 75 cm a 1,5 m de diâmetro, mas algumas podem chegar a 3,5 m. São necessários até vinte homens para levantar algumas pedras. Como as pedras perdem valor se quebradas, o povo Yap não costuma mover as pedras, mesmo quando estas mudam de proprietários. A contabilidade é feita mentalmente, e o reconhecimento de propriedade da pedra é feito por toda a comunidade, pois as moedas ficam expostas nas próprias ruas de Yap[1].

STONE MONEY OF UAP, WESTERN CAROLINE ISLANDS.

(From the paper by Dr. W. H. Furness, 3rd, in Transactions, Department of Archæology, University of Pennsylvania, Vol. I., No. 1, p. 51, Fig. 3, 1904.)

Figura 4. Moedas de pedra do Povo Yap. Fonte: Wiki Commons. Autor: Dr. William Henry Furness, 1910. Domínio público.

O sistema monetário do povo Yap é bastante semelhante à confiança distribuída oferecida pelo blockchain:

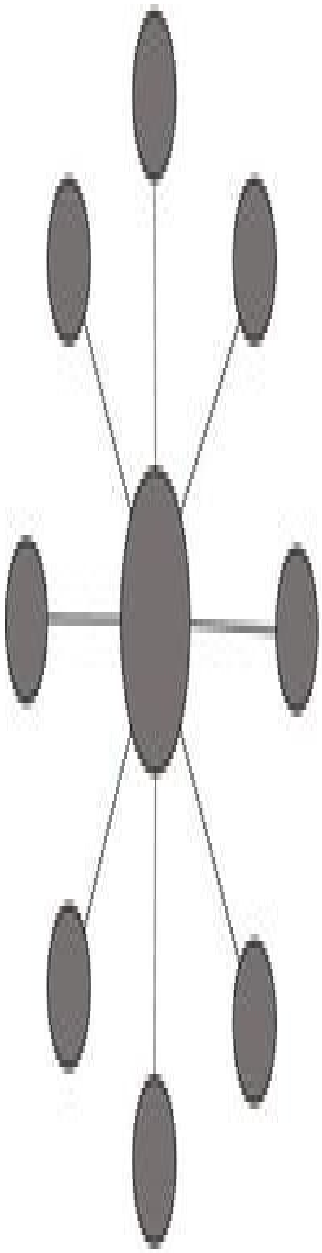
• A confiança é descentralizada, não há necessidade de bancos ou intermediários para assegurar a propriedade. A propriedade é reconhecida pelo consenso dos participantes do sistema.

• Assim como as pedras de Yap, para se roubar o sistema, seria necessária a ajuda de outros participantes, além de um grande esforço. Como em Yap são necessários até vinte homens para mover uma pedra, no blockchain haveria necessidade da participação de quase metade dos usuários para realizar qualquer fraude.

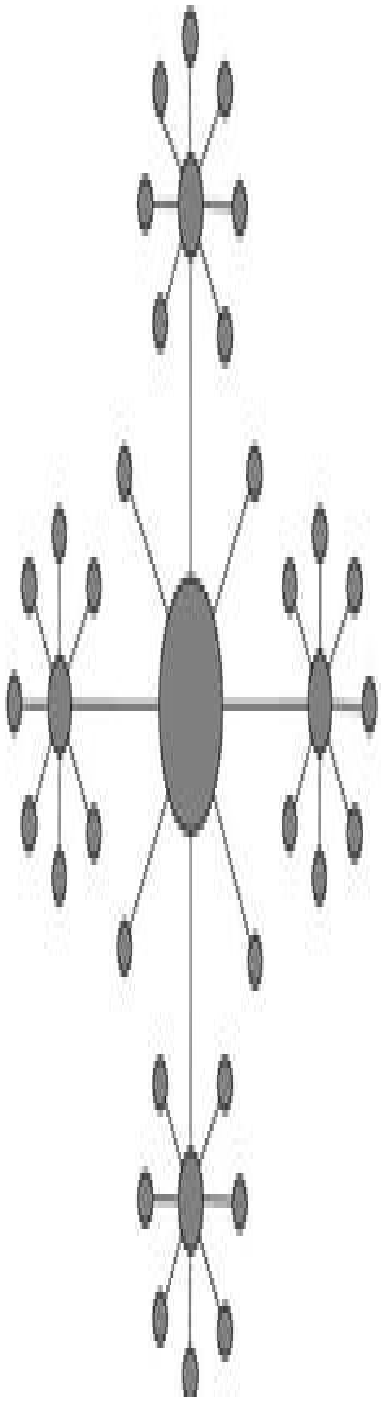
• A transparência do sistema é a segurança. As pedras de Yap ficam exibidas nas ruas igual aos ativos de um blockchain, que podem e devem estar expostos a todos os participantes da rede.

Na tecnologia da informação, a comunicação distribuída é pioneirismo do engenheiro Paul Baran, que em 1964 formulou o modelo distribuído para comunicações militares, pois percebia a vulnerabilidade nos centros de comunicações. Se estes fossem destruídos pelos inimigos, as tropas do campo ficariam sem comunicação.

Centralizado



Descentralizado



Distribuído

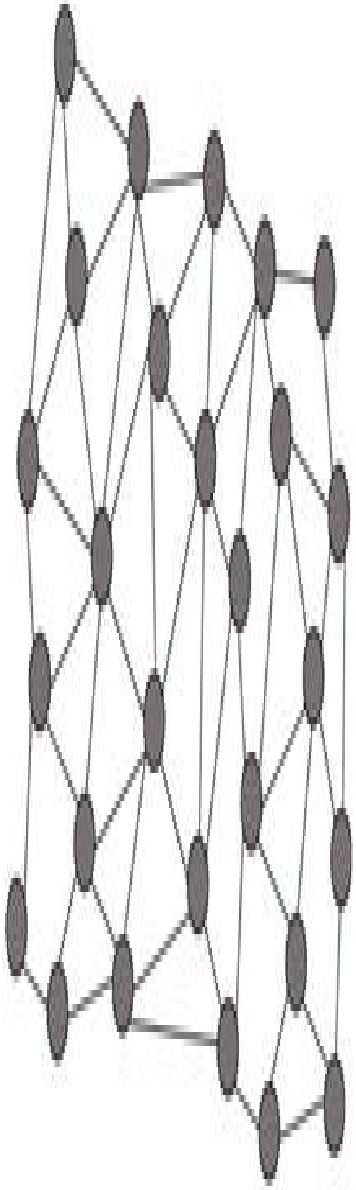


Figura 5. Rede de comunicação distribuída. Fonte: adaptada de Paul Baran, 1964.

A evolução das transmissões das informações inicia-se com modelos centralizados, passando para um modelo descentralizado, pela necessidade de facilitar o acesso e a capilaridade aos sistemas centrais. A tecnologia blockchain elimina os órgãos centralizadores, adotando o modelo distribuído. Embora muitos autores classifiquem o sistema blockchain como descentralizado, percebe-se que os blockchains se assemelham aos estudos propostos pelo engenheiro Paul Baran em “On Distributed Communications Network”, de 1964.

A ideia de moeda digital descentralizada se tornou um desafio que ultrapassou décadas. Protocolos de e-cashes (dinheiro eletrônico) anônimos foram criados nos anos 1980 e 1990 e, já com uso de criptografia, possuíam elevado grau de privacidade, mas, em grande parte, não conseguiram ganhar força devido à sua dependência de um intermediário. O b-money, criado por Wei Dai em 1998, foi o pioneiro em introduzir a proposta de resolução de puzzles (quebra-cabeças) computacionais para um consenso descentralizado. A fragilidade do b-money estava nos detalhes sobre como o consenso descentralizado poderia ser implementado. Em 2005, Hal Finney desenvolveu um conceito de “provas reutilizáveis de trabalho”. O sistema usava a ideia do b-money juntamente com os enigmas computacionais de Hashcash criado por Adam Back, surgindo o conceito de cryptocurrency, mas ainda não era satisfatório quanto ao quesito da saída do processo (backend), o que dificultava o processo de consenso descentralizado. O principal obstáculo para todas essas moedas pré-bitcoin eram as falhas bizantinas, que foram resolvidas somente em partes (BUTERIN, 2014a).

A resolução do “problema dos generais bizantinos” na computação P2P se apresenta como um dos principais avanços tecnológicos do sistema de bitcoin. Esboçado na Teoria dos Jogos com aplicação na segurança da computação, o dilema dos generais bizantinos poderia ser ilustrado assim: generais, cada um no

topo de montanhas, se preparam para um ataque conjunto a seus inimigos que estão no vale. O ataque ao inimigo deve ser em conjunto e no mesmo horário. Como os generais poderiam enviar mensageiros informando o horário sem que eles fossem capturados por seus inimigos? E, mesmo se os mensageiros conseguissem escapar dos inimigos, como os generais saberiam que a mensagem foi recebida? Seria necessário o envio de outro mensageiro para confirmar o recebimento da mensagem. Mas mesmo assim sempre ficaria a dúvida se a mensagem de confirmação do recebimento foi realmente entregue. Isso criaria uma infinita necessidade de confirmações de recebimento de mensagens, e a Teoria dos Jogos ainda é acrescentada ao dilema da possibilidade de traição de algum dos generais, o que aumenta a insegurança das transmissões da informação (KENNARD, 2015). Trata-se de um ambiente inseguro e traiçoeiro muito próximo ao que ocorre no compartilhamento de dados na internet.

Mougayar (2016) afirma que o importante é compreender as soluções do protocolo proposto por Nakamoto:

• Possibilita transações em uma rede peer-to-peer (P2P) sem necessidade de intermediários.

• Os registros possuem uma criptografia de difícil violação, tornando os registros imutáveis.

• As transações possuem registro de data e hora (timestamp), que, junto com a criptografia do sistema, cria uma cadeia progressiva de transações.

• Resolve o problema da Teoria dos Jogos conhecido como “Generais Bizantinos” nas redes ponto a ponto (P2P), o que evita gastos duplos.

• As validações das transações são realizadas por todos os usuários, pois todas as transações são distribuídas a todos, que atualizam seus registros próprios, os ledgers.

Mas quais são os elementos essenciais de um blockchain que possibilitam a resolução do Dilema dos Generais Bizantinos e viabilizam essa inovação?

Elementos básicos dos blockchains

Antonopoulos (2014) esclarece boa parte dos componentes de um blockchain.

Rede e nodos

Uma rede ponto a ponto (peer-to-peer) propaga transações e blocos para cada nó de bitcoin na rede. Existem alguns tipos de nodos em uma rede: carteira, minerador, nodo completo e roteador da rede. Todos os nodos incluem a função de roteamento para participar na rede e podem incluir outras funcionalidades (ANTONOPOULOS, 2014).

Os chamados nodos completos possuem cópia completa e atualizada do blockchain. Os nodos completos podem verificar de maneira autônoma e autoritária qualquer transação sem referência externa (ibid.).

As carteiras de usuários podem fazer parte de um nodo completo, que é o que geralmente ocorre em clientes desktop do bitcoin (ibid.).

Endereço ou chave pública

Um endereço em um blockchain é semelhante a um e-mail, no qual se pode enviar e receber de outras pessoas as unidades de troca daquele bloco. O endereço da rede blockchain é criptografado e, ao se criar um endereço, simultaneamente é criada uma chave privada ou senha (ibid.). A interface com o endereço é realizada pelas carteiras.

Um endereço de uma rede blockchain se parece com:
3JowMKcM3R3ErnNLW4XT2sjs6tGzpwRzgd

Chave privada ou senha

É a única forma de acesso para destravar os tokens e enviar para um determinado endereço. Se houver perda dessa chave, não há como mover os tokens desse endereço (ibid).

Uma chave privada se parece com:

7R46xG3L6jTyzE96r66Sg3xka6y46whpJjMwCxR3tzLh3fbVOtu.

Token

Unidade de troca de uma cadeia de blocos que pode assumir diferentes funções: votos, registros, atestado, utilitário, direito de propriedade, ativos, currency e identidades (ANTONOPOULOS; WOOD, 2018). Muitas vezes um token assume mais de uma dessas funcionalidades e é chamado de híbrido.

Criptografia

As informações em um blockchain só podem ser compartilhadas de forma pública graças à criptografia utilizada. A maioria das cadeias de blocos usa curvas elípticas em sua criptografia. A criptografia das transações de bitcoins utiliza o modelo de curvas elípticas, sendo assimétricas, baseadas em logaritmos discretos expressados pela adição e multiplicação nos pontos de uma curva elíptica. Essas funções matemáticas não podem ser derivadas. São funções que podem produzir novos resultados, mas não voltam ao resultado anterior. Simplificando a ideia, os cálculos só andam para frente e formam uma cadeia crescente de registros (ANTONOPOULOS, 2014).

O modelo utilizado no bitcoin é a curva secp256k1, estabelecida pelo Instituto Nacional de Padronização e Tecnologia (ibid.). As criptografias utilizadas são SHA-256 e a sua evolução, a SHA-3, que possui 512 bits, o dobro de bits da sua antecessora.

Algumas cadeias de blocos dizem já estar preparadas para criptografia pós-quântica, como IOTA, Quantum Resistant Ledger (QRL), Mochimo, entre outras. Atualmente já existem diversos projetos que dizem possuir criptografia resistente à computação quântica. Embora não seja um projeto aberto, pesquisadores russos do RCQ (Centro Russo de Quantum) informaram terem criado o primeiro blockchain quântico[2]. Outros blocos também já estudam a implementação de criptografias pós-quânticas, como Verge, Ethereum, entre outros.

A blockchain QRL utilizará o Extended Merkle Signature Scheme (XMSS), que se apresenta como resistente a ataques de computação quântica. Porém, é consenso entre os criptografistas que uma criptografia só pode ser considerada

segura quando muito testada, algo que não ocorreu com a maioria das propostas pós-quânticas. Assim, a criptografia é a maior segurança dos blockchains atuais e a computação quântica, a maior ameaça a todos os sistemas criptografados do mundo.

Função hash criptográfica

Uma função hash criptográfica é uma função unidirecional que mapeia dados de tamanho arbitrário para uma cadeia de bits de tamanho fixo. É inviável computacionalmente recriar a entrada, mesmo se a pessoa souber a saída. A única maneira de determinar a entrada é realizar teste de força bruta dos possíveis inputs, verificando se há uma saída correspondente (ANTONOPOULOS, 2014), algo tão difícil e custoso que seria como querer transformar produtos muito processados como os nuggets do McDonald's em galinhas novamente[3].

As hashes criptográficas são usadas nas criações dos endereços, em chaves privadas, na árvore merkle dos blocos, no timestamp, mas comumente são usadas para se referir aos registros de transações de um blockchain.

Uma transação é feita de um endereço a outro, onde o emissor assina a transação com sua chave privada única e adiciona o valor de tokens a ser transferido (NAKAMOTO, 2008). Todos esses dados são transformados em uma hash de transação semelhante a:

2c1a47833790adb8b16ba5389cfbb20ef0904882ee6ceb1c96ee2e1af8edcec6.

Timestamp (carimbo de tempo)

Um servidor de carimbo de tempo adiciona às hashes a hora e data, publicando amplamente a informação assim como em um jornal. O carimbo de tempo prova que os dados precisam obviamente ter existido naquele momento para que sejam incluídos na hash. Cada carimbo de tempo inclui o carimbo de tempo anterior em sua hash, formando uma corrente, com cada carimbo de tempo adicional reforçando os anteriores (NAKAMOTO, 2008).

Ledger ou nodos completos

A tecnologia blockchain também é conhecida como DLT (Distributed Ledger Technology). Ledgers, segundo o dicionário Cambridge, é um livro no qual as coisas são registradas regularmente, especialmente atividades financeiras de dinheiro recebido ou pago. Em português, uma adequada tradução seria “livro-razão”, onde são lançadas as entradas e saídas contábeis.

Em um livro-razão distribuído, todos os nodos validam e propagam as transações e blocos, e também encontram e mantêm conexões com outros pontos da rede. Os ledgers mantêm uma cópia completa e atualizada do blockchain. Nodos completos podem verificar de maneira autônoma e autoritária qualquer transação sem referência externa (ANTONOPOULOS, 2014). Eles possuem o timestamp de todas as transações anteriores, e para validar uma transação em um blockchain, como na contabilidade básica, para toda saída deve haver uma entrada anterior.

Todas as transações em um blockchain são enviadas para os usuários da rede, que contabilizam as operações em seus registros individuais de transações, os ledgers. Esse “livro contábil”, ao se tornar público e compartilhado, se mantém atualizado por meio dos blockchains. As transações que não forem reconhecidas pelos ledgers dos usuários do bloco não são válidas (MEIKLEJOHN et al., 2016). Uma vez que um nodo recebe dados de outro nodo, ele verifica a autenticação dos dados em seu próprio ledger. Em seguida, transmite os dados validados para outros nodos conectados a ele. Dessa forma, os dados são espalhados por toda a rede (ZHENG et al., 2018). As transações válidas se propagam como vírus computacionais.

Consenso e mineração

Os nodos dispostos a criar novos blocos e consolidar as transações validadas pelos ledgers são conhecidos como mineradores. Em blockchains abertos, a criação de blocos pode ser usada para emissão de novos tokens da rede, tornando-se uma forma de recompensar o esforço computacional, o apoio dos mineradores. A outra forma de recompensa dos mineradores é a taxa por transação, que pode ser fixa ou negociada pelos mineradores, de acordo com o protocolo do blockchain.

O consenso é a primeira camada da estrutura descentralizada, a base fundamental do protocolo que governa uma estrutura descentralizada. O consenso é o núcleo do blockchain (MOUGAYAR, 2016). É como cada blockchain valida suas transações, podendo ser executado de diferentes formas (ZHENG et al., 2018). Algumas das formas de consenso são:

Prova de trabalho – PoW (Proof-of-Work)

A prova de trabalho foi desenvolvida por pesquisadores entre 1992 e 1993 (SWANSON, 2014). Uma prova de trabalho é um problema probabilístico difícil, caro e demorado de se resolver, mas é fácil para outras pessoas verificarem se os resultados e requisitos necessários estão corretos. São necessárias muitas tentativas e erros, em média, antes que uma prova de trabalho válida seja gerada. Dessa forma, há uma exigência de grande capacidade de processamento de cálculos. Devido à Lei de Moore, a dificuldade do problema a ser resolvido vai aumentando de acordo com o crescimento do poder de processamento dos mineradores, para que se preserve o tempo de criação dos blocos[4].

No caso do bitcoin, os blocos são criados a cada dez minutos e é utilizada a prova de trabalho Hashcash, de Adam Back. Alguns outros algoritmos de hash que são usados para PoW incluem Scrypt, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, scrypt-jane, scrypt-n ou combinações destes.

Prova de participação – PoS (Proof-of-Stake)

A prova de participação provavelmente surgiu no fórum BitcoinTalk por volta de 2011. Em vez de exigir poder de processamento para resolução de problemas probabilísticos, a prova de participação compara a quantidade de tokens que um minerador detém – alguém que detenha 1% dos tokens de uma rede pode criar 1% dos blocos de uma rede[5].

Na prova de participação os mineradores apostariam seus tokens como forma de comprovar que estão preservando a integridade das cadeias de blocos. Se os outros nodos participantes não confirmarem e acreditarem que as transações do bloco minerado sejam falsas, o minerador poderia perder todos os seus tokens. Nesse tipo de consenso, acredita-se que os participantes que possuem mais tokens seriam os principais interessados em preservar a integridade dos registros da cadeia de blocos[6].

Prova de participação delegada – DPoS (Delegated Proof-of-Stake)

Daniel Lamirer teria inventado a DPoS, em 2014, junto à Bitshare. A prova de participação delegada é um sistema próximo ao PoS, sendo que, em vez de os nodos mineradores serem escolhidos pela quantidade de tokens, ela funciona usando sistemas de reputação e votações em tempo real sem atritos para criar um painel de partes confiáveis limitadas. Essas partes têm o direito de criar blocos

para adicionar ao blockchain e de proibir a participação de partes não confiáveis, se revezando na criação dos blocos. Se o minerador tentar fraudar a rede, ele perde sua delegação e com ela sua reputação (LARIMER, 2014).

O número de mineradores varia de acordo com cada rede. Na Bitshare são escolhidos 101 mineradores a cada votação; na Steem, são 21 mineradores delegados, que se revezam na criação dos blocos.

Prova de importância – PoI (Proof-of-Importance)

A prova de importância exige que o nodo minerador possua um valor mínimo de tokens da rede, mas somente isso não basta. Assim como o DPoS utiliza o critério de reputação, no caso da PoI a importância do usuário é verificada pela quantidade de transações executadas em certo período. Isso estimula os nodos a não somente economizar os tokens, mas os usar[7]. Assim como a PoS e a DPoS, a PoI exige menos poder computacional e possibilita maior escalabilidade de transações.

Quanto mais nodos em uma rede, mais distribuída e mais segura ela será. Outras formas de consenso e mineração são: PBFT, RAFT, Paxos, Proof-of-Burns, Proof-of-Capacity, entre outras.

Bloco

Um bloco compreende múltiplas transações (ZHENG et al., 2018). Os blocos são um agrupamento de transações carimbadas com registros de tempo e com uma impressão digital que faz referência ao bloco anterior. Blocos válidos são adicionados a um blockchain através do consenso da rede (ANTONOPOULOS, 2014). Uma transação sendo validada pelos nodos é replicada até um bloco em formação e é confirmada quando esse bloco também for reconhecido como válido pelos nodos.

Blockchain (cadeia de blocos)

Um blockchain é uma coleção bem ordenada de blocos, onde os usuários devem provir o consenso das transações. Isso determina o histórico do controle de ativos e fornece um cálculo determinado de tempo imutável para as transações (BACK et al., 2014). Blockchain é a cadeia de blocos de registros de transações validados pelo protocolo de consenso e incorporados a todos os ledgers de uma rede. Assim como as hashes de transações, a cadeia de blocos faz referência ao bloco anterior.

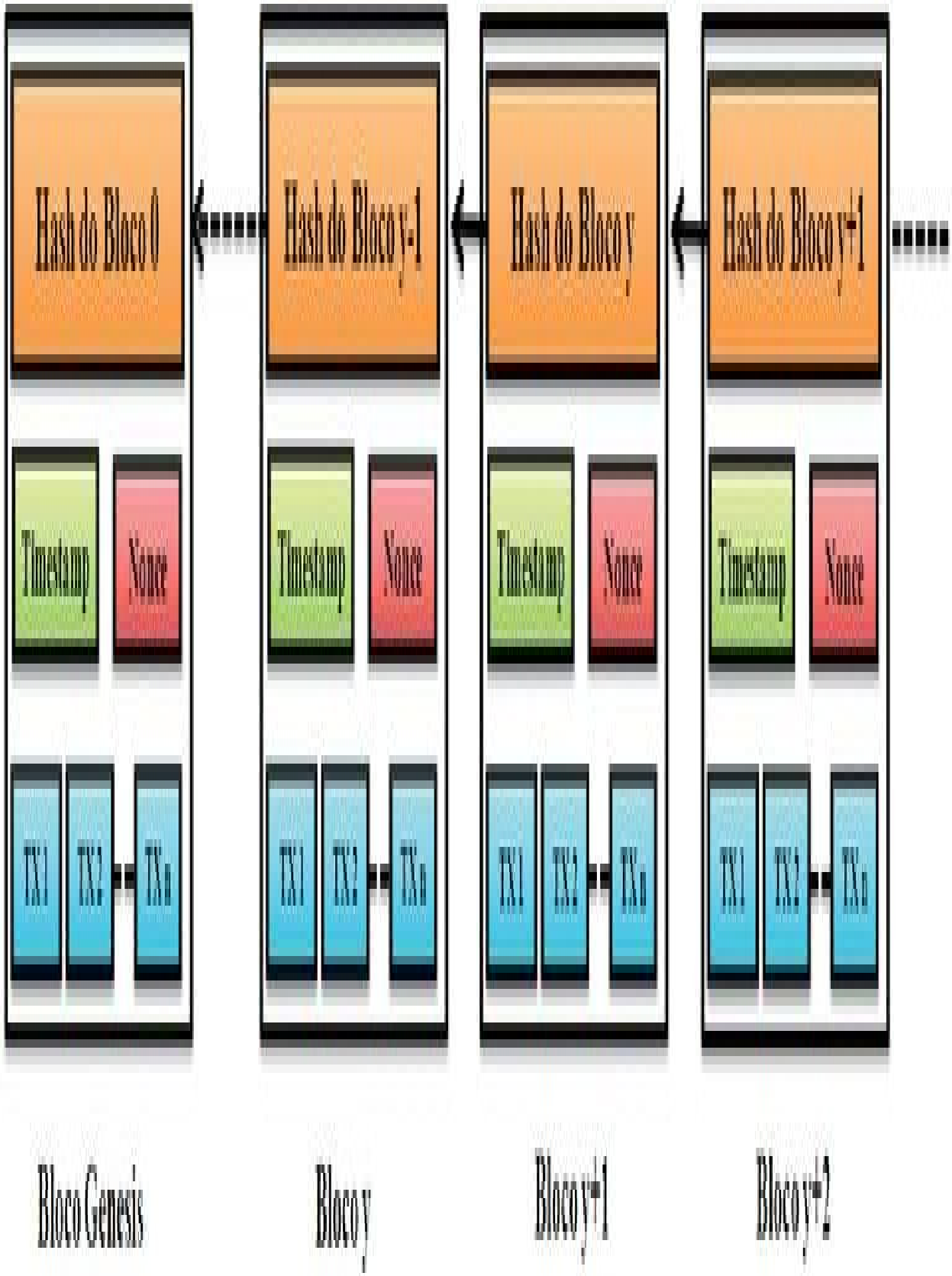

Hash do Bloco 0
Hash do Bloco y-1
Hash do Bloco y
Hash do Bloco y+1
Timestamp
Nonce
Timestamp
Nonce
Timestamp
Nonce
Timestamp
Nonce
TX1
TX2
TXn
TX1
TX2
TXn
TX1
TX2
TXn
TX1
TX2
TXn
Bloco Genesis
Bloco y
Bloco y+1
Bloco y+2

Figura 6. Exemplo da sequência de blocos do blockchain. Fonte: adaptado de Satoshi Nakamoto, 2008.

Essas cadeias crescentes de blocos que não retroagem, de registros imutáveis e distribuídos, são o blockchain. Não importam a confiabilidade do usuário e as redes que recebem as informações de uma transação de token. O fato mais importante é que as transações sejam propagadas, validadas e reconhecidas entres os nodos do sistema (ANTONOPOULOS, 2014).

As organizações descentralizadas usam, prioritariamente, blockchains públicos, e todo o conteúdo deste livro é guiado para essa concepção aberta, mas há mais dois tipos de blockchains. Vitalik (2015) explica:

• Blockchain privado: é um blockchain no qual as permissões de participação são mantidas centralizadas em uma organização. As permissões de leitura podem ser públicas ou restritas a um nível arbitrário. As aplicações prováveis incluem gerenciamento de banco de dados e auditoria interna a uma única empresa; portanto, a legibilidade pública pode não ser necessária, embora em outros casos a auditoria pública seja desejada.

• Blockchain consórcio ou híbrido: o processo de consenso é controlado por um conjunto pré-selecionado de nodos; como exemplo, Vitalik (2015) imagina um consórcio de 15 instituições financeiras, cada uma operando um nodo e das quais 10 devem assinar cada bloco para que o bloco seja válido. O direito de acesso às transações do blockchain pode ser público ou restrito aos participantes. Esses blockchains seriam considerados parcialmente descentralizados.

Fluxo do blockchain

O blockchain é um histórico de registro de transações públicas compartilhadas a todos os usuários (nodos) do sistema. No blockchain são armazenadas e compartilhadas todas as transações, desde a primeira transação até todas as futuras. Esses nodos têm acesso às atualizações do blockchain e mantêm seus registros próprios atualizados. Como dito anteriormente, esses registros próprios são conhecidos como legder, palavra que deriva do termo contábil “livro-razão”. Quando é realizada uma transação entre os nodos é criado um registro criptografado da transação, chamado de hash, que é distribuído a todos os usuários. Os nodos verificam se há alguma transação anterior que valide a real propriedade do criptoativo pelo emissor. Os nodos que reconhecem a operação a distribuem pela rede aos outros nodos, até que ela seja incorporada a um bloco em criação.

Assim podemos ilustrar o fluxo de transações em um blockchain:

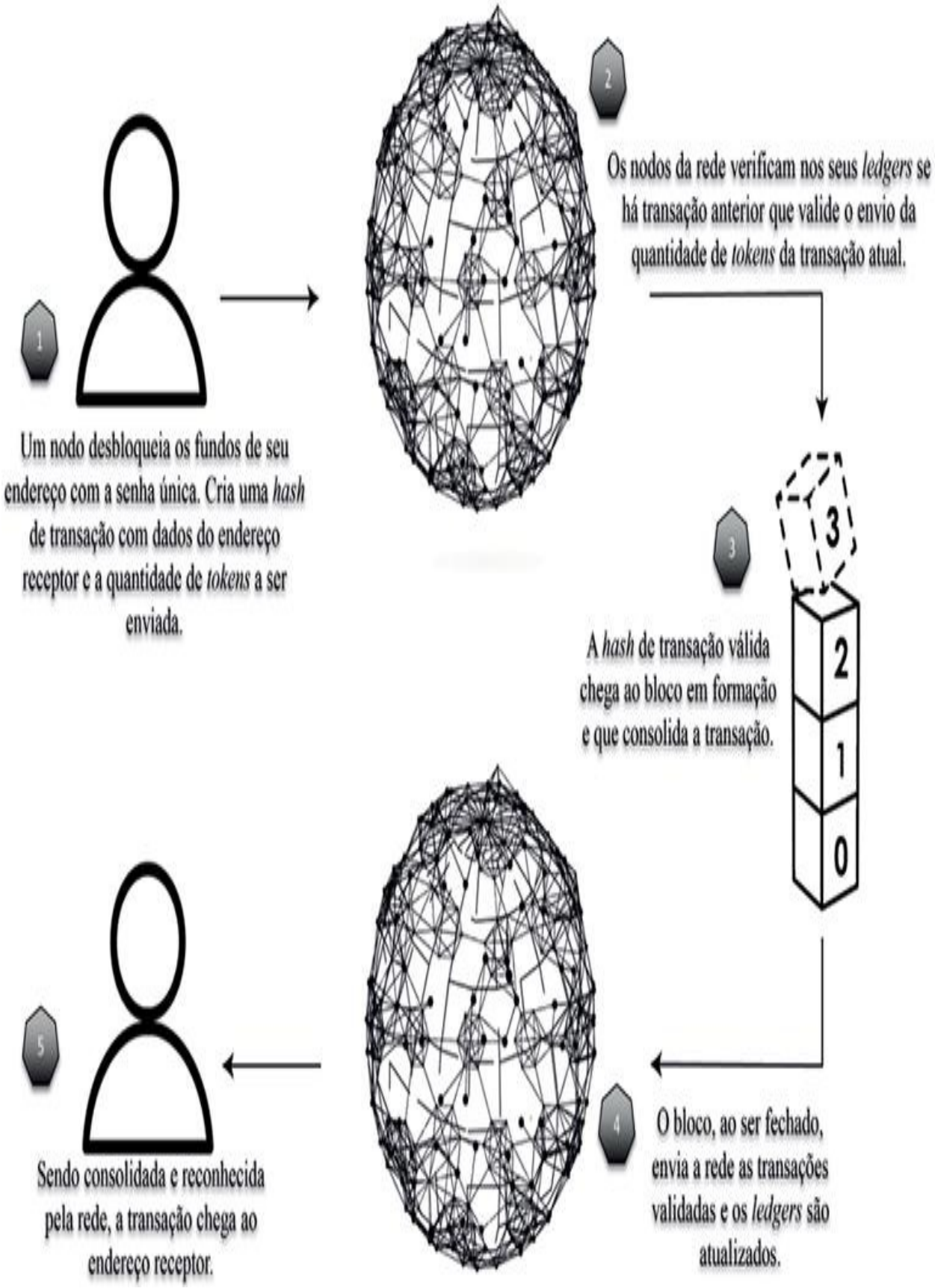

1
Um nodo desbloqueia os fundos de seu endereço com a senha única. Cria uma *hash* de transação com dados do endereço receptor e a quantidade de *tokens* a ser enviada.
2
Os nodos da rede verificam nos seus *ledgers* se há transação anterior que valide o envio da quantidade de *tokens* da transação atual.
3
A *hash* de transação válida chega ao bloco em formação e que consolida a transação.
3
2
1
0
4
O bloco, ao ser fechado, envia a rede as transações validadas e os *ledgers* são atualizados.
5
Sendo consolidada e reconhecida pela rede, a transação chega ao endereço receptor.

Figura 7. Fluxo de transações do blockchain. Fonte: o autor.

Capítulo 2. Blockchain 2.0

“São só dois lados da mesma viagem,

o trem que chega é o mesmo trem da partida”

(Milton Nascimento, “Encontros e Despedidas”)

O conceito de blockchain 2.0 se baseia na incorporação de novos recursos, como os sidechains e contratos inteligentes, que possibilitam o desenvolvimento de diversas outras aplicações que vão mais além que as criptomoedas.

O projeto Namecoin, de 2010, ampliou a possibilidade de uso do protocolo do bitcoin oferecendo registros de domínios em sua cadeia de blocos, sendo pioneiros do “bitcoin 2.0” (BUTERIN, 2014a). JR Willet escreveu, em janeiro de 2012, o artigo “The Second Bitcoin Whitepaper” e propôs uma segunda camada de protocolo e novos tokens acima do blockchain. Blockchain 2.0 é um termo introduzido por Austin Hill e Adam Back no início de 2014. Eles focaram seus estudos na incorporação de sidechains e smart contracts (contratos inteligentes) aos blockchains (SWANSON, 2014). A plataforma Ethereum focou nas aplicações dos contratos inteligentes, que ampliam consideravelmente as aplicações de caso de uso da tecnologia de contabilidade distribuída (BUTERIN, 2014a). Com os contratos inteligentes, Vitalik buscou também fortalecer e aprimorar a governança das organizações descentralizadas.

Então vamos explanar mais sobre sidechains e contratos inteligentes.

Sidechain

O artigo “The Second Bitcoin Whitepaper” argumenta que o protocolo bitcoin “pode ser usado como uma camada de protocolo, sobre a qual novas camadas de moeda com novas regras podem ser construídas sem mudar a base”. (WILLET, 2012). Tal artigo daria origem à Mastercoin, plataforma de camada 2 que atualmente se chama Omni. Todd (2014) propusera o termo treechain (cadeias de árvores). Back (2014) e Corallo (2014), o termo sidechain. Corallo (2014) afirma que, para os treechains se tornarem acessíveis aos usuários do bitcoin, eles provavelmente precisariam ser implementados em uma sidechain bidirecional. Portanto, mesmo usando nomenclaturas diferentes, as propostas possuem mais semelhanças que diferenças.

Uma filosofia de design comum entre muitos protocolos cryptocurrency 2.0 é a ideia de que, assim como na internet, o design de criptomoeda funcionaria melhor se os protocolos fossem divididos em camadas diferentes (BUTERIN, 2014a). As camadas de aplicações de um blockchain são como o modelo da internet: a camada subjacente é muito limitada e faz muito pouco, exigindo softwares razoavelmente inteligentes; no entanto, isso significa que fazer novos aplicativos sobre essa camada subjacente não requer permissão de ninguém (TODD, 2014). As cadeias laterais podem usar os recursos da camada subjacente para sua mineração ou mesmo criar novas propostas de mineração e consenso nas camadas superiores (WILLET, 2012; BACK et al., 2014). Assim, os próprios sidechains aumentariam a importância e a funcionalidade do ecossistema do bitcoin (WILLET, 2012).

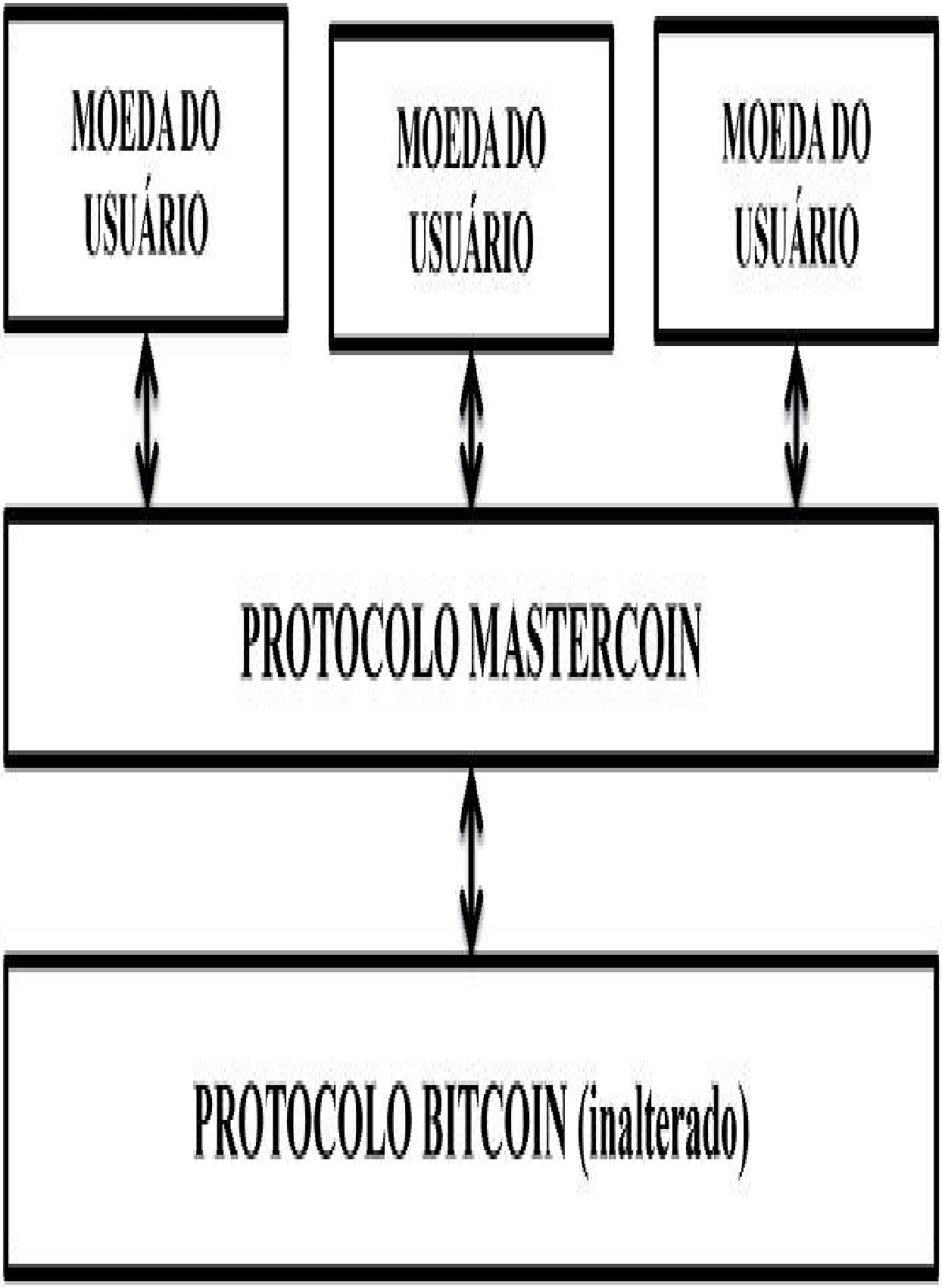

MOEDA DO USUÁRIO
MOEDA DO USUÁRIO
MOEDA DO USUÁRIO
PROTOCOLO MASTERCOIN
PROTOCOLO BITCOIN (inalterado)

Figura 8. Sidechain – Protocolos de camadas Mastercoin. Fonte: adaptada de WILLETT, J. R.,

“The Second Bitcoin Whitepaper”, 2012.

As camadas de protocolo propostas pela Mastercoin podem ser visualizadas da seguinte forma: as setas representam usuários trocando criptomoedas. Note que todas as transferências de valor ainda são armazenadas na cadeia de blocos de bitcoins normal, mas nas camadas mais altas os protocolos atribuem significado adicional às transações (WILLET, 2012).

Em uma época mais maximalista, a lógica por trás da proposta de J. R. Willett abordou várias questões: melhorar a estabilidade do bitcoin através da emissão de novas moedas que evoluíram para contratos por diferença; beneficiar os detentores de bitcoin adicionando novo valor à rede bitcoin; fornecer um mecanismo pelo qual financiar o desenvolvimento de software, marketing e manutenção das novas camadas de protocolo (ZYNIS, 2013). Os primeiros sidechains surgiram no bitcoin. O Coloredcoin permitiu que os usuários criassem suas próprias moedas na rede bitcoin e protocolos mais avançados, como Mastercoin, Bitshares e Conterparty, forneceram recursos adicionais da rede como derivativos financeiros, carteiras de poupança e trocas descentralizadas. No entanto, até esse ponto, todos os protocolos que foram inventados foram especializados, tentando oferecer conjuntos de recursos detalhados direcionados a setores específicos ou aplicações geralmente de natureza financeira (BUTERIN, 2014a).

Mesmo com a adoção de novas camadas, a escalabilidade de transações no protocolo seria uma falha específica do bitcoin. O Ethereum nasceu, em 2014, sem a pretensão de ser um protocolo de canivete suíço com centenas de recursos para atender a todas as necessidades. Em vez disso, a Ethereum pretendeu ser um protocolo de base que permitisse que outras aplicações descentralizadas fossem construídas em cima dela em vez de bitcoin, dando-lhes mais

ferramentas para trabalhar e permitindo-lhes obter todos os benefícios da escalabilidade e eficiência da Ethereum (BUTERIN, 2014). Ao separar a camada de contrato inteligente da camada blockchain da base, as cadeias de blocos como Ethereum visam fornecer um ambiente de desenvolvimento mais flexível do que o blockchain bitcoin. Em tal configuração, as regras de governança das transações podem agora ser definidas de forma flexível pelas partes de um contrato inteligente, em vez de definir todas as regras de governança diretamente na camada de consenso do blockchain (SHERMIN, 2017).

Open reSource

A possibilidade de criar camadas sem a necessidade de autorização de nada e ninguém em cima de protocolos blockchain amplia o consenso de código aberto. Os sidechains podem usufruir da participação e de recursos energéticos usados nos consensos das camadas inferiores para criar novas aplicações.

Além disso, a possibilidade de forks (que serão vistos mais adiante) e a criação de novos criptoativos dentro dos códigos do bitcoin e de outros DLTs apresentam um novo conceito que difere do open-source, pois se trata de um recurso monetário, e até mesmo energético, se pensarmos na energia dispendida para a mineração desses criptoativos, até a divisão da cadeia de blocos, e por esse motivo aqui vemos o nascimento do conceito open-reSource, que é mais adequado para as mudanças trazidas pela tecnologia blockchain.

Contratos inteligentes

Pensado em 1997 pelo cientista da computação Nick Szabo, a aplicação dos contratos inteligentes (CI) ficou durante mais de uma década sem muito uso concreto. Os principais motivos seriam a falta de uma fonte de tempo confiável para sua aplicação, além de uma auditabilidade concreta, fatores que a tecnologia blockchain suprem com a adoção do timestamp e sua contabilidade distribuída para as propostas de execução de contratos inteligentes.

Em 2002, Szabo avança seus estudos sobre contratos inteligentes e propõe a linguagem “E”, para a autoexecução das negociações por meio dessa linguagem, tendo como condicionante a performance acordada. O fluxo simplista de Szabo seria:

Negociação Contrato Desempenho

O artigo de Szabo (2002) ressalta sua preocupação com a semântica e com o desafio de transformar acordos em códigos de programação e não fornece interação com recursos externos (oráculos inteligentes) além da linguagem “E” apresentada. Com o advento do blockchain e o aumento de sua aplicabilidade, novos pesquisadores se debruçam sobre o assunto. Sillaber e Waltl (2017) criaram um modelo de ciclo de vida dos contratos inteligentes, que é bem próximo ao proposto por Szabo, mas incorporando a tecnologia blockchain no fluxo de um contrato inteligente.

Componentes do contrato inteligente

Os componentes de um CI na cadeia de blocos, para Sillaber e Waltl (2017), são:

Arranjos contratuais entre as partes (negociação e contrato)

As partes negociam suas obrigações e as transformam em códigos autoexecutáveis. As partes são identificadas através de seus endereços de cadeias de blocos (carteiras) e as transações indicam as obrigações que devem ser cumpridas entre elas. O código autoexecutável é então implementado e armazenado na cadeia de blocos distribuídos (ibid.).

Governança de pré-condições

A governança dos contratos inteligentes é realizada pelo blockchain onde ele foi criado. Os nodos e os mineradores assumem papéis de auditores das condições previamente acordadas para a execução do contrato (SILLABER; WALTL, 2017). Essa governança é facilitada com uma fonte de tempo confiável dos blockchains que não havia sido solucionada por Szabo.

Execução do contrato

Com as condições prévias sendo cumpridas e validadas pelos nodos por meio do seu consenso distribuído, o contrato é executado. Portanto, contratos inteligentes

são de autoexecução, o que significa que os ativos digitais são alocados de forma autônoma de acordo com os termos contratuais predefinidos (SILLABER; WALTL, 2017).

Os exemplos iniciais de Szabo (1997a) para a utilização de contratos inteligentes eram simples como a promessa de contratos futuros de commodities. Com o surgimento de novas tecnologias, as condições pré-acordadas em um CI aumentam de amplitude.

Com todas as tecnologias disponíveis atualmente, um exemplo de contrato inteligente poderia ser a execução de alguma transação que depende de alguma condição. Por exemplo: “transferir x quantia de moeda de Alice para Bob se a temperatura em Bariloche estiver abaixo de zero grau em pelo menos vinte dos próximos trinta dias” (PETERS; PANAYI, 2015). Os dados externos ao blockchain, como a medição da temperatura e as mudanças de preços, são conhecidos como oráculos inteligentes do blockchain. Um oráculo é um tradutor para informações fornecidas por uma plataforma externa ao blockchain (BUCK, 2017).

A vantagem de registrar esses eventos e os programas de controle em um ledger distribuído é que as várias partes podem ver todos esses programas e monitorar o progresso do fluxo de comércio conforme ele acontece. Além disso, o ledger registra sua proveniência na cadeia de custódia dos ativos envolvidos (MAGAZZENI et al, 2017).

Ciclo de vida do contrato inteligente

O ciclo de vida de um contrato inteligente geralmente consiste em quatro fases: criação do contrato inteligente, congelamento do contrato inteligente, execução do contrato inteligente e finalização do processo inteligente do contrato (SILLABER; WALTL, 2017).

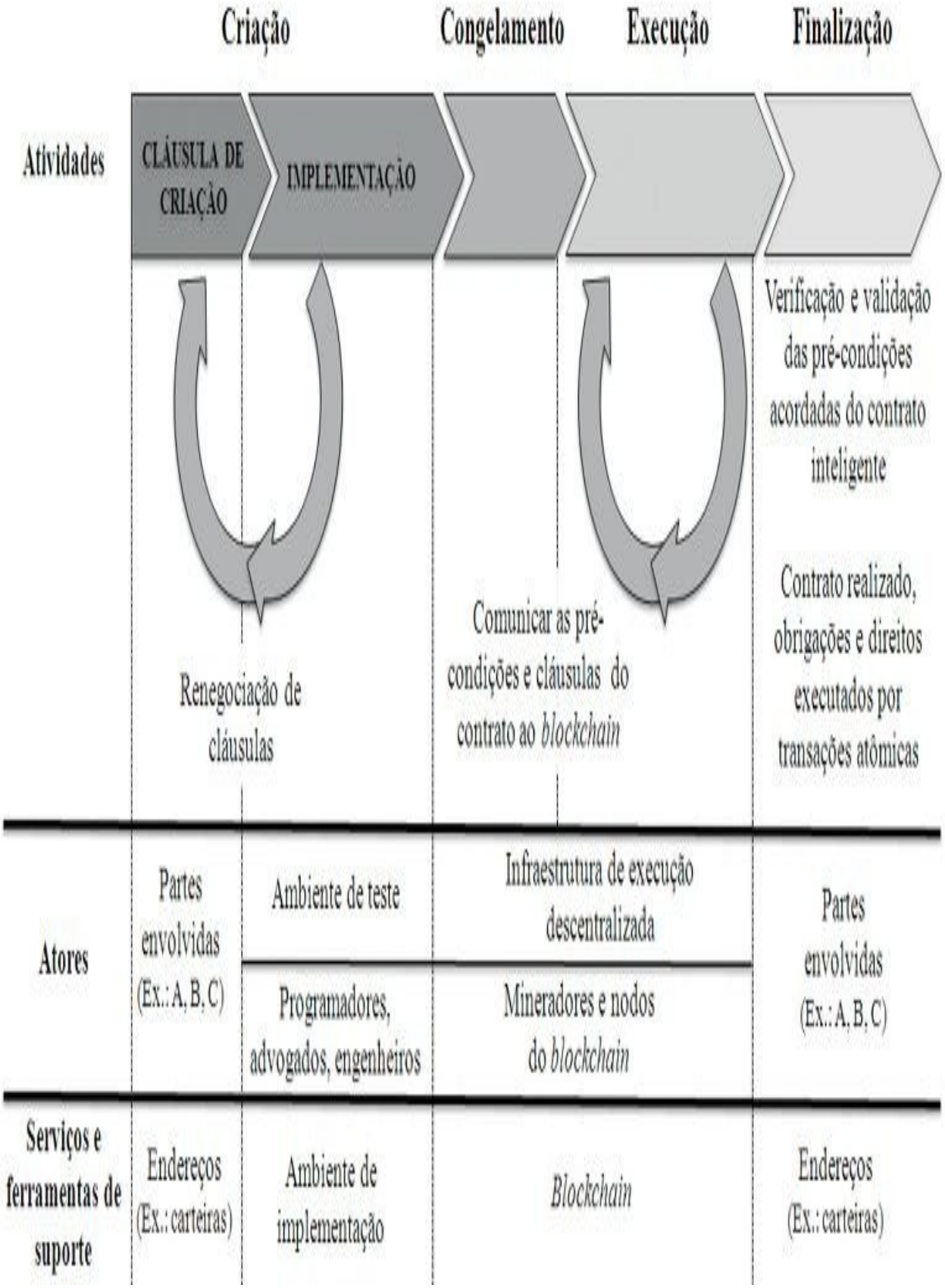

Criação
Congelamento
Execução
Finalização
Atividades
CLÁUSULA DE CRIAÇÃO
IMPLEMENTAÇÃO
Verificação e validação das pré-condições acordadas do contrato inteligente
Contrato realizado, obrigações e direitos executados por transações atômicas
Renegociação de cláusulas
Comunicar as pré-condições e cláusulas do contrato ao blockchain
Atores
Partes envolvidas (Ex.: A, B, C)
Ambiente de teste
Infraestrutura de execução descentralizada
Partes envolvidas (Ex.: A, B, C)
Programadores, advogados, engenheiros
Mineradores e nodos do blockchain
Serviços e ferramentas de suporte
Endereços (Ex.: carteiras)
Ambiente de implementação
Blockchain
Endereços (Ex.: carteiras)

Figura 9. Ciclo de vida do contrato inteligente. Fonte: adaptado de SILLABER e WALTL, 2017.

Os contratos inteligentes são roteiros de eventos futuros, e Sillaber e Walt (2017) nos orientam nas fases para construção desse roteiro:

Criar

A fase de criação se divide na parte de negociação do contrato e na parte de implementação. Primeiro, as partes têm que concordar com os amplos conteúdos objetivos e obrigações no contrato, sendo on-line ou offline, semelhante a negociações clássicas de contratos. O recurso necessário é que todas as partes devem possuir uma carteira na plataforma onde o contrato será hospedado. A identificação das partes na maioria dos casos é por endereços criptografados. Esses endereços serão usados para o reconhecimento das partes e para transferência dos fundos (ibid.).

Após ter concordado com os objetivos e o conteúdo do contrato, o acordo é transformado em código. Há que se admitir a limitação semântica entre as linguagens. A codificação do contrato é limitada à codificação da linguagem da programação usada. Boa parte das plataformas de contratos inteligentes possui ambientes de teste para a verificação do comportamento e da execução do contrato codificado. Como qualquer programação orientada por objetos, necessitam de uma interação entre programadores desde a parte de negociação até a fase de implementação.

Depois que as partes concordarem com a versão codificada do contrato, ele é enviado ao blockchain e os nodos participantes distribuem o contrato inteligente.

O bloco hospedeiro do contrato, após confirmado pela maioria dos nós, tornaria o contrato imutável, e qualquer mudança necessitaria da construção de um novo contrato, já que seria inviável alterar as condições gravadas nos ledgers de todos os nodos.

Embora um contrato inteligente tenha sido armazenado na cadeia de blocos, esse fato não deve ser considerado um acordo da parte. Como qualquer um pode criar contratos inteligentes nas cadeias de blocos, estes podem indicar obrigações para qualquer carteira aleatória, da mesma forma que os contratos inteligentes podem beneficiar qualquer participante da rede, mesmo concordando ou não.

Congelar

Após a incorporação do contrato inteligente na cadeia de bloco e para evitar uma inundação de contratos inteligentes no ecossistema, deve ser paga uma taxa (gás) aos mineiros (WOOD, 2014; SILLABER; WALTL, 2017). A partir desse momento, o contrato e as partes do acordo são públicas e acessíveis através do blockchain. Durante a fase de congelamento, todas as transferências feitas para os montantes da carteira do contrato inteligente estão sendo congeladas e os nodos assumem o papel de governança, garantindo que as condições prévias sejam honradas para a execução do contrato e a liberação dos fundos recebidos, quando se tratar de contrato monetário (SILLABER; WALTL, 2017).

Executar

Os contratos que estão armazenados no bloco são reconhecidos pelos nodos participantes. A integridade do contrato é validada e o mecanismo de inferência do ambiente do contrato inteligente interpreta e executa o código. Os insumos para a execução são coletados dos oráculos inteligentes e/ou partes envolvidas. A execução do contrato inteligente resulta em um conjunto de novas transações. O

resultado do conjunto dessas transações altera o estado do contrato inteligente e as alterações são enviadas ao blockchain e validadas pelos nodos, através do protocolo de consenso (ibid.).

Finalizar

Após o contrato inteligente ter sido executado, o resultado das novas transações, aquelas assumidas no acordo inicial, são armazenadas no blockchain e confirmadas com o consenso protocolar. Os ativos digitais previamente comprometidos são transferidos (descongelamento de ativos) e com a confirmação de todos transações o contrato foi cumprido (SILLABER; WALTL, 2017).

A formalização de relacionamentos virtuais em livros distribuídos reduziria o risco de não conformidade que qualquer um teria de suportar ao entrar em um acordo, pois, se uma rede de computadores for capacitada a cumprir os termos dos relacionamentos do protocolo, ou seja, o contrato inteligente é lançado na blockchain, ele se torna ‘independente’ da vontade das partes, não seguindo nada além de suas instruções e autoaplicando as condições nele codificadas (CUCCURU, 2017; SILLABER; WALTL, 2017).

A forma mais complexa de um contrato inteligente é uma organização autônoma descentralizada (DAO), que governa um grupo de pessoas que compartilham os mesmos interesses e metas. As DAOs são governadas de acordo com um conjunto de regras de controle de token escritas no código da camada de aplicativos, evitando a necessidade de envolvimento da gerência humana. Essas regras de governança de token, da camada de blockchain e da camada de aplicativo, têm o potencial de interromper a governança como a conhecemos (SHERMIN, 2017).

Capítulo 3. Organizações Descentralizadas

"Que eu me organizando posso desorganizar"

(Chico Science e Nação Zumbi, "Da Lama ao Caos")

A tecnologia blockchain permite a criação de sistemas descentralizados, moedas, contratos digitais autoexecutáveis e ativos que podem ser controlados pela internet (smart asset). O blockchain também permite o desenvolvimento de novos sistemas de governança com a tomada de decisão participativa e organizações descentralizadas e/ou autônomas, que podem operar através de uma rede de computadores sem qualquer intervenção humana. Essas aplicações levaram muitos a comparar o blockchain a uma evolução da internet, possibilitando o surgimento de novas interações entre as redes e desafiando o equilíbrio de poder de autoridades centralizadas nos campos de comunicações, negócios e até políticas e leis (WRIGHT; DE FILIPPI, 2015).

Blockchain e contratos inteligentes podem introduzir novas maneiras de coordenar atividades como alocação de tarefas, coordenação e supervisão de um grupo de pessoas que compartilham interesses econômicos comuns, mas são geograficamente distribuídas, sem a necessidade de uma organização gerenciada centralmente. Isso poderia ser possível com DAOs ou através de autoalinhamento automático em torno de pontos focais de Schelling (SHERMIN, 2017). As organizações descentralizadas podem reimplementar aspectos da governança corporativa tradicional usando software, possibilitando os benefícios das estruturas corporativas formais e ao mesmo tempo mantendo a flexibilidade e a escala dos grupos informais on-line. Essas organizações também podem ser operadas de forma autônoma sem envolvimento de qualquer humano. Elas podem concordar, trocar ou negociar recursos e interagir com outros seres humanos ou máquinas, levantando novas questões em torno da

tradicional noção de personalidade jurídica (WRIGHT; DE FILIPPI, 2015).

As organizações descentralizadas (DOs), em vez de uma estrutura hierárquica gerenciada por um conjunto de seres humanos interagindo pessoalmente e controlando a propriedade através do sistema legal, envolvem um conjunto de seres humanos interagindo entre si de acordo com um protocolo especificado em código imposto a todos por um blockchain. A DO pode ou não fazer uso do sistema legal para alguma proteção de sua propriedade física, mas mesmo assim tal uso é secundário (BUTERIN, 2014b).

As organizações descentralizadas podem ser divididas em duas: as organizações descentralizadas e autônomas (DAO) e as aplicações descentralizadas (DApp).

Organizações descentralizadas e autônomas (DAOs)

A ideia de organização descentralizada e autônoma (DAO) se fortalece entre os debates com Vitalik em 2014, mas o conceito DAC (Descentralizated Autonomous Corporation) usado por Daniel Larimer em 2013 já descrevia uma estrutura praticamente idêntica, exposta no projeto Bitshare. Historicamente, a rede bitcoin é considerada a primeira organização verdadeiramente autônoma governada unicamente através de um protocolo de consenso distribuído, que qualquer um é livre para participar (SHERMIN, 2017). Embora não tenha um token de propriedade (equity) que proporcione o voto junto à administração, poderíamos entender que o bitcoin possui um processo de votação indireta, que é gerido pelo poder computacional dos mineradores que implementam ou não as mudanças propostas de alteração de seus códigos e novas aplicações. Buterin (2014) chama o bitcoin de uma DAO com imperfeições de autonomia.

Retirando-se das polêmicas, Daniel Larimer (2013) afirma que uma DAO possui quatro características essenciais:

1. Não deve depender de qualquer indivíduo, empresa, organização ou governo para seu funcionamento. Ela deve possuir uma estrutura horizontalizada.

2. Deve ter seu próprio token, que permita poder de votos na gestão da empresa aos seus possuidores.

3. Não deve depender de contratos ou leis juridicamente vinculativas, como direito de propriedades ou patentes e relações trabalhistas com seus participantes.

4. Deve possuir códigos abertos de domínio público, para não se submeter a nenhuma jurisdição.

É uma estrutura extremamente nova e que até o momento não há respaldo jurídico para existir, trata-se de uma jurisdição conhecida como criptoespaço. O único amparo para sua existência é social e que a sua finalidade faça sentido para algum grupo ou comunidade em rede do mundo.

E exatamente por ser uma nova estrutura organizacional que a ausência de respaldo legal é uma fraqueza para as DAOs, pois não as permite comercializar suas aplicações com as empresas convencionais, já que estas necessitam ter registros contábeis de origens e destino dos fluxos financeiros claros por questões de auditorias fiscais e imposições legais.

Aplicações descentralizadas (DApps)

A popularização das aplicações descentralizadas começa ao final do último milênio, com o MojoNation, BitTorrent, Gnutella, eDonkey, Freenet, Napster, etc. O Napster nasceu em 1999 e oferecia trocas de arquivos musicais P2P. Embora o Napster não centralizasse o serviço de compartilhamento, havia uma empresa responsável pela gestão do software de troca de músicas de seus usuários (ANTONOPOULOS; WOOD, 2018). Em 2003 a banda Metallica entrou com uma ação judicial buscando ressarcimento de direitos autorais de suas músicas que transitavam no Napster. Resultado? Falência da empresa, embora a marca tenha sido vendida posteriormente como bem intangível, o que ajudou seus criadores no pagamento das ações judiciais[1].

E o que difere a comunicação descentralizada, P2P, da Napster das atuais organizações descentralizadas? Principalmente o capital interno distribuído a todos por forma de tokens. A possibilidade de uma contabilidade pública, transparente e consensual entre os participantes cria um ecossistema de interesse comum muito mais forte que somente aplicações descentralizadas. E esse é o grande desafio de gestão de DApps e DAOs.

Construir uma nova empresa já é difícil. Construir um ecossistema e uma comunidade de usuários ao mesmo tempo em que se constrói um produto é ainda mais difícil (MOUGAYAR, 2016).

Ao contrário de um aplicativo tradicional, um DApp (aplicação descentralizada) não pertence apenas a um único provedor ou servidor, mas a arquitetura inteira seria implantada e operada de maneira distribuída em uma rede ponto a ponto - (ANTONOPOULOS; WOOD, 2018; TAPSCOTT; TAPSCOTT, 2016). Uma DAO necessita exclusivamente de uma DApp, mas uma DApp não

necessariamente será uma DAO. Uma diferença visível entre as DApps é a aplicação descentralizada, mas o desenvolvimento e a governança da aplicação podem ser geridos por empresa, grupo conhecido, selecionado e reduzido de participantes em comparação a uma DAO, que em sua essência é aberta. Mougayar (2018) vê como principais características das DApps:

1. Dependência de uma infraestrutura de rede descentralizada, rede P2P.

2. Protocolo descentralizado subjacente, técnico ou operacional.

3. Operações descentralizadas para tomada de decisão.

4. Transações baseadas em blockchain para imutabilidade e transferência de valores P2P.

5. Armazenamento de conteúdo distribuído incluindo identidade.

6. Capacitação do usuário final sobre a propriedade do conteúdo.

7. Algum nível de autonomia descentralizada que é livre da autoridade central.

8. Distribuição equitativa de recompensas, benefícios e apostas para os usuários finais.

Atualmente a maioria das DApps que nascem no ecossistema blockchain possui responsáveis explícitos pelo projeto, com uma estrutura similar às startups do Vale do Silício, com grupos de programadores, equipe de marketing, estrutura de recursos humanos, etc. A maioria esses projetos tem fundadores ou fundações com grandes quantidades de tokens e que atuam como grandes atores centralizados que estão interessados no sucesso de suas plataformas. Dessa forma, em todo o material, quando houver referências a organizações descentralizadas (DOs), incluem-se DAOs e DApps com sua equipe gestora.

Agentes autônomos

As organizações descentralizadas possuem como características principais agentes autônomos. Maes (1990, apud FRANKLIN; GRAESSER, 1996) classifica: “agentes autônomos são sistemas computacionais que habitam algum ambiente dinâmico complexo, sentem e agem autonomamente nesse ambiente e, ao fazê-lo, realizam um conjunto de objetivos ou tarefas para os quais foram projetados”. Agentes autônomos possuem um propósito específico e são persistentes no cumprimento de suas próprias ideias sobre como realizar tarefas e suas próprias agendas.

Um exemplo de agentes autônomos são os vírus computacionais (TAPPSCOTT; TAPSCOTT, 2016; BUTERIN, 2014b). Em um agente autônomo não há nenhum envolvimento humano necessário, isto é, mesmo que haja algum esforço humano para construir o hardware em que o agente é executado, não há necessidade de existir nenhum humano que esteja ciente da existência do agente.

Os contratos inteligentes podem se tornar agentes autônomos (BUTERIN, 2014b). Quando codificados, eles poderão atuar na governança das organizações descentralizadas e na própria execução das tarefas organizacionais. Antonopoulos e Wood (2018) apontam benefícios dos contratos inteligentes, que são usados para armazenar a lógica de negócios, o estado e o cálculo das aplicações descentralizadas. Pense em um contrato inteligente como um componente do lado do servidor em um aplicativo regular. E Tapscott e Tapscott (2016) ressaltam que há uma evolução nos agentes autônomos e na sua interação com outras tecnologias.

Para Mougayar (2015), o DAO é o nirvana real em termos de agentes autônomos. Já podemos imaginar os agentes autônomos dos blockchains

realizando seu trabalho através de outras tecnologias, como inteligência artificial, internet das coisas, comunicação M2M (Machine-to-Machine), etc., o que amplia exponencialmente as possibilidades de sua utilização.

Outras considerações

É comum encontrarmos desenhos das camadas do blockchain como este a seguir. Os aspectos gráficos das camadas se diferem, mas em sua maioria essas imagens apresentam as DAOs e DApps localizadas nas partes superiores de terceira, quarta ou até mesmo quinta camada.

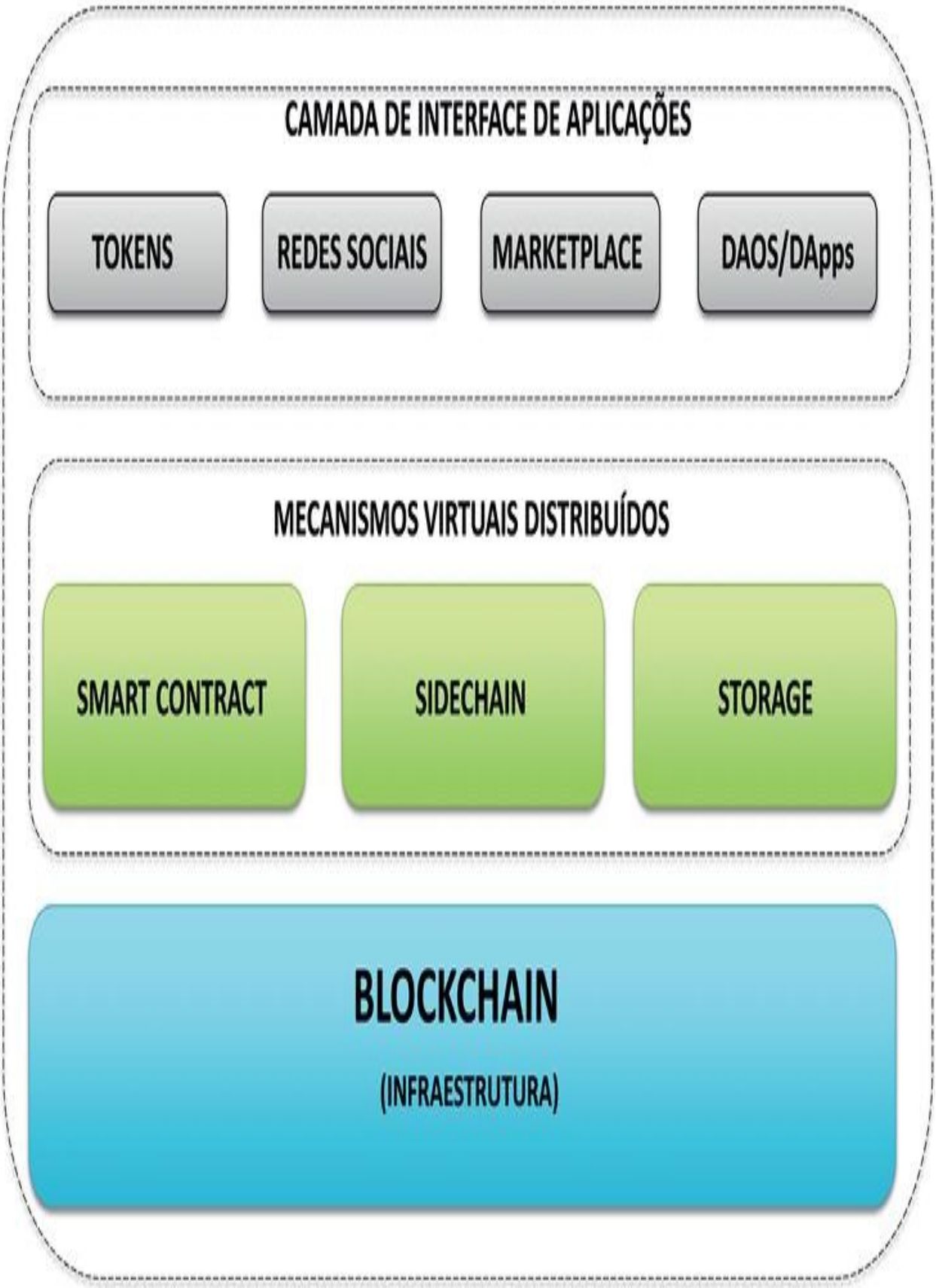

CAMADA DE INTERFACE DE APLICAÇÕES
TOKENS
REDES SOCIAIS
MARKETPLACE
DAOS/DApps
MECANISMOS VIRTUAIS DISTRIBUÍDOS
SMART CONTRACT
SIDECHAIN
STORAGE
BLOCKCHAIN
(INFRAESTRUTURA)

Figura 10. Ecossistemas distribuídos. Fonte: o autor.

Essa imagem seguramente oferece um recurso visual didático, mas é importante ressaltar que, no ecossistema dos blockchains abertos, todas as camadas anteriores podem ser consideradas DApps ou DAOs. Aqui em nosso livro, usamos DO (organizações descentralizadas) para designar as estruturas organizacionais, sejam elas DApps ou DAOs.

Apresentados os aspectos básicos de um blockchain, seu funcionamento e os principais recursos para criação de organizações descentralizadas, o livro discorrerá sobre sua forma de arrecadação, as famosas ICOs.

Capítulo 4. ICOs – Ofertas Iniciais de Moedas

“Criar meu web site, fazer minha home page

Com quantos gigabytes se faz uma jangada, um barco que veleje?

Que veleje nesse informar, que aproveite a vazante da infomaré

Que leve um oriki do meu velho orixá”

(Gilberto Gil, “Pela Internet”)

Por ser uma das principais formas de financiamentos, que cada vez se torna mais popular, as ofertas iniciais de moedas (Initial Coin Offering – ICO) merecem um capítulo neste livro.

A ICO pode ser a forma de captação financeira de organizações distribuídas. É um paralelo ao modelo tradicional das empresas que abrem seu capital em bolsas de valores, conhecidos como IPO (Initial Public Offering) (CONLEY, 2017).

Para a Comissão de Serviços Financeiros de Gilbratar (2017), as ICOs são formas não regulamentadas de obtenção de financiamento em um empreendimento ou projeto geralmente em estágio inicial e cujos produtos e serviços ainda não foram significativamente projetados, construídos ou testados, e muito menos se tornaram operacionais ou geradores de receita. São formas de crowdfunding usadas para ignorar o rigoroso e regulamentado processo de captação exigido para levantamento de capital de startups. Em uma ICO, os tokens são vendidos aos primeiros apoiadores de um projeto, que os compram com dinheiro ou criptomoedas, como bitcoin ou ether. Vale ressaltar que é

bastante comum o uso do termo crowdsales para o processo de levantamento de capital inicial de projetos em blockchain.

Mas o que motivaria as pessoas a comprar os tokens de algum projeto que nem existe?

As oportunidades de ganhos de capital com o crescimento do projeto são na maioria das vezes a prioridade de um comprador. Um projeto de ICO que foca somente nos aspectos tecnológicos e ignora os aspectos econômicos do ecossistema que se quer criar sempre é arriscado (CONLEY, 2017). Mesmo sendo um modelo crowdfunding, na grande maioria das vezes os capitalistas de ICOs não estão focados em pequenos retornos e filantropia. E a verdade é que há muita oportunidade de ganhos! Vejamos os 10 maiores retornos de investimento em ICO, até meados de 2018.

Tabela 1. Histórico dos maiores retornos de ICO. Fonte: ICO Market Data, jun. de 2018.

ICO	Arrecadado USD	Mês	Preço ICO	Preço atual US$	ROI USD	RO
Nxt	US$ 16.800,00	set-13	> 0,00	US$ 0,14	8575,56 x	184
Ethereum	US$ 15.571.000,00	jul-14	0,31	US$ 565,21	1817,40 x	152
NEO	US$ 3.800.000,00	jan-15	0,03	US$ 53,06	1658,03 x	130
Stratis	US$ 600.944,55	jul-16	> 0,00	US$ 4,48	625,84 x	54,8
Spectrecoin	US$ 15.426,50	jan-17	> 0,00	US$ 0,31	381,50 x	46,7
Ark	US$ 942.593,13	dez-16	> 0,00	US$ 2,37	238,43 x	24,0
Komodo	US$ 1.983.781,00	nov-16	0,02	US$ 2,53	114,92 x	10,9
Lisk	US$ 6.500.000,00	mar-16	0,07	US$ 8,63	112,82 x	6,2
Cardano	US$ 62.993.614,00	jan-17	> 0,00	US$ 0,20	100,35 x	2,5
Storj-x	US$ 461.802,00	ago-14	> 0,00	US$ 0,80	88,55 x	5,5

Como se pode ver na tabela, em grande parte das ICOs os tokens são vendidos em sua oferta inicial a preços menores que 1 centavo de dólar, oferecendo lucros de mais de cem vezes o valor aplicado. Os tokens geralmente servem como uma unidade contábil de troca interna para o projeto de ICO (CONLEY, 2017). Os tokens são elementos vitais de troca envolvidos ao projetar um sistema apropriado de ICO. Além de conhecimento técnico, requer um entendimento de teoria dos jogos, economia, comportamento humano e sistemas de incentivo. Sem uma visão holística dos protótipos dos tokens, eles podem se tornar um bem completamente desvalorizado, comprometendo todo o futuro do projeto de ICO (BR, 2017). Os tokens ofertados em troca nas ICOs assumem múltiplos propósitos e podem ser usados como: moeda, voto, autenticidade, reputação, identificação, acesso, entre outros.

A primeira ICO realizada foi a da plataforma Mastercoin, que hoje é a Onmi. Sua oferta de moedas ocorreu em 31 de julho de 2013. A arrecadação foi de 4.740 bitcoins. Ainda foram usados tokens Mastercoins para realização de diversos concursos para melhoria de códigos, e em troca distribuía-se parte dos fundos arrecadados aos programadores vencedores, fomentando uma criação de protocolo completamente aberta (ZYNIS, 2013).

Como vimos quando falamos dos sidechains, o projeto Mastercoin arquitetou uma camada dentro do protocolo do bitcoin para criar novos ativos digitais e dessa forma aproveitar a mineração da cadeia de blocos do bitcoin para o funcionamento de sua plataforma. Voltando às ICOs, o projeto Mastercoin, em troca dos bitcoins recebidos pelos endereços bitcoins, devolvia aos endereços dos doadores os tokens MSC. Esses tokens se tornaram os criptoativos, o seu capital próprio de seu ecossistema.

Em julho de 2014 a Ethereum lança sua ICO e consegue uma arrecadação de 18 milhões de dólares em bitcoins. A Ethereum nasce com uma visão diferente: a de criar seu próprio livro contábil distribuído para que sejam desenvolvidas

aplicações descentralizadas em sua plataforma. A ideia de não aproveitar a mineração do blockchain do bitcoin tem uma influência no sucesso da plataforma, pois atrai mais participantes ao oferecer possibilidades de retornos financeiros a nodos mineradores[1].

O sucesso de arrecadação, e de retorno financeiro, tornou as primeiras ICOs extremamente atrativas e populares para a busca de financiamento de startups e projetos de aplicações descentralizadas. Mas com elas também surgiram muitos scammers, termo usado na designação de projetos fraudulentos. Por esse motivo surgem legislações restritivas a respeito das ICOs e também sites especializados que buscam qualificar os projetos de ICO e denunciar os scammers, assumindo um papel autorregulador.

Tabela 2. Portais informativos de ICO. Fonte: o autor.

Lista de portais informativos sobre ICO

ListICO	ICO Drip	ICO Street	ICOhold
BestCoins	CryptoRadar	ICODrops	LastCryp
ICObazaar	ICOcreed	TokenMarket	CoinStal
The Tokener	ICO Watchlist	Smith & Crowns	CryptoP
ICO Map	ICO Rating	CoinLauncher	CryptoT
ICO Bench	Coin Schedule	Coinhills	ICOinde
ICO Hot List	ICO Tracker	ICO Buffer	ICOCLA
ICO Champs	Top ICO List	Crypto Smile	ICO Ma
CoinMarketPlus	ICOTOP	ICO Finch	
ICO Alert	CoinGecko	Bitcoinx	

Sites como ICO Bench e ICO Rating são portais que qualificam as propostas de ICO. Os principais critérios analisados na qualificação de uma ICO são: equipes, produtos, viabilidade, divulgação e marketing.

Vamos analisar alguns desses pontos.

Critérios de análise de ICOs

Equipes

São avaliados os currículos e a experiência em desenvolvimento de aplicações em blockchain. Influência e credibilidade dos participantes no criptomercado também são consideradas.

A equipe pode contar com apoiadores externos, como conselheiros renomados capazes de suprir deficiências técnicas, mentores e embaixadores que ajudarão na divulgação dos projetos em diversos países.

Divulgação e marketing

As ICOs já contam com muitos canais virtuais de divulgação de seus projetos. Sites especializados em ICO, criptomoedas e blockchain são ferramentas para alcance do público que já entende o funcionamento das ICOs, mas, em contrapartida, esses canais estão repletos de especuladores, o que pode ser prejudicial para o futuro do projeto.

O atual desafio das ICOs é conseguir alcançar o público que utilizará realmente os tokens, pois é uma forma de conceder liquidez a eles no mercado e de oferecer um crescimento mais sustentável a longo prazo ao projeto.

Mas por que é um desafio?

Porque grande parte das pessoas não possui conhecimento do que é uma ICO e os potenciais tecnológicos das aplicações em blockchain. White (2017) realizou uma pesquisa junto a executivos e percebeu que há até curiosidade sobre a tecnologia blockchain, mas que o nível de conhecimento é baixo. Outro desafio é realizar ICO com público exclusivamente especulativo, pois há muitos flippers[2], que compram os tokens nas pré-vendas das ICOs e logo os vendem quando abre a comercialização dos tokens nas corretoras, auferindo ganhos rápidos e saindo do projeto que muitas vezes nem foi iniciado.

Assim, outros recursos considerados nas estratégias de divulgações das ICOs são a realização de eventos explicativos junto a profissionais do setor onde a ICO pretende atuar e o uso de canais de comunicação abertos que possibilitem o surgimento de uma comunidade participativa junto ao projeto. Os mais utilizados

atualmente são Slack, Telegram, Discord, Discourse e Rocket Chat. Comum também é o uso das redes sociais e fóruns como Github, Reddit, Medium, LinkedIn, Bitcointalk, YouTube e não somente as tradicionais Twitter e Facebook. Os processos das ICOs devem ser transparentes, pois assim se oferece maior credibilidade aos investidores, que, com esses canais, conseguem contato direto com as equipes do projeto para esclarecimento de dúvidas e para informações do andamento do projeto[3].

O uso de celebridades e artistas está se tornando comum como estratégia de marketing de ICOs. O ator Steven Segal se tornou embaixador do projeto Bitcoin2GEN e a polêmica Paris Hilton se tornou garota propaganda do projeto LydianCoin. Segundo especialistas do criptoespaço, essas ações não são vistas com bons olhos, mas, claro, não há como negar a mídia espontânea que é gerada com a participação deles.

Outra personalidade que investiu em projetos de blockchain foi a cantora islandesa Björk. Diferentemente de Segal e Hilton, a cantora criou o projeto Mycelium para comercializar músicas próprias por meio de criptoativos.

Em 2018 o Twitter e Facebook proibiram publicidades e anúncios de ICOs em suas mídias sociais, o que fez com que o mercado de agências de marketing especializadas em ICO buscasse outros canais para divulgação dos projetos de ICO.

Muitas vezes essas agências acrescentam outros serviços aos seus portfólios, como assessoria jurídica, planejamento de projetos, entre outros. É um mercado extremamente atraente: somente a arrecadação de fundos dos projetos de ICO da Bitcoin MKT Team ultrapassou mais de 100 milhões de dólares em 2017[4].

Ideia de produto

Na avaliação do produto são apreciados os potenciais da solução apresentada e os critérios de diferenciação e inovação em relação aos concorrentes. Também se atenta para a segurança da proposta e para as fragilidades de códigos que podem facilitar fraudes.

Não podemos analisar somente os concorrentes de projetos que utilizam tecnologia distribuída. Há que considerar os produtos substitutos e o custo de mudanças e de aprendizagem dos clientes e usuários na análise da ICO. Existem produtos tecnológicos que podem oferecer as mesmas soluções de forma melhor e mais barata. Nem tudo pode ou deve ser “tokenizado”.

É uma excelente iniciativa mostrar um bom repositório de códigos ou, ainda melhor, um protótipo de trabalho já desenvolvido, apresentando os aspectos a serem cumpridos. No mundo open source isso pode não ser uma fraqueza, e sim um aspecto positivo das reais melhorias que os fundos arrecadados irão proporcionar ao projeto. Atualmente, a maioria das ICOs levanta fundos com base na promessa do produto. Desenvolver um protótipo do produto pode oferecer uma grande vantagem (BR, 2017).

Viabilidade

A ICO deve oferecer uma solução factível. As possibilidades de aplicações de - blockchain são inúmeras, mas claro que há limitações técnicas de códigos, assim como as limitações orçamentárias, de demanda e tecnológicas. Uma ICO deve apresentar números confiáveis e realistas aos investidores, demonstrando que há um mercado potencial a ser explorado e que os custos de desenvolvimento poderão oferecer retornos reais aos seus apoiadores.

Deve haver um fluxo econômico para o token. Por exemplo, os tokens de publicidade: quantos anunciantes necessitarão comprar no futuro? E, em posse desses tokens, quem serão os profissionais de publicidades que aceitam esse criptoativo? O garoto propaganda, as agências de marketing, os editores? Quanto mais descentralizado for o token, melhor, já que aumentará a liquidez. Devem ser evitados mercados monopolizados ou oligopolizados, claro, se esses players não aceitarem seus tokens.

É importante que o investidor procure fontes alternativas para considerar o investimento em uma ICO, considerando as taxas mínimas de atratividade, cálculos de Retorno sobre Investimento (ROI), Taxas Internas de Retorno do Projeto (TIR) e não somente se basear nas projeções otimistas dos idealizadores dos projetos. Os apoiadores e parceiros dos projetos possuem peso na análise de viabilidade, pois podem oferecer maior aceitação junto a certo mercado.

Legalidade

Trata-se de uma questão ainda muito debatida pelos governos. Muitos governos, até mesmo os que apoiam as DLTs e as utilizações de criptomoedas, fazem ressalvas sobre a modalidade de captação de recurso por meio de ICO. As autoridades monetárias dos países não se cansam de emitir alertas à população para os riscos de volatilidade e fraudes nesse tipo de investimento.

As DAOs são aplicações descentralizadas, muitas vezes sem lideranças, que habitam o universo digital. A conformidade legal não as alcança, pois não há um território e leis específicas às quais são submetidas. Quando se trata de DApps, mesmo com o modelo de negócio descentralizado, há uma entidade curadora do projeto, que tende a estar sediada em algum país para buscar interagir com o mercado "tradicional", porém o ambiente de atuação torna irrelevante a jurisdição de seu registro.

A EOS é uma DApp cuja empresa controladora é a Block.one, sediada nas Ilhas Cayman. Para evitar processos judiciais, a EOS decidiu que cidadãos, residentes e entidades dos EUA deveriam ser excluídos da compra de tokens EOS no período de ICO por causa de alguns dos desafios associados às diferentes regulamentações nos muitos estados americanos. A Block.one não acredita que a distribuição de tokens EOS em si são valores mobiliários, commodities, swaps em valores mobiliários ou instrumentos financeiros similares. Os tokens EOS não são projetados para fins de investimento ou especulação e não devem ser considerados assim[5]. Mesmo com a restrição ao mercado americano, a ICO da EOS conseguiu bater o recorde de valor arrecadado, com mais de 4 bilhões de dólares para financiar o projeto.

Países como Suíça e Japão possuem posições mais claras em relação aos ICOs.

Aplicam as leis já existentes para emissão de valores mobiliários. Quando se utiliza o token no modelo de utilidade, aplicam as regulações referentes aos meios de pagamentos e as conformidades quanto ao branqueamento de capitais. Se o apoiador da ICO somente possuir interesse especulativo, devem ser aplicadas as leis de valores mobiliários. Então não basta somente a forma como o token foi criado, mas a legislação a ser adotada dependerá da forma como o comprador usará os tokens adquiridos na ICO (FINMA, 2018).

Em relação à legalidade, os custos estimados pelas ICOs variam de acordo com o país, e é possível encontrar valores de 30 mil dólares para a legalização da oferta inicial de moedas até a provisão de gastos jurídicos de 6 milhões de dólares para a execução do projeto[6].

O fato é que, embora a legalidade jurídica seja secundária para o funcionamento das organizações descentralizadas, a conformidade jurídica é importante para aumentar a credibilidade do projeto, oferecer segurança jurídica ao investidor e evitar paralisações ou multas no funcionamento das organizações. Como exemplo, temos o projeto PressCoin, que, registrado no Reino Unido, ofereceu em sua ICO tokens híbridos de utilidade e propriedade. Após já realizada a arrecadação dos tokens, o governo emitiu notas proibindo os tokens de propriedade, pois não reconhecia aquele tipo de constituição administrativa. A solução da PressCoin foi devolver os tokens a quem não aceitasse as novas regras legais.

Por isso a Blockchain Review (2017) aconselha definir uma jurisdição para operar sob a legislação correspondente, incluindo detalhes quanto a sua estrutura corporativa, impostos, títulos, leis de branqueamentos de capitais e KYC (Know Your Customer), etc.

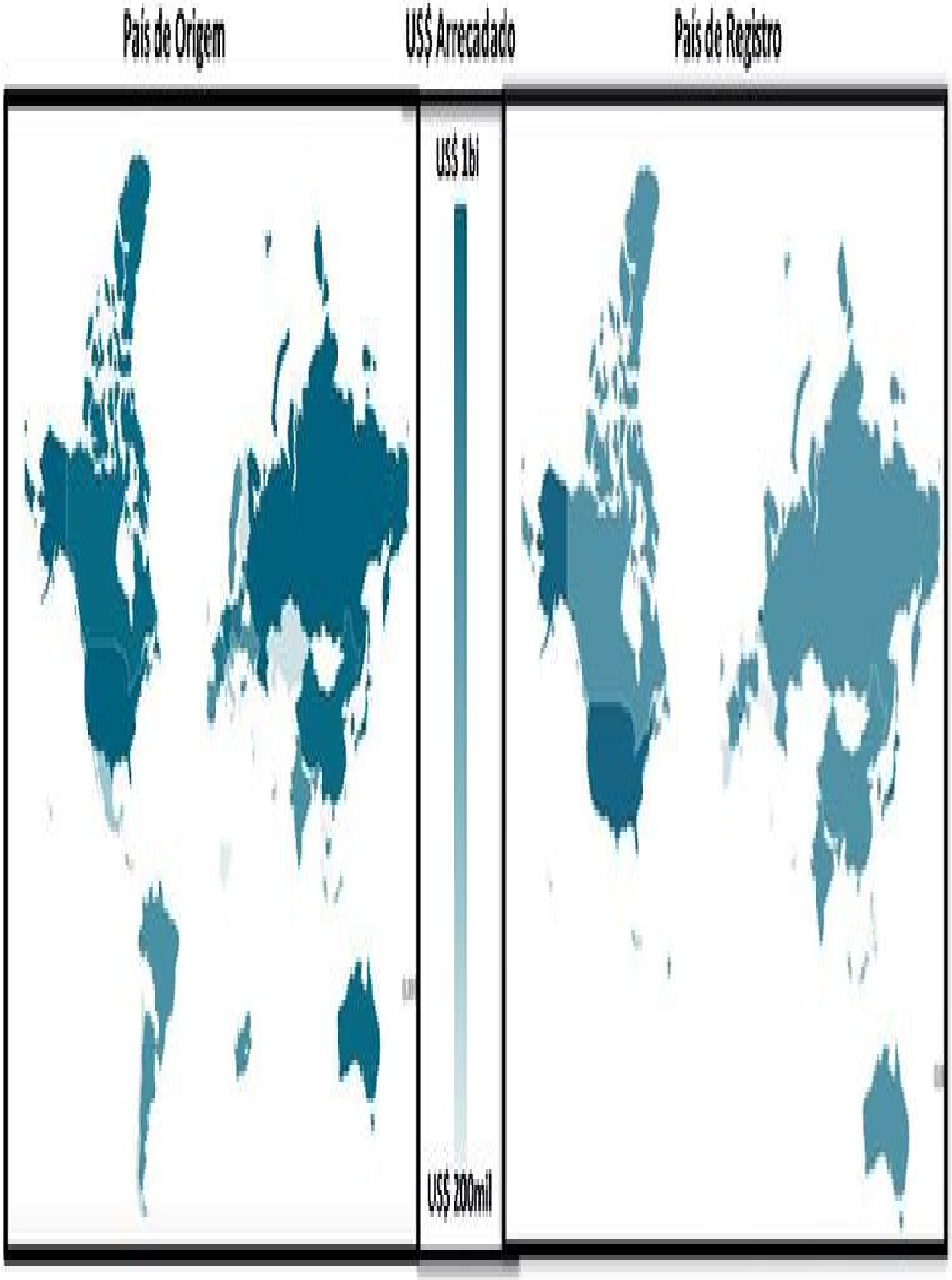

País de Origem
US$ Arrecadado
País de Registro
US$ 1bi
US$ 200mil

Figura 11. Mapa de origens e registros de ICO. Fonte: ICORating. Período: maio de 2018.

O mapa da ICORating clarifica como as organizações descentralizadas buscam países juridicamente seguros para realizar suas ICOs. No Brasil, duas ICOs foram realizadas, mas registradas em outros países que possuem uma legislação com maior segurança jurídica para captação de recursos por meio de ICO. Segundo a ICORating, 121 projetos de ICO foram criados nos EUA, mas apenas 46 se registraram em solo americano. Na Suíça 30 ICOs se submeteram a sua jurisdição, contudo apenas 18 tiveram origem no país. Até mesmo Canadá e EUA, que já possuem regulamentação mais esclarecedora para a realização de ICOs, não atraem os projetos para captar recursos financeiros em seus territórios, por possuírem regulamentações menos atraentes que outros países, como: Gibraltar, Suíça, Malta, Estônia, Liechtenstein, Ilhas Virgens, Ilhas Cayman e Cingapura.

White paper (descrição do projeto)

O white paper é um termo usado há décadas para apresentar e esclarecer projetos governamentais no Reino Unido. Adotado por empresas para enfocar apresentações comerciais, ele também incorpora partes de marketing e técnicas de projetos de ICO e de organizações descentralizadas.

Os white papers podem ser uma peça de marketing para a ICO, mas não só isso. Todos os elementos mencionados anteriormente devem estar especificados de forma clara no white paper, além de maiores informações do projeto de ICO. Nos white papers se encontram estudos de mercado, potenciais de crescimento, todos os detalhes úteis sobre o funcionamento dos tokens, a criptoeconomia do ecossistema, se os tokens serão minerados ou não, seu sistema e os termos do próprio evento de venda. Como os white papers são materiais densos e possuem conteúdos mais aprofundados dos projetos de ICO, são muito úteis os FAQs, que dão acesso mais rápido a informações sobre o projeto.

Devem ser acrescentados os prazos de arrecadação da ICO, de congelamentos do fundo, além das etapas e do roteiro (roadmap) de execução do projeto. Isso oferece garantias ao investidor, que conseguirá estimar um prazo para o uso dos tokens ou para retorno do capital. A distribuição dos tokens e o percentual designado à equipe de desenvolvedores também são informações essenciais a constar nos white papers.

Muitas vezes os códigos do smart contract da ICO e do protótipo do projeto podem não constar nos white papers, mas como a ICO é um processo de arrecadação de fundos, recomenda-se colocar os links de acesso à biblioteca de códigos do projeto.

Lembre-se: o ICO é a apresentação e a venda de um projeto futuro, não um produto já acabado. O sucesso da ICO não representa o sucesso do projeto. Continuar com transparência na gestão do projeto, alimentando os apoiadores com informações e atualizações do cronograma por meio dos canais criados, é fundamental para continuar com o apoio da comunidade, esclarecendo o status do projeto e como os recursos arrecadados estão sendo usados, e mantendo a comunidade ativa e próxima do projeto (BR, 2107).

Modelos de vendas de token

A forma como é estruturada a venda de tokens tem uma grande influência no resultado da ICO. Tem havido muito debate sobre o método ideal para uma venda simbólica, mas a verdade é que não existe um modelo único. O método ideal depende dos objetivos do projeto. Maximizar a quantidade de dinheiro a se arrecadar? Incentivar uma distribuição justa das moedas que você está vendendo entre os investidores? Evitar um despejo de moedas uma vez que ela seja ativada em trocas no mercado? Desejar minimizar os efeitos negativos de sua venda inicial no restante do ecossistema da DO? Se receberá moedas fiats[7] ou somente criptomoedas para financiamento do projeto?

Há muitas coisas a se considerar no design do modelo de venda de tokens, e a - Blockchain Review (2017) nos auxilia na apresentação de alguns:

Pré-vendas privadas

Alguns projetos têm iniciado suas ICOs convidando um público privado de investidores.

Por exemplo: o Telegram, em 2018, criou um token chamado Gram, que servirá como um criptoativo de sua plataforma de mensagem. O projeto inicial era realizar uma pré-venda junto a investidores selecionados e depois oferecer uma abertura para uma oferta pública. Porém, somente na pré-venda foram arrecadados mais de 1,5 bilhão de dólares. Devido ao grande sucesso de arrecadação na pré-venda, a equipe do Telegram desistiu de realizar sua oferta ao público em geral.

O modelo de pré-venda a investidores qualificados é bem atraente e pode selecionar o público-alvo da ICO, mas exclui inúmeros outros participantes interessados – e, pior, pode centralizar os tokens do mercado nas mãos dos investidores selecionados na pré-venda e diminuir a transparência, pois muitas vezes eles não são conhecidos pelos futuros usuários dos tokens, quando o projeto estiver em execução.

Vale ressaltar que para muitos isso não é uma ICO, e muito menos seria um - crowdsale, pela justaposição na composição da palavra. E a argumentação tem fundamentos, mas, como se trata de uma forma de arrecadação de fundos para projetos descentralizados, é importante informar que essa modalidade existe.

Limites fixos (capped sale)

Existe um limite de tokens a serem ofertados a um preço já fixado, e a venda se interrompe quando esse número é alcançado. Podem ocorrer reajustes de preços estipulados previamente durante o período de arrecadação.

As vantagens do capped sale é o fornecimento de uma avaliação fixa para o projeto, o que torna o processo mais transparente para os investidores. Se os investidores acreditarem que o projeto vale mais do que a avaliação implícita no preço simbólico, podem se sentir confiantes em comprar suas moedas. A desvantagem desse modelo é que, se as projeções e análises dos investidores forem mais positivas que a dos criadores, ocorrerá uma corrida para comprar o maior número possível de tokens, podendo deixar alguns investidores de fora do projeto ou concentrar o projeto em grandes investidores que poderão controlar os preços no futuro.

Limite flexível (soft caps)

Um limite de tokens é definido, mas se todos os tokens forem vendidos antes do tempo estipulado de captação novos lotes podem ser disponibilizados até o término do período de arrecadação.

Limite flexível é interessante por possibilitar novos participantes e evitar a concentração em poucos, se isso tiver ocorrido. Pode oferecer mais recursos financeiros ao projeto, além de demonstrar a boa receptividade do mercado à ICO. Uma fraqueza é que há uma estimativa dos tokens que serão criados e não um número exato do montante de tokens que estarão em circulação ao final do período da venda inicial.

Ilimitado e preço fixo (uncapped with fixed rate)

Modelo de venda em que se estipula o valor do token, podendo sofrer reajustes de preço de acordo com datas estipuladas no cronograma de arrecadação, sem limitar o total de tokens que serão emitidos nas trocas de criptomoedas ou moedas fiduciárias a uma relação fixa. Este modelo exige um período específico de contribuição.

A vantagem é vender suas moedas a um preço predeterminado, mas sem limitação de tokens; logo, todos os interessados podem participar do projeto e, em vez de definir o valor do seu projeto pela própria avaliação, o mercado o fará de forma mais natural. Assim, quanto mais pessoas investirem, mais tokens serão criados. Porém, embora saibam o preço dos tokens que estão comprando, os investidores não sabem a avaliação implícita do projeto porque não sabem quantos tokens existirão no final do período da venda.

Leilão holandês

Um leilão holandês é uma estrutura de oferta pública de moedas na qual o preço da oferta é definido após a aceitação de todas as propostas. Nesse tipo de leilão, os investidores fazem uma oferta pelo valor que estão dispostos a comprar em termos de quantidade e preço. Os lances são classificados do maior para o menor. As ofertas mais altas são aceitas até que a soma das quantidades desejadas seja suficiente para vender todos os tokens ofertados. Depois que o último lance for aceito, todos os proponentes com um lance aceito receberão os tokens.

Essa modalidade é interessante por deixar o mercado avaliar o valor do seu projeto, e já sabendo a previsibilidade da quantidade de tokens que serão emitidos, mas joga a incerteza do valor a ser arrecado para os desenvolvedores do projeto de ICO. Dessa forma, é um modelo a ser adotado para projetos que possuam bons recursos financeiros, redes consolidadas e que busquem ampliar seu mercado com novos participantes.

Leilão holandês reverso

No leilão holandês reverso o valor inicial dos tokens é estipulado pelos executores do ICO e assume valores decrescentes ao longo do período do tempo, até que seja alcançado o valor total de arrecadação ou todos os tokens sejam distribuídos. A venda termina no primeiro dia se apenas X% do total de tokens forem vendidos, mas alcançarem a meta de arrecadação. Se ao primeiro dia não houver o alcance da meta, no segundo dia os preços diminuem e são ofertados X + Y% dos tokens totais, e assim por diante.

O exemplo mais expoente deste modelo no criptomercado foi a ICO da Gnosis, que limitou o teto de venda a US$ 12 milhões ou 9 milhões de tokens. A cada dia o valor dos tokens da GNO cairia e a lógica seria que as pessoas estariam dispostas a comprar no último dia, quando o preço estivesse mais barato. Ocorreu o contrário. Em questão de minutos a Gnosis arrecadou os US$ 12 milhões, alcançando a meta de captação, disponibilizando apenas 5% de seus tokens no mercado e ficando com o restante dos tokens.

O benefício deste modelo é que o valor estipulado pelos idealizadores do projeto possui uma estimativa mais realista dos recursos financeiros necessários para a execução de todo o roteiro. Mas Buterin (2017a) acredita que o leilão holandês reverso trabalha o psicológico do FOMO (fear of missing out, medo de perder) dos investidores, pois a lógica deste modelo seria sempre esperar o último dia do leilão e aproveitar o melhor preço, mas o medo de ficar de fora da oportunidade é que pode fazer os investidores agirem irracionalmente. Além disso, como ocorreu no leilão da Gnosis, há o risco de o leilão terminar rápido e um grande número de tokens ficar concentrado na mão dos idealizadores, o que exige ainda mais confiança na equipe do projeto.

Recolher e devolver (collect and return)

A contribuição total do montante a ser arrecadado e o número de tokens são fixos, mas um contrato inteligente fica aberto para contribuições que podem exceder o montante fixado. Após a finalização do período de arrecadação, as contribuições são ajustadas proporcionalmente e a diferença das contribuições são devolvidas para seus legítimos proprietários.

Trata-se de um modelo de arrecadação exclusivo por criptomoedas, já que é necessária a execução de um contrato inteligente. É interessante por possibilitar a distribuição de tokens de forma mais igualitária e com o valor do criptoativo criado já estipulado. Porém, se há um grande interesse de investidores participantes do projeto em devolver os recursos financeiros disponibilizados que poderiam agilizar o prazo de execução e ser usados em outras atividades, como a de marketing, por exemplo, isso pode ser prejudicial.

Limites dinâmicos

Método com uma série de pequenos conjuntos de limites ocultos de oferta de tokens em intervalos de tempo específicos. Este método limita a quantidade máxima que pode ser investida em cada etapa da venda. Os grandes investidores devem desmembrar suas transações em lances menores, incorrendo em mais custos por transação. Se uma transação ultrapassa o limite máximo, ela é rejeitada.

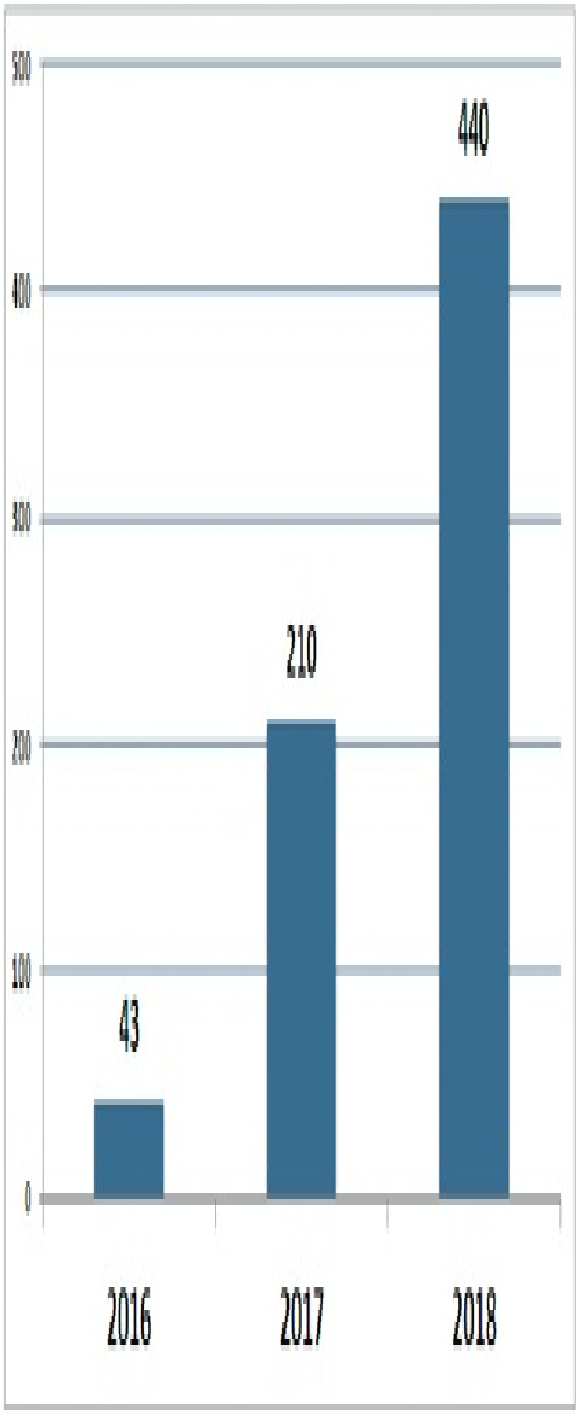
Este tipo de modalidade foi usado pela Filecoin, que ampliou em anos os intervalos de vendas de tokens. Estender o prazo de arrecadação é interessante porque demonstra os objetivos de longo prazo da ICO e passa segurança aos investidores, pois facilita o reconhecimento da aplicação dos recursos em cada etapa de arrecadação do projeto e sua evolução.

Outras considerações sobre ICOs

Quando feitos corretamente, os eventos de distribuição de tokens possuem um papel importante no futuro do projeto. Não há modelo perfeito para a realização de uma ICO. Preferencialmente, uma ICO deve ser acessível e oferecer algumas variedades de criptoativos para participação no investimento, e a distribuição de tokens deve alcançar uma base de usuários qualificada para cada projeto.

E mesmo com a enorme insegurança jurídica na maioria dos países, por falta de regulamentação específica, o modelo de arrecadação de fundos por meio de ICOs não para de crescer. Mesmo na metade do ano de 2018, o número de projetos e montante arrecadado já é mais que o dobro da soma de todos os anos anteriores.

Quantidade de ICO



Arrecadação em US$

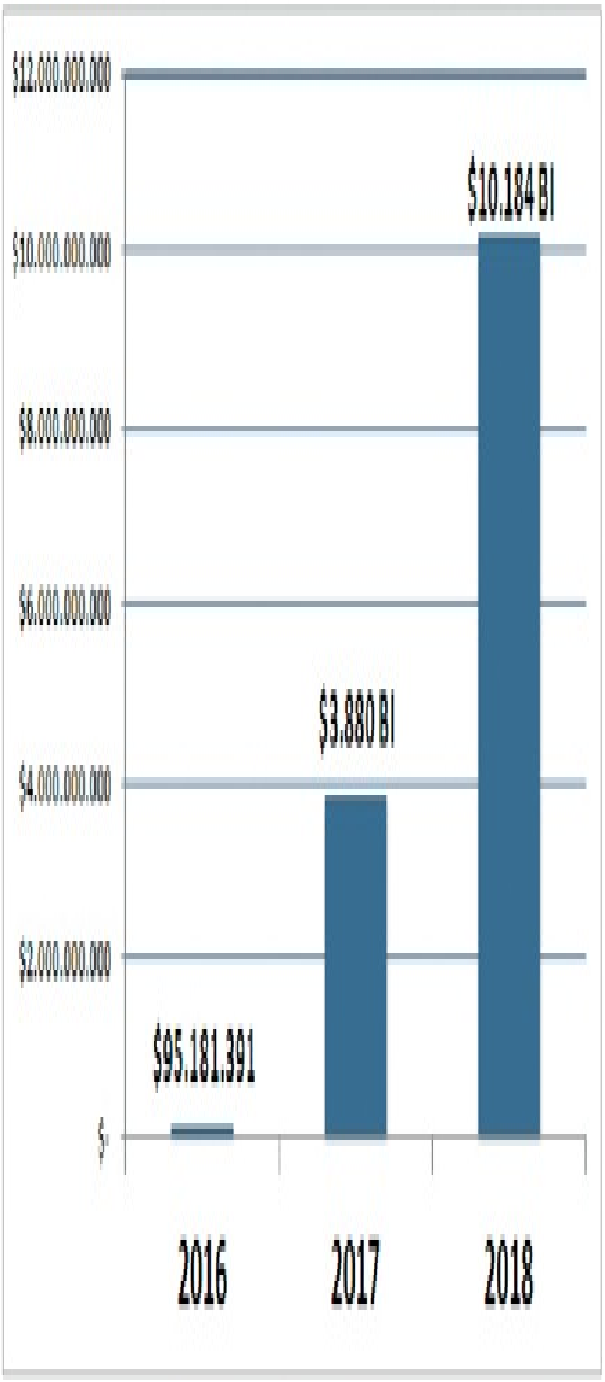


Figura 12. Gráfico anual de fundos arrecadados e projetos concluídos de ICO. Elaborado pelo autor.

Fonte: COIN SCHEDULE, junho de 2018.

A arrecadação de recursos é somente o pontapé inicial de uma DO. Devido aos grandes montantes em posse das equipes de projetos de ICO, a gestão dos fundos arrecadados deve ser transparente com os investidores e oferecer status e progressos do evento constantemente. Algumas propostas de gestão de fundos ICO têm surgido em meados de 2018, como a proposta do projeto CGS (Coin Governance System)[8] e o modelo DAICO de Vitalik Buterin, que permitem votações e liberações de recursos para a equipe executora do projeto de acordo com a sua evolução. Essas propostas de gestão coletiva de fundo também possibilitariam a retirada dos valores investidos nas ICOs e mesmo a sua extinção. Apesar de oferecer maiores garantias aos investidores, também poderiam ocorrer interesses de retiradas dos fundos por questões especulativas, como a valorização do criptoativo empregado no investimento da ICO, onde a retirada dos recursos do projeto seria mais vantajosa que a própria expectativa de retorno dos tokens do projeto. São duas propostas que até o momento não foram testadas, como grande parte dos projetos de ICO em si.

Vitalik (2017) propõe que todos os tokens não vendidos, em vez de ficarem parados, poderiam atuar na estabilidade do preço do token no mercado, com auxílio de criadores de mercados autônomos, assim como os próprios fundos arrecadados com outras criptomoedas.

Por fim, Schumpeter, em 1911, nos dizia que os banqueiros não são somente os intermediários do sistema financeiro. Eles seriam os éforos do sistema, que autorizariam o financiamento para a realização de novas combinações socioeconômicas, autorizando as pessoas a formá-las em nome da sociedade. E, como vimos, as ICOs são uma forma de financiamento inovador, sem intermediários para ditar quais serão as novas combinações que irão surgir. Esse

fato poderá redesenhar o curso da economia mundial e nos oferecer arranjos econômicos nunca vistos na história.

Capítulo 5. Fatores Intrínsecos

“É seu dever manter a ordem? É seu dever de cidadão?

Mas o que é criar desordem? Quem é que diz o que é ou não?

São sempre os mesmos governantes, os mesmos que lucraram antes.”

(Britto, Fromer e Gavin, “Desordem”)

Atividades

As atividades principais de uma organização descentralizada são realizadas por agentes autônomos, na maioria das vezes. A princípio, as organizações descentralizadas entregam os seus códigos e protocolos e as pessoas se incumbem de participar da execução das tarefas distribuídas.

Ao analisar as principais DOs, vemos que as aplicações de criptomoedas e as cadeias de blocos mais similares ao blockchain 1.0 são as que realmente possuem atividades, e seus projetos, embora em constante melhoria, estão consolidados e funcionais. Destacam-se aqui Bitcoin, Dash, ZCash, Litecoin e Monero, que são projetos que já alcançaram algum nível de maturidade. Ao analisar as propostas de tokens que oferecem infraestrutura de protocolos base e plataformas blockchain 2.0, criadas com suporte de contratos inteligentes e/ou maiores facilidades para criação de sidechains e novas DApps, com exceção do Ethereum, NEM e Steem, verifica-se que a grande maioria ainda está em fase de desenvolvimento de seus projetos apresentados na ICO.

No gráfico a seguir, onde está identificado “infraestrutura”, estamos falando das plataformas blockchain que oferecem possibilidade de hospedar os sidechains. Durante os anos anteriores, os protocolos base de consenso atraíam maiores recursos financeiros. Agora, com a consolidação dessa plataforma de infraestrutura, percebemos que em 2018 são as aplicações descentralizadas de camadas superiores que têm despertado os investidores. Isso é devido exatamente ao crescimento do blockchain 2.0.

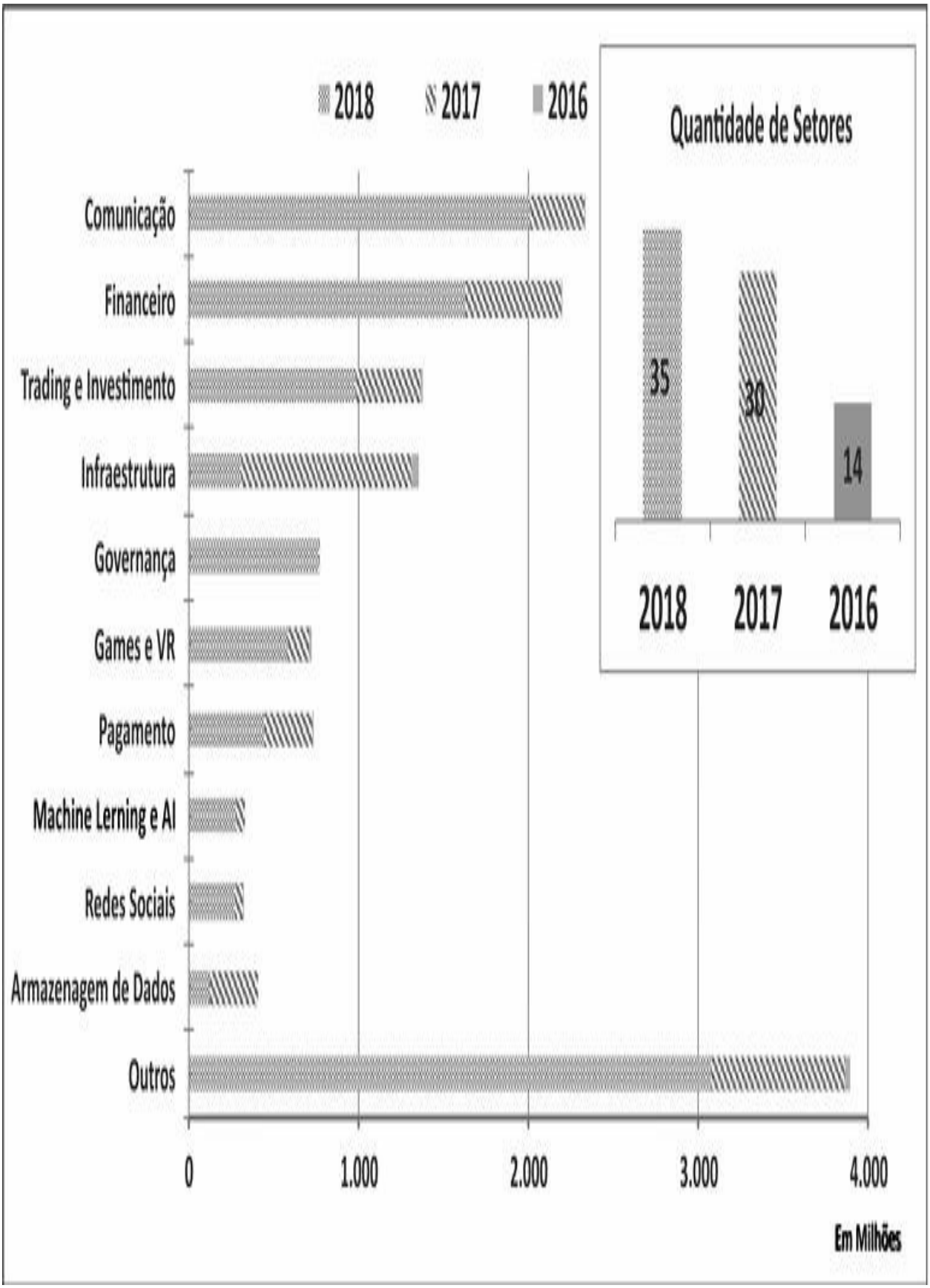

2018
2017
2016
Comunicação
Financeiro
Trading e Investimento
Infraestrutura
Governança
Games e VR
Pagamento
Machine Lerning e AI
Redes Sociais
Armazenagem de Dados
Outros
0
1.000
2.000
3.000
4.000
Em Milhões
Quantidade de Setores
35
30
14
2018
2017
2016

Figura 13. Principais setores de arrecadação das ICOs – anual. Elaborada pelo autor.

Fonte: COIN SCHEDULE, junho de 2018.

As aplicações descentralizadas atuam em diversas áreas. Oferecem serviços de nuvens, computação, mídias sociais, insurtech[1], marketing, mercados e corretoras, entre inúmeras outras possibilidades que surgem a todo momento. Somente em relação a marketing digital existem mais de cinco mil aplicações descentralizadas[2].

Até junho de 2018, foram finalizados 440 projetos de ICO, arrecadando um valor próximo de 11 bilhões de dólares. Esse valor já é o triplo da arrecadação das 210 ICOs realizadas em todo ano de 2017. Os altos valores têm participação direta da pré-venda realizada pelo Telegram, o Petro, o criptoativo lastreado em barril de petróleo da Venezuela, que arrecadou 735 milhões de dólares, e a EOS, com 4 bilhões.

A análise gráfica nos mostra a variedade dos setores das aplicações descentralizadas. São ao todo 35 setores diferentes que buscam financiamento por meio de ICO para desenvolvimento de aplicações descentralizadas[3]. E esse número é maior, pois várias DOs não iniciam seus projetos por meio de ICO. Mas ao menos o gráfico oferece alguma tendência das atividades e dos mercados em que as DOs atuarão.

Um exemplo de tarefa possível de ser executada por uma DO é a junção da inteligência artificial com o agente autônomo da AdHive, que tem a proposta de automatizar o mercado publicitário dos influenciadores digitais.

A plataforma AdHive atua como um serviço de matchmaking para anunciantes e influenciadores

Figura 14. Tarefas DApp do AdHive. Fonte: AdHive.[4]

Grande parte das tarefas das DOs é executada por seus participantes. O projeto - Filecoin, que oferece serviços de armazenamento de dados, preocupado com a qualidade dos seus serviços, exige que os participantes preencham um formulário com especificações técnicas de seus hardwares e banda larga para que possa se tornar um ofertante de serviço de aluguel de HD em seu projeto. Essa exigência preza em manter a qualidade dos serviços aos clientes finais, selecionando participantes mais bem qualificados.

Assim, percebemos que os aspectos tecnológicos das DOs frequentemente estarão no ambiente externo.

Tecnologia

A tecnologia é a essência da existência das DOs. Está presente em todas as etapas e variáveis das organizações descentralizadas, desde o início do projeto, como nos meios de comunicação, até o fim, com a entrega do produto.

A tecnologia das DOs se torna um diferencial, principalmente em relação à adoção de novos participantes. Muitos projetos são complexos em sua lógica, em seus códigos e em sua linguagem de programação. Não basta possuir uma programação ótima se apenas um número reduzido de especialistas conseguirá participar. Inúmeras plataformas já apresentam linguagens populares, como Java, C#, Python e outras, que facilitam o desenvolvimento de novas aplicações.

A maior simplicidade e a adoção de front-ends amigáveis facilitam a adoção de leigos em programação, sendo um diferencial no negócio das DOs. Block Cat, EtherParty e MyWish já possuem esses serviços para criação de contratos inteligentes. O API Storj Share facilita a configuração do computador para aluguel de HD, na nuvem distribuída da Storj. A NEM possibilita a criação de tokens em seu protocolo de segurança em menos de dois minutos em sua própria carteira. A rede social Nexus possui uma interface próxima do Facebook, o que facilita a adoção e a aprendizagem dos usuários, assim como a Steemit, que realiza constantes melhorias em seu front-end, adicionando também novos recursos em seu ecossistema.

Mas uma DO que foque somente em front-end não está com uma visão holística de sua atividade. Muitas aplicações em blockchain não são possíveis e nem recomendáveis que sejam executadas em notebooks ou smartphones. Várias necessitam de hardwares específicos. Bom exemplo é toda a cadeia de blocos da rede Ethereum, que se aproxima a 1 TB. Mesmo com a tendência de aumento de

capacidade e queda de preços dos novos HDs, o crescimento do tamanho da rede Ethereum é bem superior à adesão dos nodos participantes a HDs de capacidades maiores. Mantendo-se a tendência de crescimento dessa cadeia de bloco, possivelmente grande parte de nodos, validadores na rede, será excluída, tornando a rede centralizada a poucos privilegiados com boa capacidade de armazenamento sobressalente em hardwares.

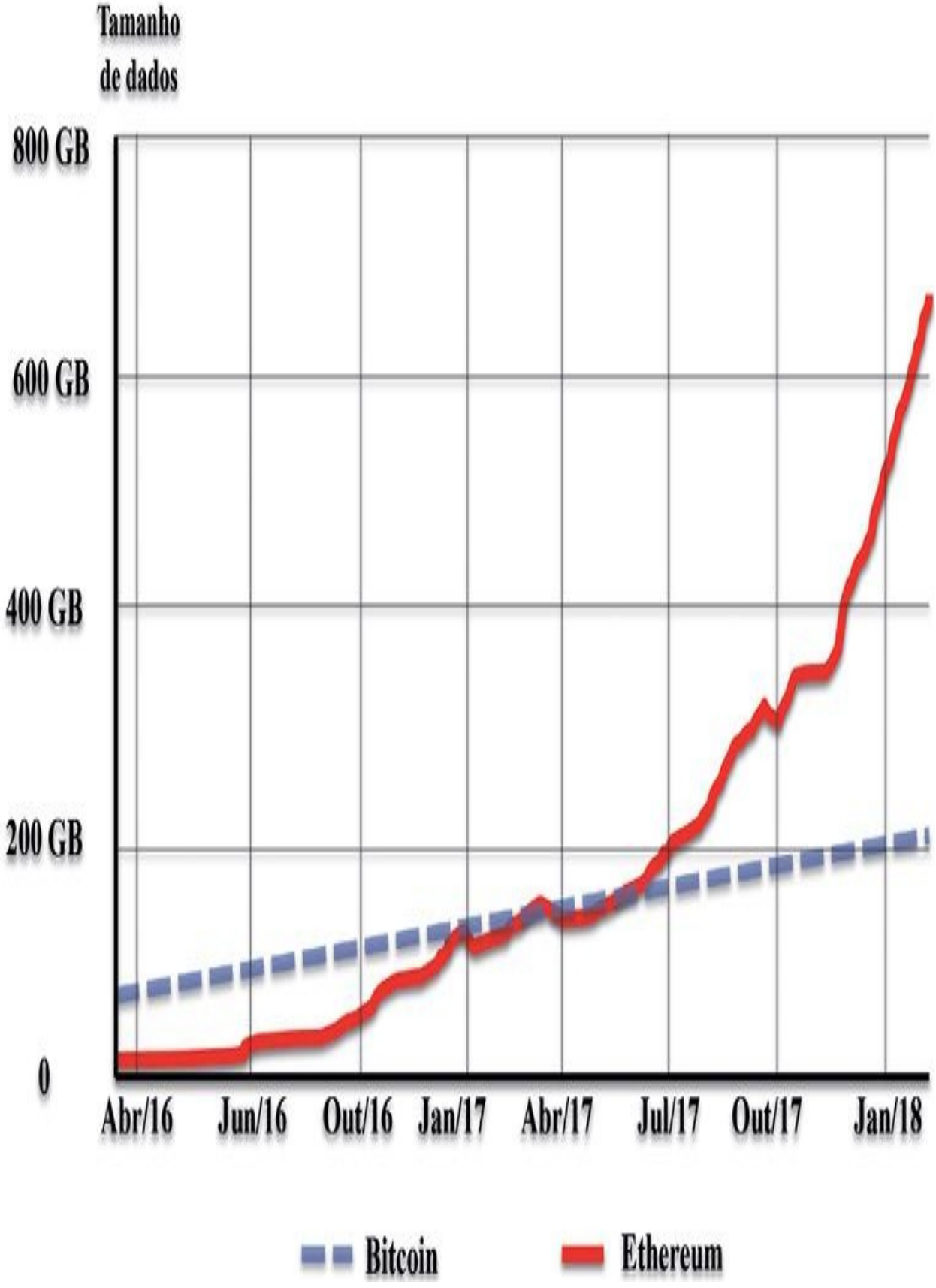

Tamanho
de dados
800 GB
600 GB
400 GB
200 GB
0
Abr/16
Jun/16
Out/16
Jan/17
Abr/17
Jul/17
Out/17
Jan/18
Bitcoin
Ethereum

Figura 15. Tamanho do blockchain Bitcoin/Ethereum. Adaptado de: <http://bc.daniel.net.nz/>.

Acesso em: 05 set. 2018.

A criação de projetos descentralizados com uma visão mais longeva deve atentar para as leis de Moore e de Nielsen. A lei de Moore afirma que a capacidade de processamento dos computadores cresce cerca de 60% por ano, enquanto os estudos de Nielsen mostram que as bandas de internet crescem apenas 50%. Em dez anos, enquanto a capacidade de processamento crescerá dez vezes mais, a velocidade da internet somente crescerá 57% (NIELSEN, 1998). Assim, o aumento de latência da rede e a falta de sincronismo entre os nodos da rede blockchain também são fatores de atenção para as DOs que adotam blocos maiores, já que a transferência de dados entre eles será maior e mais demorada. Isso corrobora o Teorema de CAP, que afirma que um sistema distribuído tem que optar entre duas das três variáveis: consistência, disponibilidade e participação (RAY, 2018).

A Parity trabalha e busca desenvolver soluções para o problema atual da rede Ethereum (SCHOEDON, 2017). Mas é possível encontrar críticos às propostas da Parity, que acreditam que as soluções não resolvem a centralização dos nodos completos. Os requisitos e custos de manutenção precisam ser baixos (STOPANDDECRYPT, 2018). As exigências físicas e de trocas constantes de hardwares são um problema não somente financeiro como ambiental, pois reduzir a vida útil de equipamentos por exigências da aplicação pode aumentar o descarte de produtos no meio ambiente.

O blockchain é um campo em rápido movimento, uma “metatecnologia”, que afeta e é afetada por outras tecnologias, também revolucionárias, que também estão distantes de suas maturidades. É difícil estimar seu alcance, mas é necessário verificar se as exigências tecnológicas externas aos protocolos podem restringir a descentralização e até mesmo centralizar as aplicações de blockchain.

Governança e estrutura organizacional

A estrutura organizacional aborda as relações hierárquicas e as relações formais e informais de uma organização (CHIAVENATO, 2014). Ao contrário das organizações tradicionais, onde a tomada de decisões é concentrada no topo, o processo decisório de uma DAO pode ser estruturado diretamente na origem de seus códigos. Ao facilitar a coordenação e a confiança, um blockchain permite novas formas de ação coletiva e tem potencial de contornar falhas de governança resolvendo muitos dos problemas relacionados à opacidade e corrupção presentes em tomadas de decisões de muitas organizações tradicionais (WRIGHT; DE FILIPPI, 2017).

Em uma DAO a estrutura é completamente horizontalizada, embora os papéis dos nodos possam assumir responsabilidades diferentes na organização da rede. As pessoas podem escolher atuar de diversas formas, como: investidores, usuários, validadores, mineradores, desenvolvedores, marketing de forma individual, coletiva e sem nenhuma ligação direta com o núcleo do projeto. Tal fato torna-se um novo desafio para a governança descentralizada de larga escala.

Após três anos de existência do bitcoin, outras criptomoedas começam a surgir com novos protocolos e propostas distintas. Por exemplo: a litecoin, que é um fork do bitcoin, com mudanças relativas à velocidade das transações. Com as novas concorrentes, a comunidade bitcoin começou a questionar como poderia atualizar os códigos do bitcoin. Estando na primeira geração de organização descentralizada e autônoma, sem a utilização de contratos inteligentes em sua gestão, o bitcoin adota um processo de governança que segue o princípio da aceitação da “maioria econômica”[5].

Meni Rosenfiel considerou que uma alteração ao protocolo imposta pela maioria

dos mineradores seria irrelevante, pois, se os mineradores tentarem mudar o protocolo por conta própria, eles simplesmente serão ignorados pelo resto da rede e suas “recompensas de mineração” serão inúteis. Uma mudança requereria uma maioria econômica – adoção pelos usuários e empresas que dão o valor da moeda[6].

Teoricamente, as propostas de melhoria do bitcoin (BIP, Bitcoin Improvement Proposal), começam em listas de discussões de desenvolvedores do bitcoin, onde qualquer um pode se cadastrar, e respeitam o fluxo a seguir.

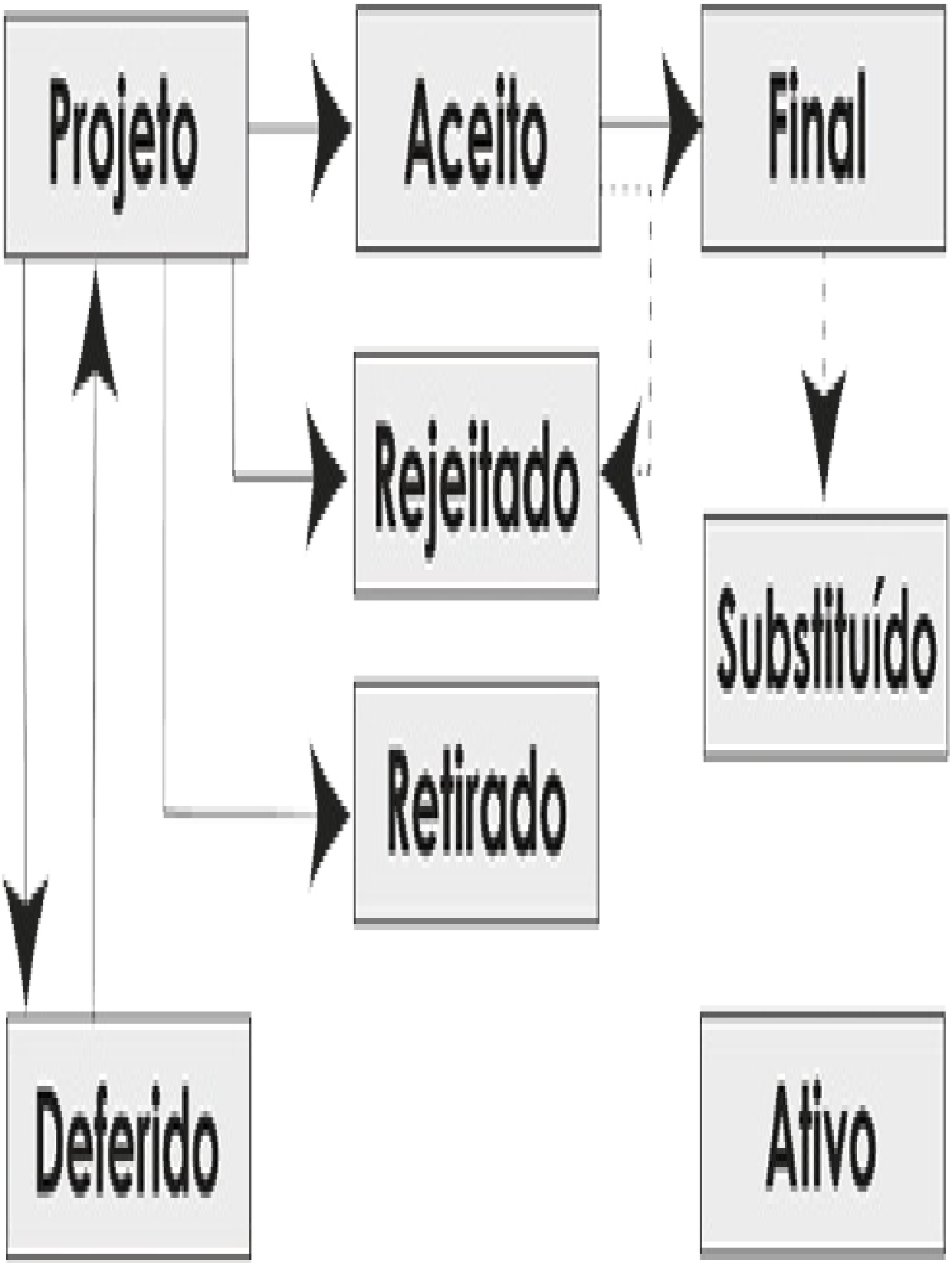

Projeto
Aceito
Final
Rejeitado
Substituído
Retirado
Deferido
Ativo

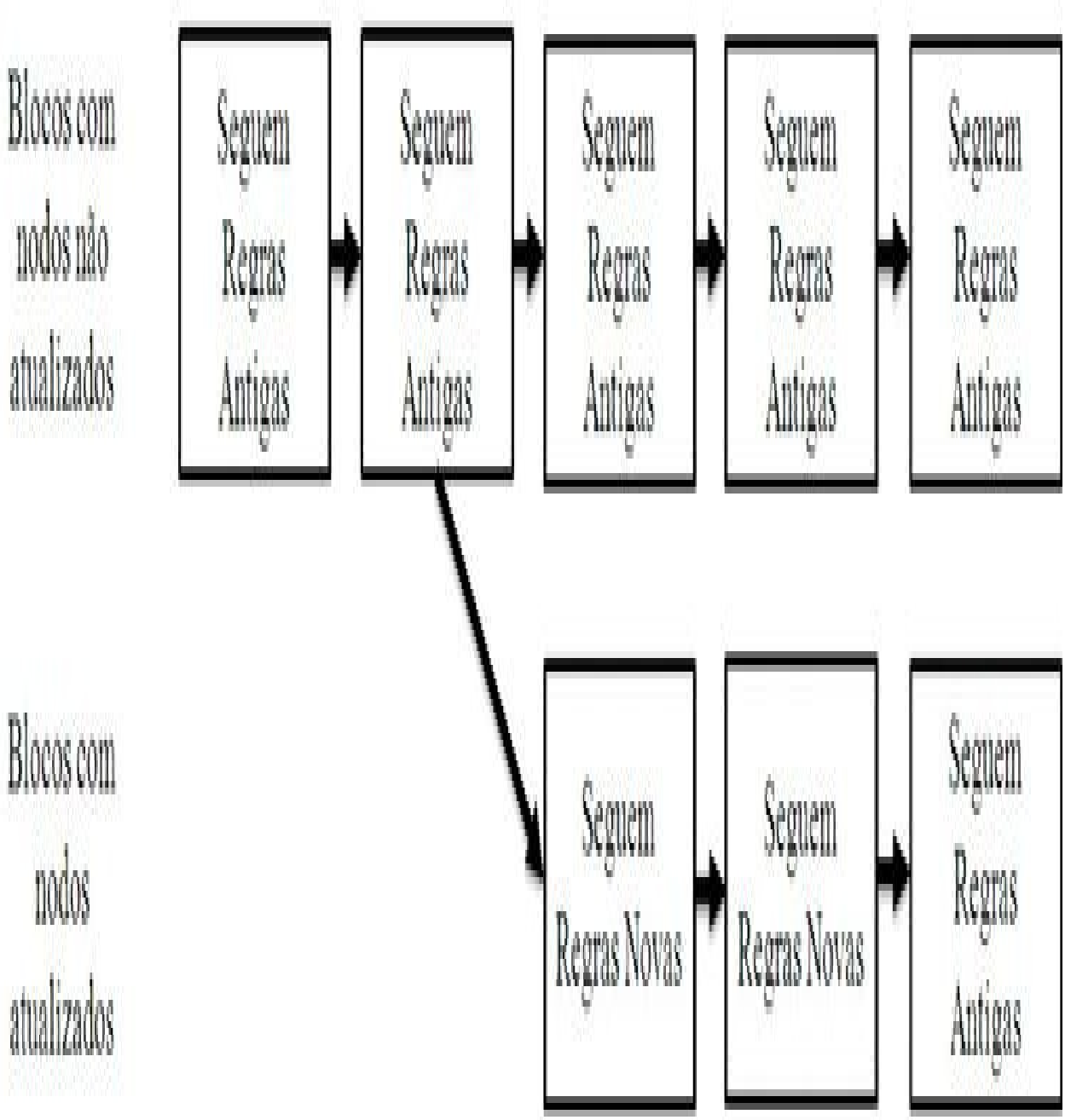
Figura 16. Fluxo de propostas de melhoria no bitcoin (BIP). Fonte: adaptado de Bitcoin Wiki.

Embora o processo pareça simples, alcançar o consenso é difícil, e reconhecer a maioria econômica é algo subjetivo. A pesquisa de Hileman e Rauchs (2017) aponta que 70% dos grandes mineradores classificam sua influência no desenvolvimento do protocolo como alta ou muito alta. E um exemplo dessa falta de consenso foi a atualização do SegWit, proposta de atualização que obteve amplo apoio entre os desenvolvedores do Bitcoin Core, maior organização de suporte aos nodos clientes do bitcoin, que, em discordância com mineradores poderosos como a Bitmain, estimularam a atualização do SegWit para o protocolo do blockchain.

A proposta do SegWit visando o aumento da escalabilidade mostrou a natureza política dos debates em relação às atualizações no bitcoin. Não há um, mas dois subreddits dedicados ao bitcoin na plataforma Reddit: “/r/Bitcoin” e “/r/btc”. Uma comunidade é veementemente oposta à outra. O “/r/Bitcoin”, com mais de oitocentos mil seguidores, é controlado principalmente pela equipe do Bitcoin Core. A comunidade “/r/btc” foi criada como uma resposta à alegada prática dos moderadores do “/r/Bitcoin” – o subreddit original do bitcoin – de banir os membros por expressarem críticas negativas ao SegWit e/ou apoio a outras propostas contrárias aos interesses da Bitcoin Core. Hoje, ambas as páginas estão repletas de acusações mútuas, diálogos imaturos e propagandismo. Os recém-chegados podem ficar mais propensos a ler apenas o subreddit “/r/Bitcoin”, possivelmente sendo influenciados pelas discussões e propostas que acontecem ali (MARSHALL, 2017). Essa crise na governança do protocolo do bitcoin estimulou mais um garfo rígido (hard fork) na cadeia de blocos.

Hard fork

Uma bifurcação forçada ou “garfo rígido” (hard fork) é uma mudança radical no protocolo que torna inaceitáveis blocos e transações de versões desatualizadas a partir de um certo ponto histórico de uma cadeia de blocos. Um garfo rígido causa uma divisão permanente da versão anterior da cadeia de blocos, não sendo aceita mais a participação dos nodos que executam versões anteriores. Para que se evite um garfo rígido, é necessário que todos os nodos ou usuários atualizem para a versão mais recente do software de protocolo. Não havendo consenso sobre a proposta de atualização, duas cadeias de blocos são executadas, sendo aceitas todas as transações anteriores, consolidadas até o momento da atualização, conforme imagem a seguir (TAR, 2017).



Garfo Rígido: os nodos não atualizados rejeitam as novas regras. Dividem o Blockchain.

Figura 17. Garfo rígido. Fonte: adaptada de: bitcoin.org, 2018.

Vale ressaltar que já ocorreram diversos forks no bitcoin e a falta de consenso dos participantes é somente um dos fatores possíveis para os forks nas cadeias de blocos. Por mais que melhores funcionalidades possam surgir, os constantes forks podem gerar inflação no ecossistema, duplicando o número de tokens de bitcoins no mercado.

Com a popularização dos contratos inteligentes, os possuidores de tokens começam a participar das tomadas de decisões por meio de votação, criando uma autoridade de distribuição em toda a organização, sem a necessidade de qualquer parte centralizada confiável, surgindo a possibilidade de consenso de governança através de um meio mais democrático. E para defender uma real “maioria econômica”, o peso de cada voto pode ser diferente de acordo com a quantidade de tokens de cada proprietário. Wright e De Filippi (2017) afirmam que as interações e conformações podem ser predefinidas por contratos inteligentes, e pessoas ou máquinas podem interagir sem ter que confiar na outra parte. A confiança não repousa na organização, mas antes, dentro da segurança e auditabilidade do código subjacente, cujas operações podem ser escrutinadas por milhões de olhos.

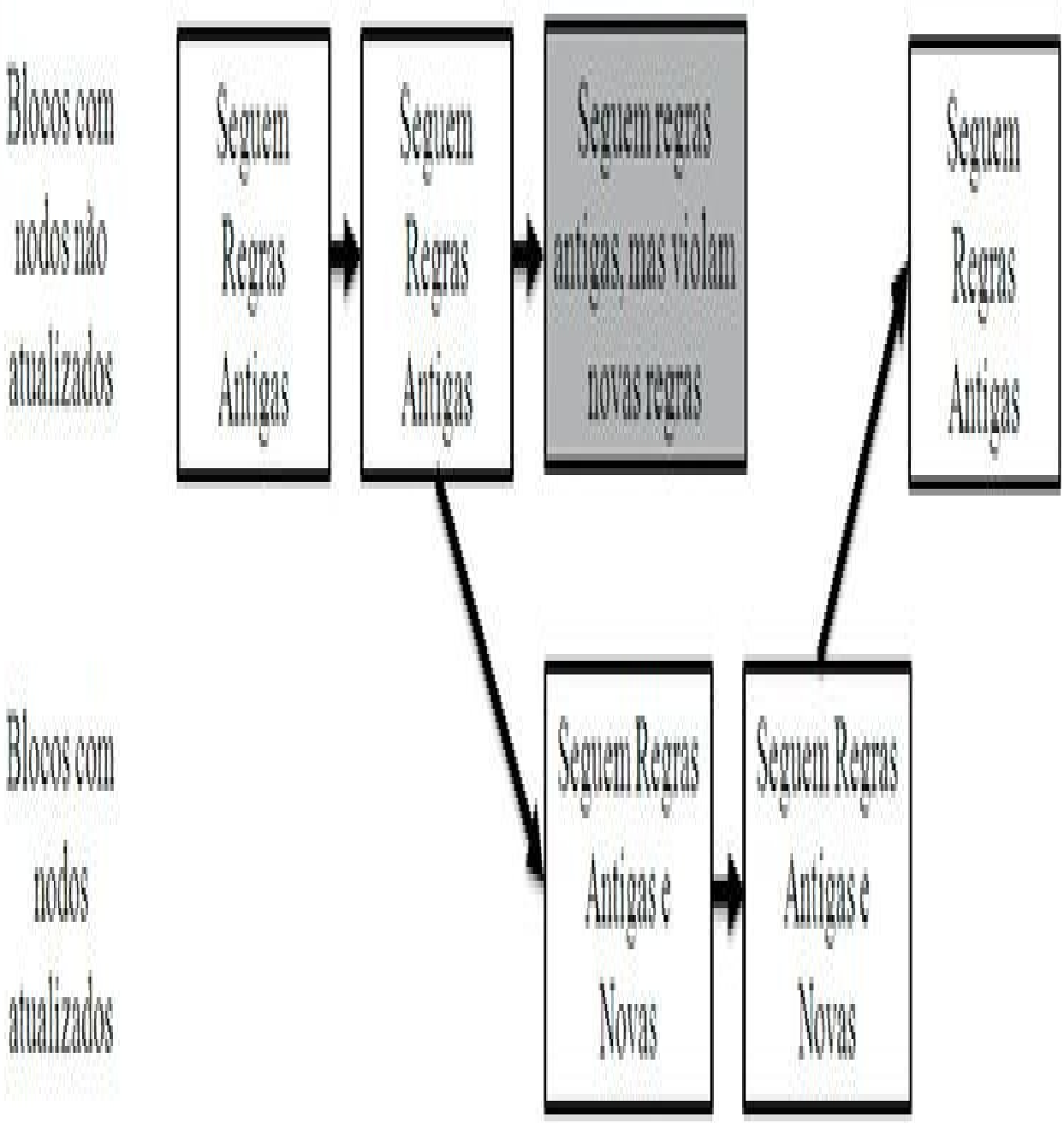
Os votos dos detentores dos criptoativos de uma rede são usados para decidir quem opera os supernodos em uma rede DPOS; por exemplo, em EOS, NEO, Lisk, entre outras DOs. Também são utilizados para votar em parâmetros de protocolo; por exemplo, Ethereum para limite de taxas. Às vezes, votam-se e implementam-se diretamente as atualizações de protocolo por atacado; por exemplo, Tezos. Em todos esses casos os votos são automáticos. O próprio protocolo contém toda a lógica necessária para alterar o conjunto de validadores

ou atualizar suas próprias regras e o fazendo automaticamente em resposta ao resultado de votos (BUTERIN, 2017b).

Embora pareça que tudo são flores, a gestão das DOs é conturbada. O fracasso do The DAO sempre é lembrado, principalmente ao se tratar do uso de contratos inteligentes na ICO e da postura adotada na resolução do problema.

A comunidade Ethereum, que estava intimamente ligada à comunidade The DAO, foi fortemente afetada pelas consequências de um ataque ao contrato inteligente que administrava o fundraiser da The DAO. Em 17 de junho de 2016, apenas algumas semanas após seu lançamento, o The DAO foi invadido. O atacante explorou um bug no código, drenando-o de 3,6 milhões de ether, valendo mais de US$ 50 milhões no momento do ataque. Dada a extensão do ataque, alguns membros influentes da comunidade Ethereum, incluindo seu inventor Vitalik Buterin, sugeriram duas maneiras possíveis de resolver o problema, que exigiriam a cooperação da comunidade Ethereum. A primeira seria a realização de um garfo rígido e a segunda um garfo flexível (soft fork). O garfo flexível foi votado pela maioria da comunidade como a melhor solução para o problema.

Um garfo flexível pode ser adotado quando um bloco que viola as regras novas de consenso é rejeitado pelos nodos atualizados, mas aceito pelos nodos não atualizados. Por exemplo, um recurso de transação abusiva é usado em um bloco: os nodos atualizados o rejeitam porque violam as novas regras, mas os nodos não atualizados o aceitam porque seguem as regras antigas, como exemplificado na imagem.



Garfo flexível: blocos que violam novas regras são tornados obsoletos pela atualização da maioria dos mineradores.

Figura 18. Garfo flexível. Adaptada de Bitcoin.org[7].

A fim de evitar que o hacker recebesse os ethers do fundraiser do The DAO após o prazo estipulado de 28 dias para a execução do contrato inteligente, o soft fork foi votado e estava realmente perto de ser introduzido. Poucas horas antes de ser lançado, alguns membros da comunidade Ethereum encontraram um bug na implementação e foi recomendado que se realizasse um garfo rígido (LANGE, 2018). O problema é que legitimar o garfo rígido equivale a voltar no tempo antes da violação dos fundos The DAO, negando assim ao atacante a oportunidade dos tokens tomados e acabando com o ideal de imutabilidade dos blockchains (DE FILIPPI, 2016).

O incidente provocou um debate animado sobre como o consenso na comunidade Ethereum deveria funcionar. Críticos de dentro das comunidades The DAO e Ethereum, e até mesmo da comunidade bitcoin, notaram que os detentores de tokens The DAO nunca tiveram direito a voto na decisão sobre como resolver a violação. A questão foi resolvida no nível blockchain Ethereum em vez de no nível de aplicação The DAO. Além disso, os defensores do garfo rígido do Ethereum foram acusados de tentar salvar The DAO por ser um projeto muito grande para falhar (até então a maior ICO já realizada). Os críticos perguntaram por que a Fundação Ethereum estava interferindo no The DAO, comparando-a com um governo resgatando um banco falido. De acordo com os críticos, voltar na história e reverter as transações matou a ideia de registros imutáveis, introduzindo assim a censura a um sistema que prometia ser resistente à censura. Os puristas insistiram na regra do código. O suposto agressor, alegaram eles, não era um atacante, mas apenas um indivíduo que usava as possibilidades do código para recursivamente enviar fundos para o seu próprio endereço, um bug no código do contrato inteligente The DAO. No The DAO o código foi referido no site como a única fonte de verdade. O atacante, a partir dessa perspectiva, não era de fato um invasor, e a culpa estava nas pessoas que escreveram o código e promoveram o The DAO (SHERMIN, 2017). Ao fim, a Fundação Ethereum seguiu a cadeia de blocos que havia retroagido para antes da ação do hacker, enquanto outros, que acompanharam a cadeia de blocos original,

passaram a chamar essa bifurcação de Ethereum Classic.

Para Freeman (1972), ao contrário do se quer acreditar, não existe um grupo sem estrutura. Qualquer grupo de pessoas de qualquer natureza que se junte por qualquer período de tempo, para qualquer propósito, inevitavelmente se estruturará de alguma forma. A estrutura pode ser flexível, pode variar ao longo do tempo, pode distribuir tarefas, poder e recursos de forma igual ou desequilibrada sobre os membros do grupo, mas uma estrutura será formada independentemente das habilidades, personalidades ou intenções das pessoas envolvidas. O fato de os indivíduos possuírem diferentes talentos, predisposições e origens torna inevitável uma estruturação.

Mas mesmo com o aperfeiçoamento de todas as formas de comunicação formal, não há como ignorar a estrutura elitista que se forma através de canais informais de comunicação. Para Freeman (1972), há natureza inevitavelmente elitista e exclusiva das redes informais de comunicação de amigos. Uma elite se refere a um pequeno grupo de pessoas que têm poder sobre um grupo maior do qual faz parte, geralmente sem responsabilidade direta com esse grupo maior e, muitas vezes, sem seu conhecimento ou consentimento. As elites não seriam nada mais do que grupos de amigos que também participam das mesmas atividades políticas. Eles provavelmente manteriam sua amizade, estando ou não envolvidos em atividades políticas, como provavelmente estariam envolvidos em atividades políticas, mantendo ou não suas amizades, porque as elites são informais, o que não significa que sejam invisíveis.

Jentzsch (2016), um dos idealizadores da catastrófica The DAO, publicou algumas lições aprendidas com o projeto – entre elas, a falta de sistemas de governança adequados e que os canais de comunicação existentes, como o Reddit, não seriam um bom ambiente para debater a governança de uma DAO e não representariam os possuidores de tokens do projeto. No caso da The DAO, Jentzsch (2016) omite que a solução alcançada foi um exemplo de uma atuação elitista na solução do problema. Nos canais “oficiais” de comunicação da The DAO, percebe-se a ocorrência de questões informativas e de marketing, e não

debates que realmente sejam úteis para a gestão descentralizada e horizontalizada. Além disso, os canais de comunicação, como Slack, Telegram, Discord, entre outros, possuem administradores, fato que por si só cria uma hierarquia na comunicação e a possibilidade de censura. Observa-se que, quando um “admin” de grupo publica ou compartilha algum conteúdo, há um aspecto de informação oficial, e a interação dos participantes acaba sendo maior com esse comentário do que com os comentários de um participante comum.

Ainda sobre a comunicação nas DOs, elas são verdadeiras Torres de Babel. O inglês é o utilizado na maioria dos canais, mas nem todos os participantes dominam o idioma, mesmo com auxílios de tradutores digitais para ruídos de comunicação. Para facilitar a comunicação, alguns projetos criam canais específicos para alguns idiomas, além de buscar traduzir seus comunicados. Wilt (2017) alerta até também para a dificuldade de comunicação quando há utilização de termos técnicos, que nem todos dominam, mesmo sendo fluentes em inglês.

Acompanhando as dificuldades de gestão dessas modernas estruturas organizacionais, novos projetos vêm apresentando modelos de governança mais enriquecedores. Começam a surgir aprimorados meios de votações de recursos externos, como a DAO Carbonvote, um projeto comunitário dedicado a ser uma importante fonte de referência de forma quantitativa para oferecer sugestões de rumos para desenvolvedores e para a Fundação Ethereum. E os chamados processos de governança on chain, onde já são acoplados recursos de mudanças nas camadas de protocolos dos blockchains, como o Decred, onde as votações, quando alcançadas as exigências, são incorporadas automaticamente em seus protocolos[8].

E algo que pode fortalecer ainda mais as elites são os baixos quóruns de participantes nas votações das DOs. Até agora, não importam os canais, as votações tendem a ter uma participação muito baixa de eleitores. A DAO Carbonvote alcança pequenas taxas de participação de votação, irrelevantes para o tamanho total do ecossistema Ethereum[9]. Outro exemplo mais ilustrativo foi o

The DAO, no qual as propostas mais votadas nem sequer superaram os 10% de participação, nem mesmo aquelas relacionadas à segurança do próprio DAO (GÓMEZ, 2016).

Provavelmente é impossível eliminar as estruturas elitistas dos projetos das organizações descentralizadas, mas uma forma de reduzir a influência centralizada é o aumento de participação. O projeto DAOstack incorpora algumas propostas de melhorias na governança on chain para organizações descentralizadas de grande escala. Usando uma tecnologia de consenso holográfica, Matan Field, engenheiro do projeto, apresenta três propostas para a gestão distribuída.

Monetização da atenção

A atenção humana, e em particular a inteligência, é um recurso escasso. Portanto, em outras palavras, a atenção tem que ser monetizada. A aquisição de atenção coletiva em uma rede de agentes inteligentes tem que ser paga por algo valioso (FIELD, 2018).

Fortalecendo a ideia de Field de monetização da atenção de participantes da DAO, vale realizar um paralelo com as organizações tradicionais, onde, na maioria das estruturas, os decisores são os funcionários mais bem remunerados. Se uma DAO pretende possuir uma participação ativa de seus membros na gestão, seus códigos devem estar preparados para remunerar a gestão coletiva. Como é sempre visto nas ICOs de provisões de tokens para remuneração dos desenvolvedores, será um diferencial provisionar tokens também para a gestão coletiva. Tal provisão poderá aumentar a qualidade de seus membros e atrair administradores mais capacitados para o projeto. A DAOstack inclui no seu projeto níveis de reputação: as pessoas que se apresentam como melhores decisores ao longo do tempo vão aumentando sua reputação, porém possuem um recurso adicional em seus códigos para dissipar uma altíssima reputação e evitar uma centralização ao longo do tempo.

E como se propõe monetizar a atenção dos usuários? Atualmente isso é feito por meios de apostas. O proponente disponibiliza fundos a fim de que sua proposta seja aprovada; sendo positiva, ele recebe alguma remuneração. Para Mark et al. (2017), este modelo estimula o voto sim à proposta, já que ela já surge com uma aposta a sua anuência. Além disso, o proponente possui tempo ilimitado para formular e submeter suas propostas, enquanto os opositores terão o tempo da votação para apresentar os argumentos contrários à ideia.

Composicionalidade

[10]

Grande parte dos processos de governança de DAOs é baseada em votos. O grande problema percebido é que nem todos os participantes possuem o conhecimento técnico, já que a maioria das propostas de melhorias apresentadas se refere a aperfeiçoamento de códigos. Isso limita o entendimento e a participação de profissionais de outras áreas de conhecimento, deixando a organização descentralizada gerenciada somente por programadores.

Field (2018) propõe uma composição confederativa em vez de uma composição de assembleia. A confederativa pode reunir grupos mais especializados por áreas, próxima a uma departamentalização. Ele exemplifica que, em vez de 15 membros alcançarem uma maioria, a DAO poderia ser dividida em grupos de atuação, onde esses 15 membros poderiam ser divididos em três grupos e a votação de cada grupo representaria um voto para a aceitação da proposta de melhoria. Os benefícios, segundo Field, seriam:

1. As partes podem se organizar em torno de diferentes tópicos de especialização e, com confiança suficiente, o grupo maior pode delegar decisões atuais às partes menores.

2. As decisões em andamento podem ser delegadas às partes menores, por exemplo, alocando um orçamento limitado para que elas gerenciem localmente.

3. As decisões de toda a confederação são mais eficientes. Uma decisão global pode ser aprovada com o consentimento de duas partes (como dois de três

agentes de votação), o que é possível com o consentimento total de seis agentes básicos, três de cada grupo, em vez de um total de oito.

A composição de poder de votos a menores grupos, proposta pela DAOstack, pode agilizar as decisões, pois a descentralização da votação é demorada e algumas ações necessitam de atuação rápida e não podem esperar o alcance de quórum. Esse tipo de modularização é um recurso também encontrado nos projetos Aragon e Colony.

A proposta de composicionalidade defendida por esses projetos é importante para se atender à restrição cognitiva do ser humano na estrutura e na dinâmica das redes sociais. Segundo Dunbar (2014), o ser humano só seria capaz de se relacionar com 150 indivíduos, tamanho máximo para criar um senso de compromisso com uma comunidade, existindo ainda hierarquias de dedicação de tempo e esforços para manter essas relações sociais dentro desse grupo reduzido.

Caso Gore-Tex

Uma ilustração das implicações do número de Dunbar pode ser contada pela anedota da Gore-Tex, uma empresa que fabrica roupas de mergulho, botas e outros produtos e é tema de uma história famosa no mundo da sociologia. Centra-se em seu fundador, Bill Gore.

Quando a empresa foi criada, Bill a montou no seu jardim, sem muita infraestrutura. Com o crescimento do empreendimento, Bill Gore abriu uma fábrica maior, que continuou a crescer. Então, um dia, Bill entrou na sua própria fábrica e ele simplesmente não sabia quem trabalhava ali. Gore se perguntou por

que isso acontecia. Gore fez algumas contagens e percebeu que, depois de colocar muitas pessoas no mesmo prédio, as coisas na Gore-Tex simplesmente não funcionavam bem. As pessoas não conseguiam acompanhar um ao outro. Qualquer senso de comunidade se foi.

Gore percebeu que, quanto maior a empresa, as pessoas que trabalham para ela tendem a ser muito menos propensas a trabalhar duro e se ajudar mutuamente. Então Gore tomou a decisão de limitar suas fábricas a 150 funcionários. Sempre que precisavam expandir a empresa, Gore construía uma nova fábrica – às vezes, até mesmo no estacionamento ao lado. Gore percebeu que as coisas funcionavam melhor assim.

Em fábricas menores, todo mundo sabia quem era quem: quem era o gerente, quem era o contador, quem fazia os sanduíches para o almoço. Com isso, a companhia pôde ser administrada de maneira mais eficiente e o crescimento foi ainda maior.[11]

Isso provavelmente refletiria o fato de que comunidades desse porte têm um equilíbrio entre o tamanho mínimo para funcionalidade efetiva e o tamanho máximo para criar um senso de compromisso com a comunidade. O sucesso de Gore-Tex como empresa é devido à sua insistência em organizar sua produção em torno de unidades fabris de 150 indivíduos (GLADWELL, 2002, apud DUNBAR, 2014). Ao criar o que Gore se referiu como sua estrutura de gerenciamento de “rede plana”, em vez de hierárquica, o fundador do Gore-Tex foi motivado pela observação de que, em empresas muito grandes, a confiança e a cooperação rapidamente quebram quando o tamanho da organização excede cerca de 200 pessoas (DUNBAR, 2014).

Consenso holográfico

Por “consenso holográfico”, permite-se que um grupo majoritário delegue a um subgrupo uma parte menor dentro de si para tomada de decisões em nome de toda a DO, sob certas condições. Um bom consenso holográfico garante um alto grau de coerência e, portanto, uma forte correlação das decisões dos subgrupos com a vontade da grande maioria (FIELD, 2018).

A DAOstack e outros projetos defendem a criação de alguns códigos imutáveis dentro da DO, que Vitalik (2017b) nomeia de constituições digitais. Eles teriam papéis próximos a cláusulas pétreas das constituições. A imutabilidade talvez traga uma segurança psicológica, mas em projetos de recursos abertos dificilmente algum código será imutável, já que há possibilidades de forks. Talvez seja mais interessante, como nas próprias constituições, processos com exigências maiores de concordância para alterações de alguns aspectos de código e governança das DOs.

Embora ainda tenham crescido projetos e estudos sobre a governança descentralizada, percebe-se que a maioria dos projetos de DAOs e DApps não atenta para a gestão. Essas aplicações para a governança descentralizada começam a nascer mais fortes em 2018. A grande maioria enfatiza as aplicações (tarefas) e não busca aperfeiçoar as práticas de gestão descentralizada de escala, talvez por ser um novo tipo de governança, com ferramentas de gestão em construção que ainda oferecem pouco benchmarking. O estudo de Wilt (2017) analisa a DigixDAO em comparação com o modelo VSM (Viable System Model), de Beer. No momento da análise de Wilt, a DigixDAO não poderia ser considerada uma organização viável porque não tinha atividades primárias. Talvez esse resultado pudesse ter sido alterado se fosse realizada uma nova análise, pois a plataforma Digix e os contratos inteligentes de governança ainda não estavam finalizados. Esse é um dos motivos pelos quais este livro utiliza o substantivo “projeto” antes de referenciar a alguma DO. Os projetos que

oferecem recursos de governança têm por objetivo facilitar essa nova forma organizacional e social que pode atuar dentro ou fora do criptoespaço. O próprio projeto DAOstack tem por objetivo explícito se tornar um Wordpress das DAOs, oferecendo simplicidade na gestão descentralizada em grande escala.

Em 1988, Drucker escreveu o artigo “The Coming of the New Organization”, que já explorava os impactos da tecnologia e a descentralização das organizações, que seriam focadas cada vez mais em especialização, como as estruturas hospitalares e orquestras sinfônicas. Drucker mencionava como desafio as sucessões e a troca de conhecimento nessas organizações a longo prazo. Drucker compreendia como um desafio gerencial futuro o trabalho de construir a organização baseada na informação (esse futuro chegou). A organização baseada na informação também colocará seus próprios problemas especiais de gerenciamento, e Drucker (1988) via como particularmente crítico:

1. Desenvolver recompensas, reconhecimento e oportunidades de carreira para especialistas.

2. Criar visão unificada em uma organização de especialistas.

3. Elaborar a estrutura de gestão para uma organização de forças-tarefas.

4. Garantir o fornecimento, a preparação e o teste de pessoas da alta administração.

Com exceção do item 4 (aparentemente, não é aceita pela comunidade das DOs uma “alta administração” centralizada), os demais problemas apresentados por Drucker (1988) parecem continuar sendo um desafio nas organização

descentralizadas, ainda mais em uma descentralização de grande escala, como as organizações mencionadas neste livro.

Pessoas

Como uma DAO é aberta, as pessoas em uma DAO se fundem entre proprietários, clientes, usuários e investidores. Tentando amenizar essa ambiguidade e possíveis conflitos de interesses de seus participantes, a DigixDAO, uma DAO com proposta de digitalização e comercialização de ativos financeiros, faz uma diferenciação entre os atuais 385 possuidores dos tokens de votos e os possuidores de seus tokens financeiros DGB. Para participar da governança da empresa, os possuidores do token DGB necessitam manter durante um trimestre seus tokens congelados em uma carteira DigixDAO, estratégia argumentada pela mecânica da teoria dos jogos[12].

Mesmo com a evolução na governança on chain, as formas de monetização dos propositores de ações de gestão ou melhorias de DAOs ainda são mais atrativas financeiramente aos desenvolvedores que ao restante dos participantes. Assim, há concentração, muitas vezes, de uma elite técnica, e isso parece ser uma fraqueza, pois até mesmo um bom programador de fora da elite com uma boa ideia poderia ter mais interesse em fazer um fork e criar uma nova DO a oferecer uma melhoria para a organização da qual participa. É sempre bom lembrar que Raymond (1997) afirma que “os bons programadores sabem o que escrever. Os grandes sabem o que reescrever (e reusar)”. Lembre-se de que os códigos das DOs são abertos e acessíveis a todos. Possibilitar remuneração a participantes que ofereçam boas contribuições às DAOs é uma forma de manter a união, evitar forks e até mesmo reter talentos no projeto, coisa pouquíssimo abordada em projetos descentralizados. Comumente se vê a disponibilidade de vagas para desenvolvedores nos projetos DOs e percebe-se que a atração de participantes de outras especialidades de conhecimento são praticamente terceirizadas, baseadas em relações de cooperação.

Visando atrair participantes com outras especialidades para os seus ecossistemas, a Fundação NEM oferece a possibilidade de monetização de pessoas externas à

Fundação através de ações de marketing que promovam o projeto em notícias e eventos, além de subsidiar pesquisas científicas junto à plataforma NEM[13]. A Dash possui um canal aberto para recebimento de propostas que agreguem valor à comunidade. O proponente participa de votações de financiamento da comunidade a projetos de patrocínio de eventos e ações educacionais. Na Dash a própria comunidade pode votar no valor do salário da equipe de desenvolvedores Dash[14]. Na DigixDAO a premissa para aprovação de um projeto de financiamento é simples: há benefícios claros para os detentores de tokens DGD e a ETH está liberada para o referido projeto. Quanto mais direta a relação, melhor (WILT, 2017).

Para que os projetos obtenham fundos de financiamento de DOs, eles devem demonstrar claramente como seu plano pode ajudar no crescimento e na utilidade do ecossistema dos tokens das DOs. O projeto Aragon, como a DigixDAO, exige que sejam prestadas contas e sejam feitos relatórios de evolução dos projetos, além de monitoramento para a manutenção dos financiamentos dos projetos. “Por que alguém ganharia uma parte da recompensa se não estivesse fazendo nada para tornar o DAO um lugar melhor?”, questionam os criadores da DigixDAO (WILT, 2017).

Mesmo uma DApp, com uma hierarquia e uma equipe fechadas no projeto, deve contar com o apoio de pessoas externas ao núcleo administrativo. Essas participações são estimuladas com concursos de desenvolvimento e aperfeiçoamento de seus códigos, aplicações de pessoas ou empresas que são desenvolvidas dentro de suas plataformas e constituição de embaixadores em diversos países. Usando o benefício de possuir seu ecossistema e sua própria moeda, torna-se mais fácil remunerar os participantes de diversos lugares do mundo com pagamento de seus próprios tokens. Uma DO é um ecossistema, e não somente um produto.

E como se trata de um ecossistema e de uma diversidade de participantes, há uma pressão externa muito maior e mais ativa que interfere na gestão das organizações descentralizadas se comparadas às tradicionais S/A. Charles Lee,

possivelmente o mais notório criador da litecoin, estava sendo acusado de usar suas publicações nas redes sociais para manipular o preço de mercado da litecoin. Claro que, como criador do projeto, ele possuía uma enorme quantidade de litecoin em sua carteira. Para manter a credibilidade do projeto como realmente uma DO, Lee decidiu vender e doar todas as suas litecoins, ficando somente com as que considerava ter valor histórico. Por que isso? Porque em uma DO a centralização em torno de um criador da organização já gera questionamentos e graves acusações[15].

Exemplo oposto ocorreu com a Dogecoin. A Dogecoin foi criada por Jackson - Palmer, que se retirou do projeto em 2015. Quando viu o valor total de mercado de seu projeto alcançar mais de 2 bilhões de dólares em 2017, Palmer ficou surpreso, pois seu projeto foi inspirado em um meme da internet e desenvolvido mais por questões de aprendizado do que por interesses financeiros. Para ele o crescimento da Dogecoin demonstraria o alto nível especulativo e a bolha que se criou no criptomercado (PALMER, 2018). Para mim, Palmer não percebeu a real limitação de um criador nas organizações descentralizadas.

O combate à centralização e à personificação de projetos de organizações descentralizadas ocorre a todo momento em uma organização descentralizada, principalmente nas autônomas. O papel dos criadores se resume somente à criação, e os rumos que a DO irá tomar depende somente da comunidade que atua nela. Assim como Santos Dumont teria se suicidado após ver sua invenção fora de controle, sendo utilizada como arma de guerra, os criadores de uma DAO não são responsáveis pelos rumos que a organização tomará[16].

Drucker (1988), em seu estudo sobre a descentralização das organizações tradicionais, ainda expunha o interesse das pessoas no crescimento horizontal e não vertical de carreiras, apontando como problemas centrais valores, estrutura e comportamento. Como via Schumpeter, no início do século XX, o alcance do sucesso industrial ou comercial ainda seria, para o homem da época, a melhor maneira possível de se aproximar da nobreza medieval. A fascinação seria ainda mais forte nas pessoas que não teriam nenhuma outra chance de atingir distinção

social. A sensação de poder e independência é, em grande parte, ilusória. Há então o desejo de conquistar, o impulso de lutar, para provar-se superior aos outros, de ter sucesso em nome não de seus frutos, mas do próprio sucesso (SCHUMPETER, 1961). Tal carência individual e a busca por supri-la com uma imagem de sucesso profissional na figura de engravatados executivos de grandes empresas são oportunidades pouco oferecidas nas DOs.

Mougayar (2016) afirma que as DAOs nascem de forma participativa, colaborativa e cooperativa. Esses são os perfis pessoais necessários para criar um ecossistema descentralizado.

E a mescla entre as pessoas dessas organizações com o ambiente nos leva à próxima variável: ambiente.

Capítulo 6. Fatores Extrínsecos

“Com tanta riqueza por aí, onde é que está?

Cadê sua fração?

Até quando esperar a plebe ajoelhar

esperando a ajuda de Deus?”

(Seabra, André X e Worthmann, “Até Quando Esperar”)

Como vimos, seriam inúmeras as variáveis externas de uma organização, mas neste capítulo destacaremos alguns dos principais aspectos extrínsecos das DOs atualmente.

Limitações à descentralização

Como estamos falando de organizações descentralizadas distribuídas a nível mundial, pode-se dizer que o ambiente virtual é o ambiente interno dessas organizações, e seu protocolo e agente autônomo sempre estarão expostos a ataques mal-intencionados. Uma falha de comunicação em uma rede distribuída não afeta seu funcionamento, mas uma falha no protocolo afeta diretamente o funcionamento das organizações descentralizadas.

Buscando reconhecer as limitações de alcance de uma organização descentralizada, deve-se refletir onde os nodos e participantes da DO estarão instalados. O ambiente tarefa pode se limitar às exigências tecnológicas de cada local do mundo. Como exemplo, é possível pensar em uma aplicação descentralizada que exija uma internet de velocidade 5G. Tal velocidade de internet ainda é restrita a poucos países, logo, o ambiente tarefa dessa organização será limitado aos locais onde essa tecnologia está disponível. O próprio acesso à internet é desigual no mundo.

A redução do ambiente tarefa também poderá ocorrer pelas legislações locais e restrições de acesso à internet em alguns países, embora seja importante ressaltar que muitos protocolos e aplicações descentralizadas podem ser acessados por outros meios fora de alcances governamentais.

Influência das camadas anteriores

Embora seja uma variável externa, os protocolos complementares incorporados aos protocolos das organizações descentralizadas afetam diretamente seu ambiente tarefa.

E a decisão da Storj em alterar a plataforma que a hospedava ilustra a influência das plataformas e camadas anteriores nas DOs. A Storj estava hospedada dentro da plataforma Counterparty, que, por sua vez, era um sidechain situado no protocolo do bitcoin. A Storj estaria em uma terceira camada, onde as outras duas anteriores afetavam diretamente a qualidade e os valores de seus serviços. O que motivou a migração da Storj, em 2017, foi a lentidão e as altas taxas cobradas nas transações do bitcoin. A falta de atualizações e a dificuldade de interface das carteiras da Counterparty, além das poucas aplicações baseadas nesse ecossistema, exigiam que a própria Storj financiasse as melhorias na plataforma Counterparty. A migração para o protocolo do blockchain do Ethereum ocorreu por ser um ecossistema mais ativo, onde novas atualizações são constantes, a velocidade das confirmações das transações é mais rápida que as do bitcoin e as taxas, mais baratas, além da utilização do padrão de token ERC20, que obrigou a Storj a trocar os tokens StorjcoinX dos parceiros, utilizados na Counterparty, para o novo padrão de token Storj (WILKINSON, 2017).

Esse tipo de migração se acentuou no ano de 2018. Após a Storj, é possível - encontrar outras migrações de plataforma das organizações descentralizadas. Em 2018 as DApps de conteúdo WooWoo e Narrative migraram o desenvolvimento de seus projetos para a plataforma NEO, mesmo com sua ICO ocorrendo na plataforma Ethereum (O’NEILL, 2017). Eles alegam que a tecnologia NEO é superior em escalabilidade das transações, possuem taxas mais baratas e, no caso da WooWoo, eles veem o NEO como um ajuste melhor não apenas tecnologicamente, mas moralmente, e que são projetos que compartilham os

mesmos valores (JOHNSTON, 2018). Com argumentos semelhantes, a Tutellus, DApp da área educacional, migrou da cadeia da Ethereum para a cadeia de blocos NEM (HONTORIA, 2018).

O surgimento de novos blockchains e a incorporação de novas aplicações nas plataformas já existentes tendem a tornar as migrações das organizações descentralizadas mais constantes no futuro.

Ambiente legal

Os aspectos legais dos criptoativos são embrionários. Assim como abordado nas ICOs, as questões legais não possuem um consenso entre os governos. Em 2013 a Tailândia foi o primeiro país a proibir o uso e a comercialização de bitcoins. Posteriormente reviu sua posição e permitiu o uso de criptoativos por seus cidadãos (PALMER, 2014).

Da mesma forma que a Tailândia, outros países possuem posturas contraditórias, como a Estônia, que apoiava a adoção de criptomoedas – em abril de 2017 foi até mesmo noticiado que o governo teria planos de criação de um token estatal - (SUNDARARAJAN, 2017). No entanto, por pressão da União Europeia, que só admite o euro como moeda corrente, o que ocorreu foi um aumento na restrição de uso de criptoativos no país[1]. Algo semelhante ocorreu na Coreia do Sul, que até o fim de 2017 era o maior mercado do token ETH e possuía uma legislação amigável aos criptoativos, mas no início do ano foi responsável por uma forte queda no criptomercado devido a regras mais duras relativas à atuação das corretoras no país e à discussão de proibições de ICOs no território coreano (RAMIREZ, 2018).

Equador, Bangladesh, Bolívia, Argélia, Camboja e Nepal proíbem por completo o uso de criptomoedas em seus territórios; entretanto, é fácil encontrar vendedores de bitcoins nesses países, em sites como localbitcoins, que possibilita encontrar comerciantes e realizar transações peer-to-peer em diversos países do mundo. Em países islâmicos como Egito, Turquia, Arábia Saudita e outros, o uso de criptomoeda seria um haraam, atitude contrária aos ensinamentos islâmicos (DIAA, 2018).

A grande maioria dos países até o momento não possui legislações específicas. O

Banco Central Finlandês publicou artigo com uma postura de não interferência no desenvolvimento da tecnologia, reconhecendo o bitcoin como um sistema econômico e revolucionário e que, portanto, mereceria a atenção e o escrutínio de economistas, mesmo que não fosse funcional, mas sua aparente funcionalidade e utilidade devem incentivar ainda mais os economistas a estudar essa maravilhosa estrutura (HUBERMAN et al., 2017).

A mesma postura se encontra no artigo “Are Bitcoin and other crypto-assets money?” (SÖDERBERG, 2018), que defende a atuação do estado na regulamentação dos criptoativos. Mesmo não considerando o bitcoin uma moeda, o autor acredita que só a segurança jurídica apoiará a tecnologia. Söderberg (2018) defende mais debates sobre o tema, pois “uma nova tecnologia não surge no vácuo, mas está ligada e pressupõe um contexto social e legal. Isso significa que uma discussão contínua sobre os recursos de criptografia deve ser ampliada para incluir também esses aspectos”.

Esses debates são quase inexistentes nos órgãos regulamentadores, pois é praticamente uniforme o discurso contra a adoção de criptoativos. Os argumentos contrários à sua utilização são: financia o crime e o terrorismo, estimula a lavagem de dinheiro, não há órgão emissor nem garantidor do ativo oficial. Até meados de 2018, a maioria das manifestações governamentais acerca da regulamentação do uso de criptoativos é feita pelos bancos centrais e as entidades de supervisão financeiras dos países, e não por seus legisladores. Assim, o funcionamento do criptomercado atua amparado pelo princípio da legalidade, em seu aspecto básico do direito civil, que diz ao particular que “tudo aquilo que não é proibido é permitido”.

A verdade é que, para uma DAO, é irrelevante se submeter a uma jurisdição. O crescimento e a popularização do bitcoin ocorreram sem que estivesse em nenhuma jurisdição, com base somente nas pessoas. A DigixDAO, após anos de seu nascimento, pensa em se registrar em Cingapura para facilitar sua interação com organizações constituídas de forma tradicional, colocando em jogo sua essência como DAO (WILT, 2017).

Corretoras de criptoativos

O valor monetário dos criptoativos é estipulado junto ao mercado e às corretoras de criptoativos (exchanges). Estas possuem papel fundamental no ecossistema das DOs para referenciação de valores com as moedas fiats. Em abril de 2018 existiam mais de dez mil corretoras pelo mundo, e cada exchange representa um mercado específico. Essa diversidade é importante para aumentar a capilaridade de participantes e a liquidez do criptoativo.

O mercado de ações e a centralização das bolsas de valores permitem aos grandes investidores (“baleias”) mais facilidade na manipulação do ativo naquele mercado. Claro que no caso dos criptoativos isso é factível; dessa forma, um token passará maior credibilidade estando à venda em diversas corretoras.

É comum encontrar diferenças de valores dos criptoativos entre uma corretora e outra. Essa variação gera a oportunidade de arbitragem financeira. Algumas empresas oferecem serviços que exploram as oportunidades geradas por essas variações. Atlas Quantum e Arbtrade são empresas no Brasil que exploram as oportunidades de arbitragem. No mundo encontram-se Zenbot e HaasBot. E ainda existem diversos bots disponíveis no Github que permitem arbitragem automática, como Dealer Bitcoin, Merlo Black, Melro-Black, entre outros. A arbitragem traz o benefício de ajudar a diminuir a volatilidade do mercado de criptoativos.

O uso de bots de investimento no mercado de ações é comum. Em 2010 houve um flash-crash: em vinte minutos o índice Dow Jones caiu 9% devido a um pequeno comerciante londrino que conseguiu manipular os bots adicionando diversas ordens de venda a preço baixo e as cancelando. Logo em seguida ele comprava as ações com valores mais baixos ainda, pois os algoritmos do

mercado reconheciam aquelas disparidades como uma queda no mercado (LEVINE, 2015).

Segundo Shuoji, 80% das transações de bitcoin são realizadas por bots[2]. Mas os mercados de criptomoedas são muito mais voláteis e difíceis de prever do que a bolsa de valores. Eles também são mais influenciados por eventos que os bots não podem analisar, como o anúncio de um novo regulamento do governo na China. A capacidade dos hackers invadirem as trocas ou mesmo alterar o código usado pelos bots oferece outro nível de risco que os traders tradicionais geralmente não precisam considerar. Portanto, a ascensão de bots talvez traga alguma estabilidade aos mercados de criptomoedas, podendo agir para interromper os flash crashes nos mercados em vez de apenas causá-los (COMM, 2017).

Não só os bots de arbitragem são vítimas de hackers. As corretoras de criptomoedas já foram vítimas de inúmeros ataques que causaram perdas aos seus usuários e provocaram quedas no mercado como um todo. Em 2014, desapareceram da corretora japonesa Mt. Gox mais de 850 mil bitcoins, que somavam um valor de 450 milhões de dólares, cotação da época, o que causou uma grande queda no mercado. Em 2016, na Bitfinex foram roubados 120.000 bitcoins[3]. Em 2018 a corretora Coinchek também foi alvo de um roubo da criptomoeda XEN no valor de 400 milhões de dólares[4].

A descentralização do ativo é benéfica aos investidores, mas há outros tipos de fraudes que surgem sem necessariamente serem causadas por hackers. Como forma de autorregulação do criptomercado, algumas corretoras excluem de sua lista de tokens aqueles que possam apresentar manipulação de preço. A Bitrex, em 2018, excluiu 80 tokens de sua lista ao ser alertada pela Business Insider. A Business Insider observou esquemas de pump-and-dump para as criptomoedas UBQ, VCash, Chill Coin, Magi Coin e Indorse na Bittrex e na Yobit. Os esquemas muitas vezes eram organizados por grupos informais de comunicações no Telegram, onde os investidores criavam estratégias para manipular o mercado (WILLIAN-GRUT, 2017). Porém, há também a possibilidade de a própria

corretora maquiar os volumes de seu próprio booking. Ribes (2018) apresentou um estudo onde concluiu que três bilhões do volume diário de transações seriam inexistentes e os próprios responsáveis seriam as próprias corretoras, que adulterariam seus volumes para atrair investidores.

Corretoras descentralizadas (DEX)

Além das inúmeras questões de insegurança apresentadas nas corretoras centralizadas, inserir um criptoativo nas principais exchanges é oneroso. Entre fevereiro e março de 2017, apenas oito corretoras concentravam 75% das trocas de bitcoins nas exchanges no mundo (HILEMAN; RAUCHS, 2017, p. 31). Pela alta liquidez que essas corretoras oferecem, é atraente para qualquer DO inserir seus tokens nesses mercados; porém, os valores cobrados para inserir novos tokens em uma corretora podem variar de 1 a 3 milhões de dólares (NEXT AUTONOMOUS, 2018).

Para atrair novos projetos para seus blockchains, Waves, Stellar, BitShares e Komodo oferecem suas próprias corretoras para a comercialização de tokens criados em seu ecossistema. Além de ajudar na liquidez dos tokens novos, hospedados nas plataformas, as corretoras descentralizadas (DEX) são mais seguras em relação aos ataques de hackers, pois as únicas pessoas que têm acesso às chaves criptografadas dos usuários são os próprios usuários. Trata-se do mesmo nível de segurança usado nas wallets próprias das criptomoedas.

As DEXs estão ganhando força no mercado. Até mesmo a Binance, uma das maiores corretoras de criptoativos do mundo, já está desenvolvendo sua própria DEX[5]. Por se tratar de novas opções de trocas, as exchanges descentralizadas (DEX) ainda possuem baixo volume de negociação, mas suas transações atômicas retornam à proposta inicial de Satoshi Nakamoto e à essencial tecnologia blockhain, que priorizam as transações P2P e excluem a necessidade de um intermediário como nas exchanges centralizadas (LUU, 2017). Entre as corretoras descentralizadas mais populares em 2018 estão: IDEX, WEX DEX, OasisDex e Bisq (KHATWANI, 2018).

Criptoeconomia

A teoria econômica de Schumpeter foi pioneira em considerar as inovações um aspecto endógeno ao sistema econômico, portanto as alterações econômicas são resultado das interações e/ou impactos das inovações tecnológicas no sistema econômico (TAVARES; KRETZER; MEDEIROS, 2005). Schumpeter (1961) afirma que as “mudanças não constituem nem um processo circular nem movimentos pendulares em torno de um centro”. A tecnologia blockchain apresenta propriedades econômicas notáveis e potencialmente revolucionárias, construindo redes financeiras globais, sendo usada para criar organizações autônomas distribuídas, permitindo contratos autoexecutáveis e organizando indivíduos e comunidades em redes de maneira nunca antes vista na história da humanidade[6].

Algumas suposições sobre a dinâmica econômica do criptomercado começam a surgir. Cermak (2017) considerou o bitcoin um ativo risk-off semelhante ao ouro. Em sua pesquisa ele argumenta que a limitação de valor do governo chinês a remessas internacionais teria influenciado o aumento do valor do bitcoin, assim como as inseguranças econômicas proporcionadas pelo Brexit (saída do Reino Unido da União Europeia).

Os resultados de Cermak nos remete a acontecimentos históricos. As criptomoedas oferecem segurança aos cidadãos e dificultam o confisco de seus bens pelo governo. Em 1933, o governo americano confiscou os depósitos de ouro de seus cidadãos (SALSMAN, 2011). Em 1990, o governo brasileiro confiscou os depósitos bancários no famigerado Plano Collor (VILLELA, 2015).

No início deste século, na Argentina, o governo De La Rua impôs as mesmas restrições aos seus habitantes (KIDD, 2011).

A adoção por criptoativos pode ocorrer por crises inflacionárias, como a da Venezuela de 2017. A inflação no país superou 500% e uma alternativa para os venezuelanos diluírem a desvalorização de seus recursos financeiros foi a compra de bitcoins (FRANCO, 2017). O fato é interessante para questionar as afirmações do presidente do Bank of England, Mark Carney, em 2018, de que as criptomoedas não funcionam como reserva de valor. A afirmação é válida havendo um comparativo: reserva de valor em relação a quê? No caso da Venezuela, em relação à moeda local, bolívar. O bitcoin se apresenta como uma reserva de valor melhor que a moeda fiat local (MILLIKEN, 2018).

Continuando uma análise corroborativa da visão de Cermak (2017), que os criptoativos se apresentam como um risk-off por instabilidades políticas, no Zimbábue, devido ao golpe militar ocorrido em novembro de 2017, houve um aumento do valor local do bitcoin, pois a população, em busca uma alternativa monetária devido à instabilidade política local, comprava o bitcoin (ALTHAUSER, 2017). Por fim, os criptoativos podem ser usados por empresas e países para driblar os embargos comerciais impostos por outros estados ou pela ONU (TWEED, 2018). Ao considerar os criptos um ativo risk-off, diversos aspectos políticos do sistema econômico centralizado podem se tornar obsoletos por conta da nova configuração econômica distribuída. Imaginar países que sofrem tragédias naturais ou, indo ao extremo, guerras que impossibilitem as pessoas de usar o sistema financeiro tradicional, o criptomercado se apresenta como uma alternativa a ser considerada para preservação de patrimônio.

Agora, voltando ao ambiente do criptomercado, a influência do preço do bitcoin em relação ao demais criptoativos ainda é forte. É fácil observar uma correlação positiva entre as variações de valores do bitcoin e os valores dos tokens das DOs em relação ao preço do dólar. O coeficiente de correlação de Pearson é um número entre 1 e -1 e verifica o nível de associação entre duas variáveis. Quanto mais próximo de 1, maior a associação direta entre as variáveis. Isto é, quando uma variável aumenta, a outra também aumentará; e quando uma variável diminuir, a outra também diminuirá. No caso de um coeficiente negativo, enquanto uma variável aumenta, a outra diminui (SWEENEY et al., 2013). No

caso do bitcoin em relação aos tokens analisados, o coeficiente de correlação médio é de 0,79, podendo ser interpretado como uma correlação forte.

Tabela 3. Índice de correlação do bitcoin x tokens. Fonte: sifrdata. Cryptocurrency Correlation Matrix. Intervalo de dados de 08 de março a 08 de junho de 2018.

Índice de correlação bitcoin			
Bitcoin	1	NEM	0,72
Ethereum	0,88	Ethereum Clasic	0,8
Ripple	0,85	Zcash	0,71
Bitcoin Cash	0,75	Lisk	0,82
Litecoin	0,86	SiaCoin	0,75
Stellar	0,8	Augur	0,54
Monero	0,81	Factom	0,8
DASH	0,84	Nxt	0,78

Algumas suposições podem ser levantadas para esse fenômeno. A primeira seria a predominância do bitcoin na capitalização total do criptomercado. O bitcoin, mesmo com uma tendência de queda, ainda representa aproximadamente 40% do mercado total de criptoativos, em meados de 2018[7].

A segunda suposição seria a capilaridade do bitcoin. Em pesquisa de 2017, todas as corretoras comercializavam bitcoins (HILEMAN; RAUCHS, 2017). Provavelmente, a grande participação do bitcoin no criptomercado facilitaria o acesso de novos usuários às exchanges, aumentando a liquidez do mercado específico. Tal influência do bitcoin no criptomercado faz com que haja duas cotações dos criptoativos no CoinmarketCap: uma em dólar e outra em bitcoins. Devido à alta correlação mostrada entre o valor em dólar do bitcoin e dos outros criptoativos, o ganho real para os investidores seria quando há valorização do criptoativo em relação ao bitcoin.

Entre 27 de março e 27 abril de 2018, o volume financeiro de transações de bitcoins representou 34% do total do criptomercado[8], percentual inferior ao encontrado na pesquisa de julho de 2017, onde o valor encontrado por Pisa e Juden (2017) era de 47%. No período entre as duas pesquisas, o número de criptoativos no mercado praticamente dobrou e as corretoras aumentaram o número de criptomoedas em seus portfólios, o que poderia justificar a queda.

A dissociação do preço dos tokens do valor do bitcoin seria benéfica, pois uma queda brusca no valor do bitcoin pode causar prejuízos nas atividades de indivíduos que colaboram com outras DOs. Os custos de participação em DApps de crowdsource como a Golem e Storj estão mais atrelados ao valor da energia, da internet e dos hardwares necessários para o serviço. Outro exemplo é a rede social Steemit, um ambiente de troca de experiências dos participantes onde é mais fácil encontrar textos sobre a utilidade das novas formas de monetização proporcionada pelas DOs e verificar como a volatilidade do bitcoin afeta todo o ecossistema de criptoativos. Uma usuária, em janeiro de 2018, postou um texto

que dizia que os ganhos com sua participação na rede social, em tokens Steemit, estavam ajudando na reforma de sua casa (MULLER, 2018). Após a forte queda do preço do bitcoin a partir de fevereiro do mesmo ano, perguntei a ela, pelo chat Discord, sobre o andamento da reforma. A resposta obtida foi que a reforma está parada por causa da queda do mercado.

Ocorre que a plataforma Steem cresce constantemente em relação ao número dos usuários. Novas aplicações como D.tube, similar ao YouTube, Steepshot, similar ao Instagram, estão atraindo usuários para aplicações da rede Steem[9]. Logo, seria plausível acreditar que o crescimento do ecossistema da Steem aumentaria o valor de seu token, mas devido à forte queda do bitcoin, o valor das recompensas aos usuários despencou.

A influência do valor do bitcoin nos outros criptoativos também afeta os fundos arrecadados das ICOs, pois a grande maioria mantém os fundos em criptomoedas, e não em contas em banco e moedas fiats. Os fundos estão principalmente em ETH, token da plataforma Ethereum, que hospeda o maior número de ICOs em 2018. Essa volatilidade abre portas para intermediários como os crypto funds, que oferecem serviço de administração dos fundsraisers das ICOs, como o australiano Ibagroup.

Uma saída para mitigar a volatilidade do mercado seria utilizar o token Tether (USDT), que oferece paridade com o dólar. Mas o token USDT é polêmico. A falta de transparência com os fundos garantidores da paridade sempre é notícia na mídia especializada, sendo alvo de investigação de autoridades monetárias americanas (ROSSOW, 2018). Em abril de 2018, a moeda estável Tether era a segunda maior em volume de transação, com 74 bilhões de dólares, representando aproximadamente 14% do volume negociado. Nas corretoras, os traders precisam desesperadamente de uma criptomoeda estável em termos de preço para que possam usar como reserva de valor quando esperam por quedas no criptomercado. Os traders podem preferir aguardar as quedas de mercado com Tether, porque converter o valor em moedas fiats constitui um evento tributável em diversos países (AL-NAJI et al., 2017).

Além de ser uma necessidade do mercado, a alta participação da Tether no mercado fez surgir, em 2018, diversas stablecoins, moedas que buscam criar uma paridade com algum ativo e funcionar como reserva de valor. A TrueUSD, token já listado na corretora Bittrex, diz possuir parceria com empresas fiduciárias licenciadas e bancos para manter com segurança os fundos que apoiam os tokens TrueUSD. Dessa forma, como a Tether, a TrueUSD também incorpora um intermediário no criptoespaço para garantir a paridade do token em relação aos fundos.

Projetos como Basis e MakerDAO acreditam que o uso de algoritmos que controlem o número de oferta e demanda pode estabilizar o valor do token. A questão é que o algoritmo só funcionará se houver comprador – se ninguém estiver disposto a pagar 1 dólar por esses tokens, o valor será nulo.

Capítulo 7. Rede e Propósito

“Eu não quero mais mentir

Usar espinhos que só causam dor

Eu não enxergo mais o inferno que me atraiu

Dos cegos do castelo me despeço

E vou a pé até encontrar

Um caminho, o lugar

Pro que eu sou”

(Nando Reis, “Cegos do Castelo”)

A rede é o lastro

Adam Smith escreve, em 1776, o clássico livro “A Riqueza das Nações”, crendo que as nações seriam capazes de se autorregular economicamente promovendo a própria distribuição de riquezas. Havia uma restrição espacial entre o comércio entre as nações. Para Smith (1776), haveria pouco ou nenhum comércio de qualquer espécie entre as distantes regiões do mundo. No início dos anos 1980, com a comercialização dos sistemas precursores da internet, Metcalfe propôs que o cálculo de valor de um sistema de comunicação cresce na razão do quadrado do número de usuários do sistema. Então se uma rede é muito pequena, seu custo excede seu valor; mas se uma rede se tornar grande o suficiente para atingir massa crítica, então o céu seria o limite (METCALFE, 2013). Logo, surge a estratégia das empresas de comunicação de buscar a adesão de muitos participantes em suas redes de sistemas e aplicativos de comunicações de internet para que se tornem viáveis e lucrativas. Já em 2006, com a consolidação da internet e sua grande adesão mundial, Benkler observa a facilidade de conectar as pessoas e percebe que os altos custos de capital, que antes eram um pré-requisito para coletar, trabalhar e divulgar informações, conhecimento e cultura, foram diluídos entre seus usuários. Admirado com a redução das barreiras de entrada nos canais on-line e a retirada da hegemonia dos meios de comunicação e grandes corporações, e o surgimento de redes colaborativas de conhecimentos como as wikis, Benkler escreve o livro “The Wealth of Networks”.

Com a tecnologia blockchain, essas redes possuem sua unidade de valor própria – dessa forma, muitos creem que está nascendo a Internet do Valor. Para Shermin (2017), o sucesso relativo do bitcoin desafia a noção de que os governos nacionais são uma condição necessária para estabelecer sistemas monetários funcionais. Aplicando o mesmo princípio a outros serviços tradicionalmente fornecidos pelos governos, BitNation propõe a noção de DVBN – Decentralized Virtual Borderless Nation (DVBN). OS DVBNs são simplesmente DAOs que coordenam a provisão de (tradicionais) serviços

governamentais, como registros de nascimentos, casamentos e mortes através de um blockchain e o potencial de programar leis, regras e regulamentos em um contrato inteligente no topo de um blockchain, desafiando o papel tradicional de burocratas, políticos e executivos.

O dólar americano deixou de ser lastreado em 1971. Qual seria o lastro do dólar atualmente? (GHIZONI, 1971). O lastro do dólar hoje poderia ser considerado a economia americana e a aceitação mundial dessa moeda. As moedas são um tipo de bem que regularmente é aceito por vendedores em troca de bens e serviços. As moedas fiats são consideradas de “curso legal” (MANKIW, 2009, p. 628). Não há que se falar em lastro, trata-se somente de uma imposição legal de um estado para sua aceitação em seu território.

O token de uma DO deve ter aceitação e deve possuir uma gama de usuários, por isso é fácil encontrar ações de marketing de DOs que distribuem tokens, como a realizada pela plataforma Stellar, em abril de 2018, em parceria com a corretora brasileira CryptoMarket (GUSSON, 2018).

O poder da rede pode ser mais bem entendido analisando o artigo de Peck “Let’s destroy Bitcoin” (2018), que sugere três formas de acabar com o bitcoin.

1. Aquisição do governo

A primeira seria a criação de uma criptomoeda estatal onde os bancos do sistema financeiro seriam os validadores e os criadores de carteiras dos usuários. Segundo o autor, a criptomoeda estatal teria ainda o benefício de cobrar impostos diretamente das carteiras dos usuários.

A proposta de Peck não difere em nada do dólar de hoje, que se baseia na imposição de uma moeda de curso legal e lastreada na aceitação dos bancos e na consolidada amplitude do sistema financeiro americano. Ignora por completo a crise de confiança nas instituições e ainda reduz a rede de usuários do dólar no mundo, já que há países que utilizam o dólar como moeda oficial, além de outras milhões de pessoas que possuem dólares e nunca pisaram nos Estados Unidos. Então qual seria o interesse dessas pessoas de ter descontados impostos diretamente de suas carteiras pelo governo americano e não utilizar os serviços públicos daquele país?

2. Ataque furtivo do Facebook

A segunda proposta é uma grande rede social, como o Facebook, que criasse sua própria moeda, assim como o Telegram está fazendo com o token Gram. A nova criptomoeda proporcionaria uma penetração maior e quase que imediata em um mercado, tendo um alto nível de aceitação e utilidade. Além disso, a "Facebookcoin" poderia remunerar os usuários com suas postagens e participações na rede.

Peck reconhece a riqueza da rede nesse caso e, claro, que uma moeda criada pelo Facebook poderia torná-la maior que o bitcoin rapidamente. O que Peck ignora é o fato de o Facebook ser uma empresa com acionistas que visam ao lucro. Como convencer os acionistas do Facebook a abrir mão de seus lucros para distribuí-los na rede de usuários? Como já dito, redes sociais como Steem, Akasha e Nexus já fazem isso, mas nunca possuíram acionistas.

3. Tornar o bitcoin irrelevante

A terceira "novidade" que é apresentada por Peck, que poderia acabar com o bitcoin, seria estimular grandes corporações a criar seus próprios tokens. Cita o

exemplo da Kodak, mas ignora que o projeto de tokens Kodak se aproxima de um grande scam e foi refutado pela comunidade de criptomoedas por diversos motivos, como não possuir uma equipe de desenvolvedores confiáveis, um white paper fraco e não oferecer real utilidade. O caso do token Kodak foi considerado uma atitude desesperada de uma empresa à beira da falência em busca de novas formas de sobreviver em um novo mundo (MAC, 2018).

Em nenhum momento este livro apresentou o bitcoin único e soberano. Foram apresentadas diversas fraquezas da plataforma bitcoin e explanadas inúmeras inovações de outros projetos do criptomercado que claramente poderão retirar a liderança do bitcoin do mercado de diversas formas, mas claro que todas só seriam eficazes com o aumento de sua aceitação, e essa é a única concordância com o artigo de Peck. Uma rede maior pode tornar um token mais atrativo em relação à sua liquidez e utilidade. Essa competitividade entre os tokens se aproxima a antiga Lei de Gresham, que demonstra que existe faz tempo competitividade entre as moedas: “a má moeda tende a expulsar do mercado a boa moeda”.

“Não há razão para que, dentro de uma determinada comunidade, deva haver apenas um tipo de dinheiro que seja geralmente (ou pelo menos amplamente) aceito”. Moedas paralelas e/ou alternativas, como cigarros e batatas, já foram usadas inúmeras vezes na história (HAYEK, 2017). Mas nenhuma até hoje como o bitcoin sem um centralizador, e isso assusta governos, empresas e muitas pessoas.

Como afirmado por Peck, a única forma de “destruir o bitcoin” seria criar uma rede maior que a do bitcoin atualmente. O grande problema de Peck é crer que uma rede forte nascerá por imposição ou com um objetivo pouco louvável como o de destruir uma outra rede. Se uma rede nascesse somente com esse propósito, assim que o alcançasse, já não teria mais razão de existir.

Propósitos das redes

A pesquisa de Titmuss, de 1970, sobre doação de sangue em diversos países, fomentou debates sobre as motivações econômicas das pessoas. A pesquisa de - Titmuss concluiu que apenas 9% dos doadores de sangue nos EUA doavam sangue por altruísmo. Os demais doadores faziam para doar diretamente a um receptor já conhecido ou “doavam” o sangue em troca de dinheiro. Mas a conclusão mais alarmante foi que, nos países que proibiam a compra de sangue, o índice de contaminação por hepatite era menor que em países que permitiam a comercialização de sangue (ARROW, 1972). A pesquisa de Titmuss demonstra que, por interesses individuais de recompensas, as pessoas estariam dispostas até mesmo a contaminar outra.

Ao criar um ecossistema, além de pensamentos destrutivos do ambiente externo como o de Peck, as DOs devem se preparar para receber “sangue contaminado”. Os próprios participantes internos do ecossistema poderão ser uma ameaça ao ecossistema. Atitudes irracionais na busca de maximização dos lucros individuais podem ser destrutivas, como a ilustrada no ensaio “Tragédia dos Comuns”, de Hardin (1968).

Na “Tragédia dos Comuns” os pastores de ovelhas compartilham um pasto comum a todos. Por interesse pessoal, um pastor adiciona mais uma ovelha ao pasto. Dessa forma, outros pastores vão adicionando animais até o momento em que ocorre o fenômeno do sobrepastoreio, a desertificação do pasto e a destruição de todo o ecossistema comum a todos (HARDIN, 1968).

Como pioneiro, o bitcoin foi uma DAO que cresceu de forma orgânica, sem ICO e investidores. Inicialmente seus usuários eram formados por grupos de hackers e pesquisadores, e a recompensa financeira não era a principal motivação do

grupo. Com o aumento da rede, a valorização do bitcoin foi algo natural e atraiu uma nova leva de participantes focada exclusivamente em ganhos rápidos com criptoativos. Foram nascendo empresas focadas exclusivamente na mineração de bitcoins. Isso aumentou a necessidade de poder computacional e elevou os investimentos em hardware e gastos com energia. Como consequência, o poder de mineração se concentrou e, com isso, a distribuição nas emissões das moedas, a influência de um pequeno grupo na governança do sistema e uma exposição maior a um ataque 51% à rede[1].

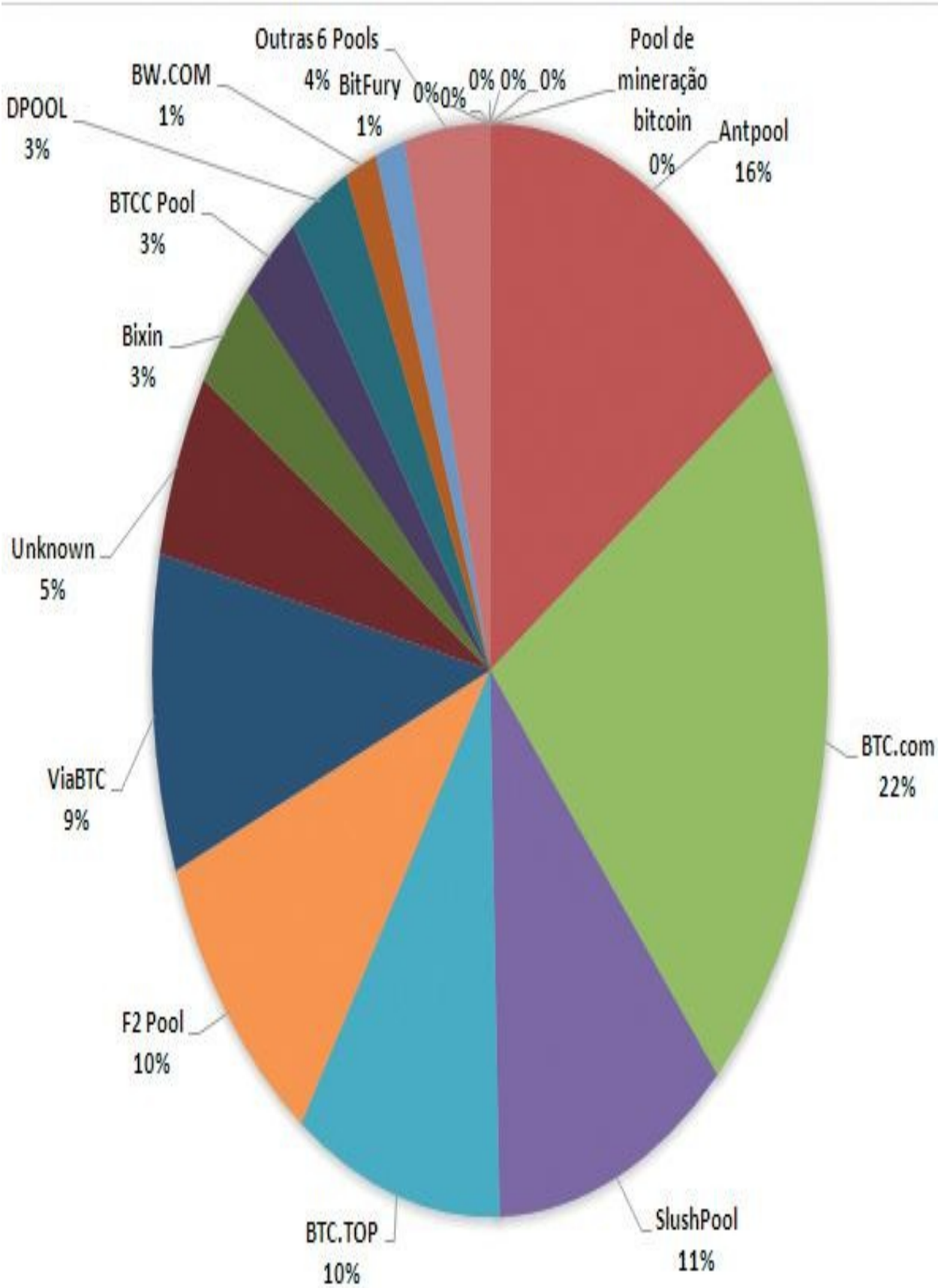

Outras 6 Pools
4%
BitFury
1%
0%
0%
0%
0%
0%
Pool de mineração bitcoin
0%
Antpool
16%
BW.COM
1%
DPOOL
3%
BTCC Pool
3%
Bixin
3%
Unknown
5%
ViaBTC
9%
F2 Pool
10%
BTC.TOP
10%
SlushPool
11%
BTC.com
22%

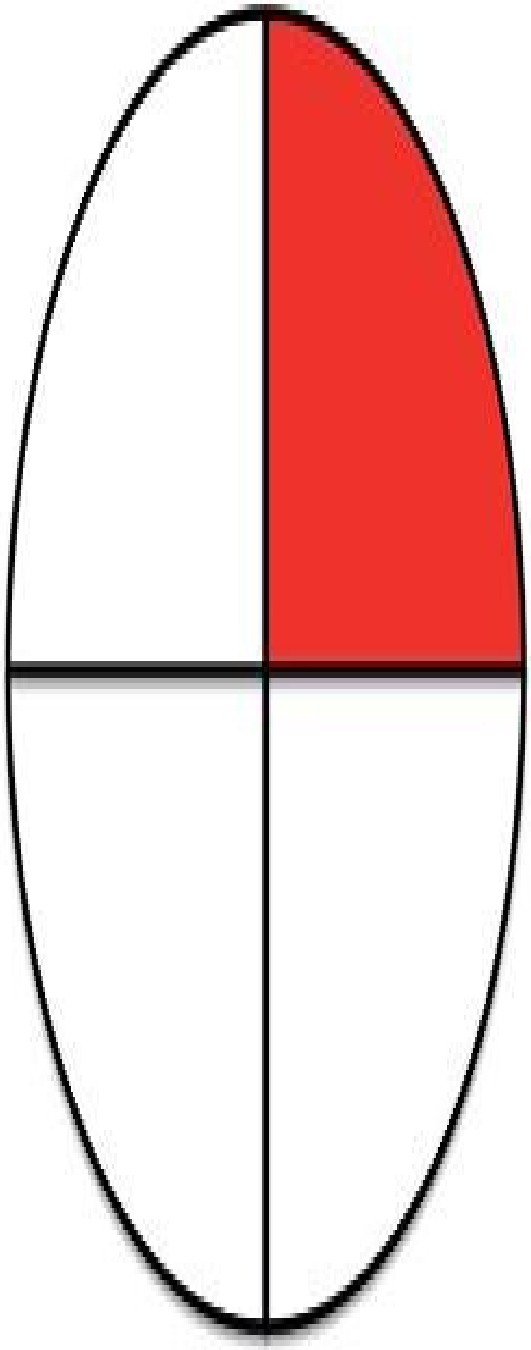
Figura 19. Pool de mineração bitcoin. Fonte: BLOCKCHAIN, junho de 2018.

Essa concentração na criação de blocos em poucos mineradores é uma das críticas atuais ao bitcoin da qual outras DOs tentam se prevenir alterando algoritmos de consenso, visando evitar a mineração em ASIC (Application Specific Integrated Circuit) ou adotando outras formas de consenso[2,3]. As DOs devem sempre buscar formas de se manter realmente descentralizadas, pois a centralização pode criar grupos que assumam o controle das DOs na exclusiva busca de maximização de seus retornos individuais. Ilustramos esse desafio com a Teoria dos Jogos e o Ponto de Schelling.

As pesquisas de Schelling em 1960 demonstram que as pessoas são capazes de atingir alto nível de coordenação, mesmo sem nenhuma comunicação, somente estimuladas por rótulos salientes em prol de recompensas simétricas. Mas pesquisas de Crawford demonstram que pontos focais baseados os rótulos salientes podem perder muito do seu poder quando a saliência do rótulo é oposta pela saliência de pagamento (CRAWFORD et al., 2008).

Pode-se ilustrar as pesquisas em relação aos pontos focais e as recompensas como a divisão de um pedaço de torta, onde se destaca um pedaço em relação aos outros e se pede para que os participantes escolham o mesmo pedaço que outros participantes, para que os dois sejam recompensados.

Ponto Simétrico



Ponto Assimétrico

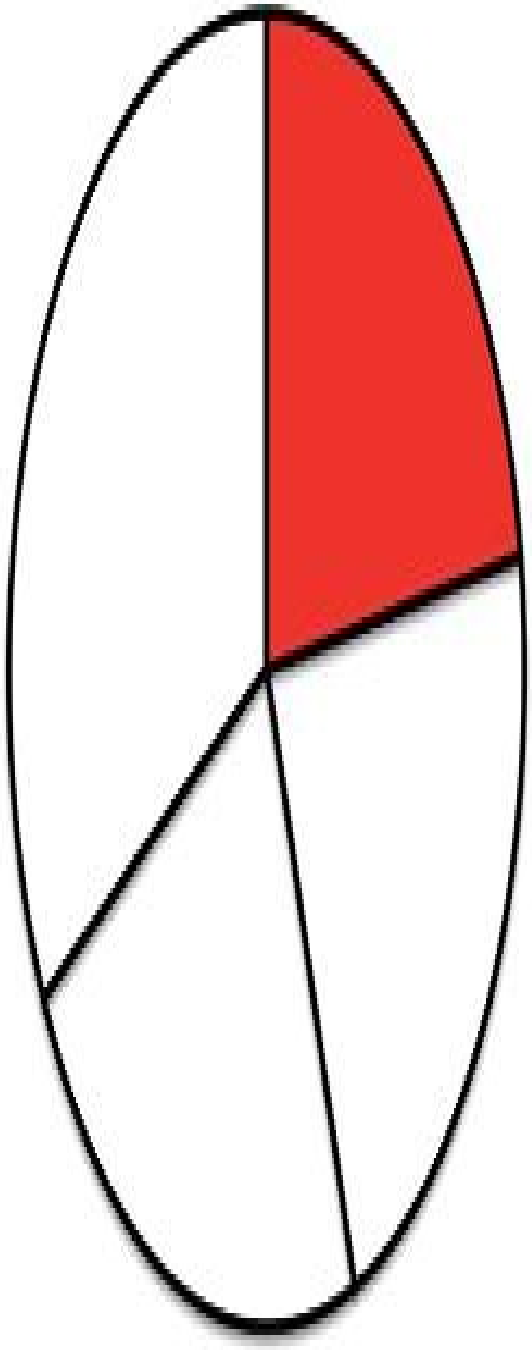


Figura 20. Pontos focais de Schelling. Fonte: o autor.

O nível de escolha dos participantes do pedaço saliente em uma torta de pedaços idênticos chega a 90%. Quando se realiza a pesquisa com pedaços assimétricos, mesmo que se ressalte um pedaço em relação aos demais, o nível de coordenação despenca para próximo a 60%, pois o pedaço maior atrai muitos participantes (CRAWFORD et al., 2008). Essa perda de foco já ocorre em organizações tradicionais, onde os indivíduos buscam promoções salariais ou outras recompensas individuais. Shermin (2017) afirma que se deve buscar expressar o máximo possível em códigos de programação o foco das DOs e evitar que recompensas assimétricas confundam a coordenação descentralizada.

E ainda não está claro qual tipo de coordenação seria a mais adequada em uma DO. Isso fica evidente com a análise da estrutura de coordenação dos maiores criptoativos de valor de mercado. O bitcoin, o maior e mais conhecido criptoativo, é uma DAO. O segundo criptoativo com maior capitalização é o Ethereum, que possui uma fundação na coordenação do projeto. E em terceiro lugar está a empresa Ripple, que foca em soluções financeiras e é um blockchain híbrido. Mas o foco dos investidores é meramente especulativo e irracional. Assim, analisar os objetivos das DOs somente por seu valor de mercado não permite verificar se o seu objetivo é alcançado.

Mudando a amostra para a relação de objetivos com o volume comercializado, se consegue uma melhor análise. Como já informado, o Tether assume a segunda posição em volume de troca mensal, o que mostra que a proposta de utilidade do token no criptomercado está sendo alcançada. Merece destaque o token da Verge, que em valor de mercado é a 24ª e assume a décima posição quando se trata de volume de troca. Esse dado pode supor que, como proposta de projeto de

criptomoeda, a Verge vem atingindo seus objetivos[4].

A Verge nasceu em junho de 2014 com o nome de DogeCoinDark e aprimorou o blockchain do bitcoin com a missão de realizar transações diretas, rápidas, eficientes e privadas. Em 2017 o projeto muda seu nome para Verge, lançando um novo white paper (dark paper) e incorporando melhorias com foco na privacidade em seu protocolo. A Verge não foi financiada por empresa ou ICO e sim por um grupo de pessoas que dedicou seu tempo ao projeto. Observa-se em seu site que o foco é o engajamento e o crescimento da comunidade, oferecendo diversos canais de contato com a equipe para proposta de melhorias, como fóruns, e-mail e github dos códigos disponíveis. O site destaca uma vasta lista de comerciantes que aceitam o token como forma de pagamento, o que incentiva e oferece publicidade espontânea aos apoiadores. Por já possuir uma comunidade sólida e participativa, a Verge usa um recurso de limitar a participação de pessoas em seu grupo do Telegram. Usando um bot do Telegram que só permite a entrada de pessoas com endereço com tokens Verge nas carteiras, torna o Telegram um canal produtivo, com debates que focam mais em melhorias de projetos e com stakeholders reais[5].

As ideias de comunidade e coesão social são contrapostas a uma sociedade drasticamente reduzida na qual os indivíduos se encontram apenas como compradores e vendedores de mercadorias (ARROW, 1972). E a Verge, ao nascer sem uma ICO que oferece tokens como troca aos financiadores, foca mais na atuante comunidade e cresce com um grupo coeso, sem a necessidade de especuladores para realização do projeto.

Mesmo assim, é igualmente falho analisar o alcance do propósito e avaliar o êxito dos objetivos de uma DO considerando somente o valor de mercado e o volume de tokens comercializados, pois Cardano, TRON e EOS já figuravam entre os top 10 criptoativos em capitalização de mercado e volume comercializado mesmo em maio de 2018, quando ainda estavam em processo de desenvolvimento de aplicações.

Estratégia taxa zero

Em meados de 2018 têm surgido projetos focados em taxa de transações a custo zero. Difícil saber se isso atrairá participantes para realmente criar uma rede distribuída, pois qual seria o interesse dos nodos em participar de uma rede que muitas vezes necessita de hardwares específicos para manter a qualidade do serviço? Além disso, as taxas de transação são utilizadas como defesa do sistema para evitar spams e travamento da rede. Possivelmente essa estratégia de competitividade seja interessante para aplicações M2M (Machine-to-Machine) e blocos privados ou consórcios.

Até o momento, creio que a construção de redes de qualidade e com objetivos claros e explícitos a todos os participantes seja a melhor forma de competir e alcançar algum sucesso no mercado distribuído, mesmo que vejamos a complexidade de conseguir uma união e proteção exclusivamente codificada em protocolos.

Outras considerações

Como disse Gilberto Gil, “a gente vai ficando velho e o mundo vai ficando novo”.

Schumpeter já ressaltava que em novas combinações socioeconômicas serão utilizados os “meios de produção que já não estejam à disposição do Ministério da Economia”. A essência das operações e comunicações P2P é exatamente a retirada de qualquer agente intermediário. Assim como as organizações descentralizadas retiram a figura do empresário e a ideia de lucro organizacional, é retirada também a atuação governamental. Claro que essas mudanças podem afetar a estrutura dos estados e sua arrecadação fiscal.

E como os estados podem mitigar os impactos, principalmente monetário e fiscal, das novas combinações socioeconômicas?

É importante recordar aspectos basilares da sociedade moderna. Em 1762, Rousseau escreveu o livro “Do Acordo Social”. O ilustre filósofo afirma que os “homens nascem livres” e a força, inclusive a estatal, não é um direito, é somente uma convenção de bases autoritárias. No pacto social todas as partes são juízes, e se no julgamento dos particulares os seus direitos não são respeitados, até mesmo a legitimidade da força se perderia e a associação entre as partes seria inútil ou tirânica.

As DOs se aproximam do liberalismo mercantil, próximo aos conceitos da Mão Invisível de Adam Smith, de 1776, e da autorregulação do mercado. Com a retirada da interferência estatal, a possibilidade de sonegação de impostos poderá

aumentar. Por esses motivos a necessidade de transparência na administração pública e a eficiência dos serviços estatais serão importantes para reafirmar o pacto social. Mariana Dahan (2016), economista do Banco Mundial, considera a confiança um recurso social escasso na atualidade, e esse problema seria maior nos países em desenvolvimento, onde há instabilidade política e alto índice de corrupção. Para Dahan, as oportunidades desses novos arranjos de mercado "podem depender de quão bem identificamos onde as instituições, que até agora desempenharam um papel na mediação da confiança entre as pessoas, estão aquém, especialmente na área-chave do dinheiro".

A política econômica e a influência estatal na economia crescem com as teorias de Keynes, na primeira parte do século XX, e começam a entrar em declínio por volta dos anos 70. Nessa época, economistas liberais assumem as doutrinas majoritárias nas políticas econômicas estatais (CHOMSKY, 2017). Com eles em cena, entraria a "Doutrina do Choque", onde os governos poderiam se aproveitar e até mesmo criar crises para um interesse distinto da coletividade (KLEIN, 2008).

A pesquisa anual Edelman Trust Barometer, que avalia a confiança nas instituições em 28 países, constata que 57% das pessoas não confiam nos governos, índice mais baixo entre todas as instituições avaliadas. No Brasil o índice é 72%. Ironicamente, a maioria das pessoas credita aos governos a condução da prosperidade econômica (EDELMAN, 2018).

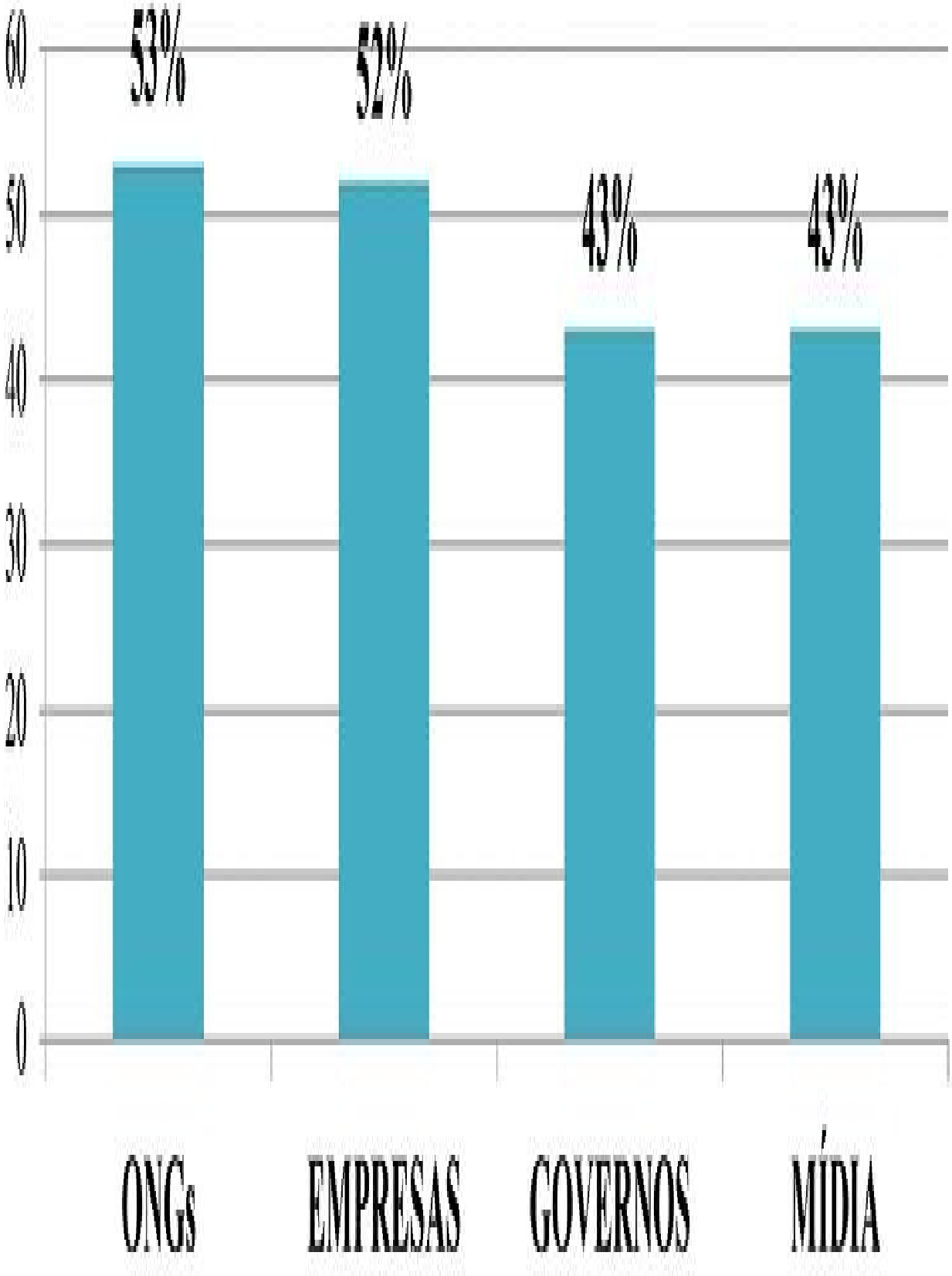

60
50
40
30
20
10
0
53%
52%
43%
43%
ONGs
EMPRESAS
GOVERNOS
MÍDIA

Figura 21. Nível de confiança – 2018. Fonte: 2018 Edelman Trust Barometer.

“Quase toda transação comercial tem em si um elemento de confiança; certamente, qualquer transação conduzida ao longo de um período de tempo. Pode-se argumentar de maneira plausível que muito do atraso econômico no mundo pode ser explicado pela falta de confiança mútua” (ARROW, 1972). No capitalismo novas formas de arranjos socioeconômicos sempre surgirão (SCHUMPETER, 1961). E quando há grandes discrepâncias no sistema capitalista, a própria sociedade buscará ajustar (REICH, 2016).

Identificar e reconhecer os potenciais das redes ausentes de lideranças que se formam nos meios virtuais será um desafio para os legisladores deste século. Foram visíveis as mudanças de configuração política dessas redes no movimento da Primavera Árabe, em 2011, derrubando ditadores que há décadas estavam no poder em nações do Oriente Médio e do norte da África. No Brasil, foi visível a falta de preparo dos governantes nas manifestações de 2013 para negociar com um movimento que começou com protestos contra o aumento de passagens de ônibus e se tornou um movimento apartidário e sem liderança de combate à corrupção de proporções nunca antes ocorridas no país. Agora essas redes se estruturam de forma econômica, e incorporá-las aos ordenamentos jurídicos será instigante. Não se pode imputar crime de evasão de divisas em ativos que não possuem fronteiras.

No início de 2018, Malta criou uma legislação de reconhecimento de DAOs. Em vez de submeter a apreciação dos criptoativos ao órgão financeiro local, foi criada uma nova entidade reguladora, mais voltada para os aspectos de auditoria de códigos-fonte das aplicações do que para aspectos econômicos clássicos de um ativo mobiliário (RONSTEDT; EGGERT, 2018). Seguramente, trata-se de um avanço nas legislações, mas principalmente na postura do governo de reconhecer o novo mundo que nasce. A ideia de que os ministros da economia continuarão no controle do “progresso econômico” das nações tende a se tornar ultrapassada. Em uma economytech a influência dos ministros da tecnologia, e a

forma de interação dos governos nessas novas economias, poderá distinguir realmente os governos progressistas e libertários dos presos e submissos a centralizadores tradicionais.

No mais, é necessário sermos realistas e percebermos que o modelo econômico atual se torna cada vez mais excludente, e essas redes crescem para suprir uma necessidade social dos seres humanos. Whyte e Nocera (1956) afirmam em “The Organization Man” que “o homem existe como uma unidade da sociedade. De si mesmo, ele é isolado, sem sentido; somente quando ele colabora com os outros, vale a pena, pois ao sublimar-se no grupo, ele ajuda a produzir um todo que é maior do que a soma de suas partes”. Enquanto as organizações tradicionais se tornaram fonte de exclusão social, as organizações descentralizadas são uma fonte colaborativa e includente para uma sociedade que hoje não consegue mais se reconhecer em seus representantes. As organizações descentralizadas são um real abrigo produtivo para homens que buscam criar um todo para todos.

Por fim... durante séculos os relógios das igrejas eram a única fonte verdadeira do tempo nas cidades. Se esse relógio atrasasse as horas, todos acreditariam que ele era a única fonte correta e todos os demais relógios estariam desajustados. Confiar em novas entidades e acreditar que possa haver uma confiança distribuída, que você pode ter poder direito nas decisões e na administração de seus bens, é uma mudança radical na mentalidade de muitos, e aqui faço o convite a você para que ajuste seu próprio relógio para construir um novo tempo, pois o criptoespaço é uma construção coletiva e distribuída!

Muito obrigado!

Referências Bibliográficas

ADHIVE. Site. Disponível em: <https://adhive.tv/#summary>. Acesso em: 01 nov. 2018.

ALLEDI FILHO, Cid. Sistema de Gestão: Sustentabilidade. 20 jul. 2017. Notas de aula.

AL-NAJI, Nader; CHEN, Josh; DIAO, Lawrence. Basis: A price-stable cryptocurrency with an algorithmic central bank. 2017.

ALTHAUSER, Joshua. Demanda de Bitcoin cresce no Zimbábue após o bem-sucedido golpe. Coin Telegraph, 19 nov. 2017. Disponível em: <https://br.cointelegraph.com/news/bitcoin-demand-surges-in-zimbabwe-following-successful-coup>. Acesso em: 04 set. 2018.

ANTONOPOULOS, Andreas M. Mastering Bitcoin: unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly Media, 2014.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. Mastering Ethereum. Disponível em: <https://github.com/ethereumbook>. Acesso em: 03 set. 2018.

ARROW, Kenneth J. Gifts and exchanges. Philosophy & Public Affairs, vol. 1, n. 4, Summer 1972, p. 343-362.

BACK, Adam et al. Enabling Blockchain Innovations with Pegged Sidechains. Oct. 22, 2014. Disponível em: <https://blockstream.com/sidechains.pdf>. Acesso em: 03 set. 2018.

BARAN, Paul. On distributed communications networks. IEEE transactions on Communications Systems, v. 12, n. 1, 1964, p. 1-9.

BENKLER, Yochai. The wealth of networks: how social production transforms markets and freedom. New Haven, CT: Yale University Press, 2006.

BENNETT, Nathan; LEMOINE, G. James. What a difference a word makes: understanding threats to performance in a VUCA world. Business Horizons, v. 57, n. 3, 2014, p. 311-317.

BINANCE Dexathon. Binance, Mar. 16, 2018. Disponível em: <https://medium.com/binanceexchange/binance-dexathon-845dc0cbfffe>. Acesso em: 03 set. 2018.

BITCOIN FORUM. Topic: Proof of stake instead of proof of work. Disponível em: <https://bitcointalk.org/index.php?topic=27787.0>. Acesso em: 03 set. 2018.

BITCOIN MARKETING TEAM. Site. Disponível em: <https://bitcoinmarketingteam.com/>. Acesso em: 03 set. 2018.

BITCOIN WIKI. Economic majority. Disponível em:

<https://en.bitcoin.it/wiki/Economic_majority>. Acesso em: 03 set. 2018.

BITCOIN.ORG. Bitcoin Developer Guide. Consensus Rule Changes. Disponível em: <https://bitcoin.org/en/developer-guide#consensus-rule-changes>. Acesso em: 03 set. 2018.

BITCOINWIKI. Proof of Stake. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_Stake>. Acesso em: 03 set. 2018.

BITCOINWIKI. Proof of work. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_work>. Acesso em: 03 set. 2018.

BLECHER, Nelson. O segredo das Casas Bahia. Revista Exame, 18 fev. 2004, p. 44-54.

BLOCKGEEKS. 5 High Profile Cryptocurrency Hacks. Disponível em: <https://blockgeeks.com/guides/cryptocurrency-hacks>. Acesso em: 03 set. 2018.

BR – THE BLOCKCHAIN REVIEW. How to Launch an Initial Coin Offering: a comprehensive guide of all you need to know. BR, 2017. Disponível em: <https://blockchainreview.io/wp-content/uploads/2017/12/How-to-launch-ICO.pdf>. Acesso em: 03 set. 2018.

BRINKER, Scott. The Blockchain Marketing Technology Landscape. Chiefmartec, Sep. 26, 2017.

BUCK, Jon. Oráculos Blockchain, Explicado. Coin Telegraph, 18 out. 2017. Disponível em: <https://br.cointelegraph.com/explained/blockchain-oracles-explained>. Acesso em: 05 set. 2018.

BUTERIN, Vitalik. A next-generation smart contract and decentralized application platform. White paper, 2014a.

BUTERIN, Vitalik. Analyzing Token Sale Models. Vitalik Buterin's website, Jun. 9, 2017a. Disponível em: <https://vitalik.ca/general/2017/06/09/sales.html>.

BUTERIN, Vitalik. DAOs, DACs, DAs and more: an incomplete terminology guide. Ethereum Blog, May 6, 2014b. Disponível em: <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>. Acesso em: 06 set. 2018.

BUTERIN, Vitalik. Notes on Blockchain Governance. Vitalik Buterin's website, Dec. 17, 2017b. Disponível em: <https://vitalik.ca/general/2017/12/17/voting.html>. Acesso em: 06 set. 2018.

BUTERIN, Vitalik. On Public and Private Blockchains. Ethereum, 2015.

CARBONVOTE. Site. Disponível em: <http://carbonvote.com/>. Acesso em: 03 set. 2018.

CERMAK, Vavrinec. Can Bitcoin Become a Viable Alternative to Fiat

Currencies? An Empirical Analysis of Bitcoin Volatility Based on a GARCH Model. 2017.

CHIAVENATO, Idalberto. Introdução à Teoria Geral da Administração. 9.ed. Barueri: Manole, 2014.

CHOHAN, Usman. Cryptoanarchism and Cryptocurrencies. 2017a.

CHOHAN, Usman. The Decentralized Autonomous Organization and Governance Issues. 2017b.

CHOMSKY, Noam. Requiem for the American Dream: the 10 principles of concentration of wealth & power. New York, NY: Seven Stories Press, 2017.

COBLEE. Litecoin price, tweets, and conflict of interest. Reddit, Jan. 2018. Disponível em: <https://www.reddit.com/r/litecoin/comments/7kzw6q/litecoin_price_tweets_and Acesso em: 03 set. 2018.

COIN GOVERNANCE SYSTEM. Site. Disponível em: <https://cgs.vote/>. Acesso em: 05 set. 2018.

COIN SCHEDULE. Cryptocurrency ICO Stats 2018. Disponível em: <https://www.coinschedule.com/stats.html>. Acesso em: 01 nov. 2018.

COINMARKETCAP. Site. Disponível em: <https://coinmarketcap.com/>. Acesso em: 01 nov. 2018.

COMM, Joel. The Bots of Bitcoin. Forbes, Dec. 1st, 2017. Disponível em: <https://www.forbes.com/sites/forbescoachescouncil/2017/12/01/the-bots-of-bitcoin/#4c36c08d5b08)>. Acesso em: 03 set. 2018.

CONLEY, John P. Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings. Vanderbilt University Department of Economics Working Papers, Vanderbilt University Department of Economics, 2017. Disponível em: <https://ideas.repec.org/p/van/wpaper/vuecon-sub-17-00007.html>. Acesso em: 03 set. 2018.

CORALLO, Matt. A look at a few Questions and Misconceptions Regarding Pegged Sidechains. BlockStream, Oct. 30 2014. Disponível em: <https://blockstream.com/2014/10/30/a-look-at-a-few-questions-and-misconceptions-for-pegged-sidechains/>. Acesso em: 03 set. 2018.

CRAWFORD, Vincent P.; GNEEZY, Uri; ROTTENSTREICH, Yuval. The power of focal points is limited: even minute payoff asymmetry may yield large coordination failures. American Economic Review, v. 98, n. 4, 2008, p. 1443-58.

CRYPTOECONOMICS. Site. Disponível em: <http://cryptoeconomics.com.au/>. Acesso em: 03 set. 2018.

CUCCURU, Pierluigi. Beyond Bitcoin: an early overview on smart contracts. International Journal of Law and Information Technology, v. 25, n. 3, 2017, p. 179-195.

DAHAN, Mariana. Blockchain technology: redefining trust for a global, digital economy. World Bank, June 16, 2016. Disponível em: <http://blogs.worldbank.org/ic4d/blockchain-technology-redefining-trust-global-digital-economy>. Acesso em: 06 set. 2018.

DASH BUDGET PROPOSAL VOTE TRACKER. Site. Disponível em: <https://dashvotetracker.com>. Acesso em: 03 set. 2018.

DE FILIPPI, Primavera. A $50M Hack Tests the Values of Communities Run by Code: the ideal of a perfectly trustless technology is nothing more than an ideal. Motherboard, July 11, 2016. Disponível em: <https://motherboard.vice.com/en_us/article/qkjz4x/thedao>. Acesso em: 03 set. 2018.

DECRED. Decred Documentation. Overview. Disponível em: <https://docs.decred.org>. Acesso em: 03 set. 2018.

DIAA, Mona. Inside Egypt's cryptocurrency market. Egypt Today, Jan. 26, 2018. Disponível em: <https://www.egypttoday.com/Article/3/40995/Inside-Egypt%E2%80%99s-cryptocurrency-market>. Acesso em: 03 set. 2018.

DIGIX. Site. Disponível em: <https://digix.zendesk.com/hc/en-us>. Acesso em: 03 set. 2018.

DON'T Believe Facebook; You Only Have 150 Friends. NPR, June 05, 2011. Disponível em: <https://www.npr.org/2011/06/04/136723316/dont-believe-

facebook-you-only-have-150-friends>. Acesso em: 03 set. 2018.

DRUCKER, Peter Ferdinand. The coming of the new organization. Harvard Business Review, jan. 1988. Disponível em: <https://hbr.org/1988/01/the-coming-of-the-new-organization>. Acesso em: 05 set. 2018.

DUNBAR, Robin I. M. The Social Brain: psychological underpinnings and implications for the structure of organizations. Current Directions in Psychological Science, v. 23, n. 2, 2014, p. 109-114.

EDELMAN, R. Edelman Trust Barometer. 2018. Disponível em: <https://www.edelman.com/trust-barometer>. Acesso em: 06 set. 2018.

EOS. Frequently Asked Questions: here are some common questions about EOS and EOSIO. Disponível em: <https://eos.io/faq>. Acesso em: 03 set. 2018.

ESTCOIN Backs Down as Banking Authorities Bully Estonia. Coinnews, Mar. 06, 2018. Disponível em: <http://www.coinnews.life/events/estcoin-backs-down-as-banking-authorities-bully-estonia/>. Acesso em: 03 set. 2018.

ETHEREUM. History of Ethereum. Disponível em: <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>. Acesso em: 03 set. 2018.

FIELD, Matan. Decentralized Governance Matters. DAOstack, Feb. 06, 2018. Disponível em: <https://medium.com/daostack/decentralized-governance-first-

principles-1fc6eaa492ed>. Acesso em: 05 set. 2018.

FINMA. FINMA publishes ICO guidelines. FINMA, Feb. 16, 2018. Disponível em: <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung>. Acesso em: 03 set. 2018.

FOUNDATION FOR YOUNG AUSTRALIANS. The New Work Order: ensuring young Australians have skills and experience for the jobs of the future, not the past. FYA, 2015. Disponível em: <http://www.fya.org.au/wp-content/uploads/2015/08/fya-future-of-work-report-final-lr.pdf>. Acesso em: 03 set. 2018.

FRANCO, Marina. Venezuelanos investem em bitcoin para encarar desemprego, hiperinflação e falta de notas. G1, 11 nov. 2017. Disponível em: <https://g1.globo.com/mundo/noticia/venezuelanos-investem-em-bitcoin-para-encarar-desemprego-hiperinflacao-e-falta-de-notas.ghtml>. Acesso em: 03 set. 2018.

FRANKLIN, Stan; GRAESSER, Art. Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages, Springer-Verlag, 1996, p. 21-35. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.52.1255&rep=rep1&type=pdf>. Acesso em: 03 set. 2018.

FRED. Shares of gross domestic income: compensation of employees, paid: wage and salary accruals: disbursements: to persons [W270RE1A156NBEA]. Federal Reserve Bank of St. Louis, 2018. Disponível em: <https://fred.stlouisfed.org/series/W270RE1A156NBEA>. Acesso em: 01 nov. 2018.

FREEMAN, Jo. The tyranny of structurelessness. Berkeley Journal of Sociology, p. 151-164, 1972.

FURNESS, William Henry. Yap of the Carolines. JB Lippincott Company, 1910.

GARTNER GROUP. Top Strategic Predictions for 2017 and Beyond: Surviving the Storm Winds of Digital Disruption. Disponível em: <https://www.gartner.com/doc/3471568?srcId=1-6595640805>. Acesso em: 03 set. 2018.

GHIZONI, Sandra Kollen. Nixon Ends Convertibility of US Dollars to Gold and Announces Wage/Price Controls. Federal Reserve History, Aug. 1971. Disponível em: <https://www.federalreservehistory.org/essays/gold_convertibility_ends>. Acesso em: 04 set. 2018.

GIBRALTAR FINANCIAL SERVICES COMMISSION. Statement on Initial Coin Offerings. Gibraltar Financial Services Commission, Sep. 22, 2017. Disponível em: <http://www.gfsc.gi/news/statement-on-initial-coin-offerings-250>. Acesso em: 03 set. 2018.

GILSON, Dave; PEROT, Carolyn. It’s the inequality, stupid. Mother Jones, Mar./Apr. 2011. Disponível em: <https://www.motherjones.com/politics/2011/02/income-inequality-in-america-chart-graph/>. Acesso em: 01 nov. 2018.

GOING to War: Monero Sticks to Anti-ASIC Guns with emergency Software Update. CCN, Mar. 26, 2018. Disponível em: <https://www.ccn.com/monero-sticks-to-anti-asic-guns-with-emergency-software-update>. Acesso em: 04 set. 2018.

GÓMEZ, Eduardo. The DAO Undergoes Low Voting Turnout. NullTX, June 11, 2016. Disponível em: <https://nulltx.com/the-dao-undergoes-low-voting-turnout/>. Acesso em: 03 set. 2018.

GUSSON, Cassio. Exchange distribui Stellar para novos usuários em sua plataforma. Criptomoedas Fácil, 27 abr. 2018. Disponível em: <https://www.criptomoedasfacil.com/exchange-distribui-stellar-para-novos-usuarios-em-sua-plataforma>. Acesso em: 04 set. 2018.

GUSSON, Cassio. Vitalik Buterin é contra hard fork para impedir a Bitmain na Ethereum. Criptomoedas Fácil, 10 abr. 2018. Disponível em: <https://www.criptomoedasfacil.com/vitalik-buterin-e-contra-hard-fork-para-impedir-a-bitmain-na-ethereum/>. Acesso em: 04 set. 2018.

HACKER, Jacob S.; PIERSON, Paul. Winner-take-all politics: Public policy, political organization, and the precipitous rise of top incomes in the United States. Politics & Society, Vol. 38, n. 2, May 24, 2010.

HARARI, Yuval Noah. Homo Deus: a brief history of tomorrow. New York, NY: Random House, 2016.

HARDIN, Garrett. The tragedy of the commons. Journal of Natural Resources Policy Research, v. 1, n. 3, 2009, p. 243-253.

HAYEK, Friedrich A. Desestatização do Dinheiro. São Paulo: LVM, 2017.

HIGH Speed Traders Are Taking Over Bitcoin. Bloomberg, Jan. 16, 2017. Disponível em: <https://www.bloomberg.com/news/articles/2017-01-16/high-speed-traders-are-taking-over-bitcoin-as-easy-money-beckons>. Acesso em: 03 set. 2018.

HILEMAN, Garrick; RAUCHS, Michel. Global Cryptocurrency Benchmarking Study. Cambridge, UK: Cambridge Centre for Alternative Finance, 2017. Disponível em: <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf>. Acesso em: 05 set. 2018.

HONTORIA, Nacho. NEM vs Ethereum: why do we migrate of Blockchain in Tutellus? Tutellus.io, Feb. 28, 2018. Disponível em: <https://medium.com/tutellus-io/nem-vs-ethereum-why-do-we-migrate-of-blockchain-in-tutellus-2e823526fb19>. Acesso em: 03 set. 2018.

HUBERMAN, Gur; LESHNO, Jacob D.; MOALLEMI, Ciamac C. Monopoly Without a Monopolist: an economic analysis of the bitcoin payment system. Columbia Business School, Oct. 17, 2017. Disponível em: <https://moallemi.com/ciamac/papers/bitcoin-2017.pdf>. Acesso em: 06 set. 2018.

ICO MARKET DATA. Site. Disponível em: <https://www.icomarketdata.com/>. Acesso em: 01 nov. 2018.

IMF. IMF Fiscal Monitor: Capitalizing on Good Times. IMF, Apr. 2018.

INSTITUTE FOR THE FUTURE; DELL. The Next Era of Human|Machine Partnerships: emerging technologies' impact on society & work in 2030. IFTF/Dell Technologies, 2017. Disponível em: <http://www.iftf.org/fileadmin/user_upload/downloads/th/SR1940_IFTFforDellTMachine_070717_readerhigh-res.pdf>. Acesso em: 03 set. 2018.

INSTITUTE OF INTERNATIONAL FINANCE. Global Debit Monitor. IIF, 2018. Disponível em: <https://www.iif.com/publications/global-debt-monitor>. Acesso em: 03 set. 2018.

JAPANESE crypto exchange says US$400 million in NEM currency lost. South China Morning Post, Jan. 27, 2018. Updated Feb. 06, 2018. Disponível em: <http://www.scmp.com/business/banking-finance/article/2130804/japanese-crypto-exchange-says-us400-million-nem-currency>. Acesso em: 03 set. 2018.

JENTZSCH, Christoph. The History of the DAO and Lessons Learned. Slock.it Blog, Aug. 24, 2016. Disponível em: <https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5>. Acesso em: 05 set. 2018.

JOHNSTON, Alistair. WoWoo Announces Blockchain Migration to NEO Platform. ICO Examiner, Feb. 19, 2018. Disponível em: <https://www.icoexaminer.com/ico-news/woowoo-announces-blockchain-migration-neo-platform>. Acesso em: 03 set. 2018.

KENNARD, Fredrick. Thought Experiments: popular thought experiments in philosophy, physics, ethics, computer science & mathematics. Lulu.com, 2015.

KHATWANI, Sudhir. 9 Best Decentralized Exchanges Which You Can Use To Trade Right Now. Coin Sutra, June 13, 2018. Disponível em: <https://coinsutra.com/best-decentralized-exchanges-dex>. Acesso em: 03 set. 2018.

KIDD, Natalia. Diez años después del ‘corralito’. El Mundo, 01 Dic. 2011. Disponível em: <http://www.elmundo.es/america/2011/11/30/argentina/1322664968.html>. Acesso em: 03 set. 2018.

KLEIN, Naomi. A Doutrina do Choque: a ascensão do capitalismo de desastre. Rio de Janeiro: Nova Fronteira, 2008.

LANGE, Felix. Security Alert – DoS Vulnerability in the Soft Fork. Ethereum Blog, June 28, 2018. Disponível em: <https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork/>. Acesso em: 03 set. 2018.

LARIMER, Daniel. DAC Revisited. Let’s Talk Bitcoin, Nov. 2nd, 2013. Disponível em: <https://letstalkbitcoin.com/dac-revisited>. Acesso em: 03 set. 2018.

LARIMER, Daniel. Delegated proof-of-stake (DPOS). Bitshare white paper, 2014.

LEVINE, Matt. Guy Trading as Home Caused the Flash Crash. Bloomberg, Apr. 21, 2015. Disponível em: <https://www.bloomberg.com/view/articles/2015-04-21/guy-trading-at-home-caused-the-flash-crash>. Acesso em: 03 set. 2018.

LUU, Loi. Solving the Liquidity Challenge of Decentralized Exchanges. Coindesk, Aug. 13, 2017. Disponível em: <https://www.coindesk.com/solving-liquidity-challenge-decentralized-exchanges>. Acesso em: 03 set. 2018.

MAC, Ryan. This Is Why Experts Are Calling Kodak's New Bitcoin Scheme a Scam. Buzzfeed, Jan. 10, 2018. Disponível em: <https://www.buzzfeed.com/ryanmac/experts-call-kodaks-bitcoin-mining-scheme-a-scam?utm_term=.dmWBgYq3g#.tanmW4MKW>. Acesso em: 04 set. 2018.

MAGAZZENI, Daniele; MCBURNEY, Peter; NASH, William. Validation and Verification of Smart Contracts: a research agenda. Computer, v. 50, n. 9, 2017, p. 50-57.

MANKIW, N. Gregory. Introdução à Economia. 3.ed. São Paulo: Cengage Learning, 2009.

MARK, Dino; ZAMFIR, Vlad; SIRER, Emin Gün. A Call for a Temporary Moratorium on The DAO. Hacking Distributed, May 27, 2016. Disponível em: <http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/>. Acesso em: 06 set. 2018.

MARSHALL, Andrew. Bitcoin Unlimited Hard Fork. Should I Do Something About It? Coin Telegraph, Apr. 01, 2017. Disponível em: <https://cointelegraph.com/news/bitcoin-unlimited-hard-fork-should-i-do-something-about-it>. Acesso em: 03 set. 2018.

MEIKLEJOHN, Sarah et al. A Fistful of Bitcoins: characterizing payments among men with no names. Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013, p. 127-140. Disponível em: <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>. Acesso em: 03 set. 2018.

METALLICA x Napster aconteceu há 8 anos. Revista Rolling Stone, 12 abr. 2008. Disponível em: <http://rollingstone.uol.com.br/noticia/metallica-x-napster-aconteceu-ha-8-anos/#imagem0>. Acesso em: 03 set. 2018.

METCALFE, Bob. Metcalfe's Law after 40 Years of Ethernet. Computer, vol. 16, n. 12, Dec. 2013, p. 26-31.

MILLIKEN, David. Bitcoin has 'failed' as a currency, says Mark Carney. Independent, Feb. 20, 2018. Disponível em: <https://www.independent.co.uk/news/business/news/bitcoin-currency-failed-mark-carney-digital-bank-of-england-a8218971.html>. Acesso em: 04 set. 2018.

MONTARROYOS, Heraldo Elias de Moura. A anarquia ordenada e suas regras de decisão: uma concepção da emergência da cooperação social. Tese. (Doutorado em Filosofia) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2006. Disponível em: <http://www.teses.usp.br/teses/disponiveis/8/8133/tde-09012008-100000/pt-br.php>. Acesso em: 03 set. 2018.

MOORE, Michael. Capitalism: a love story. Filme. Ascot Elite Home Entertainment, 2010.

MOUGAYAR, William. The Business Blockchain: promise, practice, and application of the next Internet technology. Hoboken, NJ: John Wiley & Sons, 2016.

MOUGAYAR, William. Where Are All The Decentralized Applications?. Startup Management, May 28, 2018. Disponível em: <http://startupmanagement.org/2018/05/28/where-are-all-the-decentralized-applications>. Acesso em: 03 set. 2018.

MULLER, Caroline. Estamos construindo nossa casa graças ao Steemit. Steemit, 31 jan. 2018. Disponível em: <https://steemit.com/pt/@caroline.muller/estamos-construindo-nossa-casa-gracas-ao-steemit>. Acesso em: 04 set. 2018.

NAKAMOTO, Satoshi. Bitcoin: a peer-to-peer electronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 03 set. 2018.

NEM. General Information. Disponível em: <http://docs.nem.io/en>. Acesso em: 01 nov. 2018.

NEM. Site. Disponível em: <https://nem.io/>. Acesso em: 03 set. 2018.

NEXT AUTONOMOUS. CRYPTO: Token and Coin Exchange Listing Fees.

Apr. 03, 2018. Disponível em: <https://next.autonomous.com/thoughts/crypto-exchange-listing-fees>. Acesso em: 03 set. 2018.

NIELSEN, Jakob. Nielsen's Law of Internet Bandwidth. Nielsen Norman Group, Apr. 5, 1998. Disponível em: <https://www.nngroup.com/articles/law-of-bandwidth/>. Acesso em: 03 set. 2018.

O'NEILL, Ted. Big News: KYC and Our Switch to NEO. Narrative, Jan. 12, 2018. Disponível em: <https://blog.narrative.network/big-news-kyc-and-our-switch-to-neo-2f34215beef9>. Acesso em: 03 set. 2018.

OECD. Hours worked (indicator). doi: 10.1787/47be1c78-en. Disponível em: <https://data.oecd.org/emp/hours-worked.htm>. Acesso em: 01 nov. 2018.

PALMER, Daniel. Bank of Thailand Suggests Bitcoin Not Illegal But Warns Against Its Use. Coindesk. Mar. 18, 2014. Disponível em: <https://www.coindesk.com/bank-thailand-says-bitcoin-illegal-warns-use/>. Acesso em: 03 set. 2018.

PALMER, Jackson. My Joke Cryptocurrency Hit $2 Billion and Something Is Very Wrong: Dogecoin's inventor looks to the past for insight into the future. Motherboard, Jan. 11, 2018. Disponível em: <https://motherboard.vice.com/en_us/article/9kng57/dogecoin-my-joke-cryptocurrency-hit-2-billion-jackson-palmer-opinion>. Acesso em: 03 set. 2018.

PECK, Morgen. Let's destroy Bitcoin. MIT Technology Review, Apr. 24, 2018. Disponível em: <https://www.technologyreview.com/s/610809/lets-destroy-bitcoin/>. Acesso em: 06 set. 2018.

PETERS, Gareth W.; PANAYI, Efstathios. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. Nov. 18, 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2692487>. Acesso em: 03 set. 2018.

PISA, Michael; JUDEN, Matt. Blockchain and Economic Development: hype vs. reality. Center for Global Development Policy Paper, n. 107, July 2017. Disponível em: <https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality>. Acesso em: 06 set. 2018.

PISTONO, Federico. Os robôs vão roubar seu trabalho, mas tudo bem: como sobreviver ao colapso econômico e ser feliz. São Paulo: Companhia das Letras, 2017.

RAMIREZ, Elaine. Why South Korea Is Banning All Foreigners From Trading Cryptocurrency. Forbes, Jan. 23, 2018. Disponível em: <https://www.forbes.com/sites/elaineramirez/2018/01/23/why-south-korea-is-banning-all-foreigners-from-trading-cryptocurrency/#57f065897345>. Acesso em: 03 set. 2018.

RAY, James. Sharding FAQs. Github, 2018. Disponível em: <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>. Acesso em: 03 set. 2018.

RAYMOND, Eric S. A Catedral e o Bazar. Trad. Erik Kohler. 2000. Disponível em: <https://www.vivaolinux.com.br/artigo/A-Catedral-e-o-Bazar-Eric-S.-Raymond>. Acesso em: 05 set. 2018.

REICH, Robert B. Saving Capitalism: for the many, not the few. New York, NY: Vintage, 2016.

RIBES, Sylvain. Chasing fake volume: a crypto-plague. Medium, Mar. 10, 2018. Disponível em: <https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e>. Acesso em: 06 set. 2018.

RONSTEDT, Marlene; EGGERT, Andre. Among Blockchain-Friendly Jurisdictions, Malta Stands Out. Coindesk, July 04, 2018. Disponível em: <https://www.coindesk.com/among-blockchain-friendly-jurisdictions-malta-stands-out/>. Acesso em: 04 set. 2018.

ROSSOW, Andrew. The Rise of Stablecoins Continues In Volatile Crypto Market. Forbes, Apr. 04, 2018. Disponível em: <https://www.forbes.com/sites/andrewrossow/2018/04/04/the-rise-of-stablecoins-continues-to-grow-in-volatile-crypto-market/#371f3e2c7a10>. Acesso em: 04 set.2018.

RUSSIAN Quantum Center developed the first quantum blockchain. Russian Quantum Center, 25 maio 2017. Disponível em: <http://www.rqc.ru/news/?ELEMENT_ID=1270>. Acesso em: 30 ago. 2018.

SALSMAN, Richard M. The Bank Runs of the Early 1930s and FDR's Ban on Gold. Forbes, Apr. 06, 2011. Disponível em: <https://www.forbes.com/sites/richardsalsman/2011/04/06/the-bank-runs-of-the-early-1930s-and-fdrs-ban-on-gold/#374229043ee5>. Acesso em: 03 set. 2018.

SCHELLING, Thomas C. The strategy of conflict. New York, NY: Oxford University Press, 1963.

SCHOEDON, Afri. The Ethereum-blockchain size will not exceed 1TB anytime soon. DEV, Nov. 29, 2017. Updated on Dec. 17, 2017. Disponível em: <https://dev.to/5chdn/the-ethereum-blockchain-size-will-not-exceed-1tb-anytime-soon-58a>. Acesso em: 03 set. 2018.

SCHUMPETER, Joseph A. Teoria do desenvolvimento econômico. Rio de Janeiro: Fundo de Cultura, 1961.

SHERMIN, Voshmgir. Disrupting governance with blockchains and smart contracts. Strategic Change, v. 26, n. 5, 2017, p. 499-509.

SILLABER, Christian; WALTL, Bernhard. Life Cycle of Smart Contracts in Blockchain Ecosystems. Datenschutz und Datensicherheit-DuD, v. 41, n. 8, 2017, p. 497-500.

SMITH, Adam. A riqueza das nações: investigação sobre a natureza e suas causas. São Paulo: Nova Cultural, 1988.

SÖDERBERG, Gabriel. Are Bitcoin and other crypto-assets money? Economic Commentaries, n. 5, Mar. 14, 2018. Disponível em: <https://bank.gov.ua/doccatalog/document?id=71289967>. Acesso em: 06 set. 2018.

STACK EXCHANGE. How could the bitcoin protocol be changed? Has this ever occurred? Bitcoin questions, s.d. Disponível em: <https://bitcoin.stackexchange.com/questions/3945/how-could-the-bitcoin-protocol-be-changed-has-this-ever-occurred#comment4983_3948>. Acesso em: 03 set. 2018

STEEM TOOLS. Site. Disponível em: <http://steemtools.com>. Acesso em: 04 set. 2018.

STOPANDDECRYPT. The Ethereum-blockchain size has exceeded 1TB, and yes, it's an issue. Hackernoon, May 23, 2018. Disponível em: <https://hackernoon.com/the-ethereum-blockchain-size-has-exceeded-1tb-and-yes-its-an-issue-2b650b5f4f62>. Acesso em: 03 set. 2018.

SUNDARARAJAN, Sujha. Estonia Inches Closer to National 'Crypto Token' Launch. Coindesk, Dec. 19, 2017. Disponível em: <https://www.coindesk.com/estonia-inches-closer-to-national-crypto-token-launch/>. Acesso em: 03 set. 2018.

SWANSON, Tim. Bitcoin Hurdles: the public goods costs of securing a decentralized seigniorage network which incentivizes alternatives and centralization. Rev. Apr. 09, 2014. Disponível em: <http://www.ofnumbers.com/wp-content/uploads/2014/04/Bitcoins-Public-Goods-hurdles.pdf>. Acesso em: 03 set. 2018.

SWANSON, Tim. Blockchain 2.0 – Let a Thousand Chains Blossom. Let's Talk Bitcoin, Apr. 08, 2014. Disponível em: <https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom>. Acesso em: 03 set. 2018.

SWEENEY, Dennis J.; WILLIAMS, Thomas A.; ANDERSON, David R. Estatística Aplicada à Administração e Economia. São Paulo: Cengage Learning, 2013.

SZABO, Nick. A formal language for analyzing contracts. Nick Szabo's Papers and Concise Tutorials, 2002. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literatu Acesso em: 03 set. 2018.

SZABO, Nick. Formalizing and securing relationships on public networks. First Monday, v. 2, n. 9, Sep. 1997b. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First>. Acesso em: 03 set. 2018.

SZABO, Nick. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 1997a. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literatu Acesso em: 03 set. 2018.

TAPSCOTT, Don; TAPSCOTT, Alex. Blockchain Revolution: how the technology behind bitcoin is changing money, business, and the world. New York, NY: Penguin, 2016.

TAR, Andrew. UASF vs. UAHF, Explained. Coin Telegraph, July 19, 2017. Disponível em: <https://cointelegraph.com/explained/uasf-vs-uahf-explained>. Acesso em: 03 set. 2018.

TAVARES, Paulino Varela; KRETZER, Jucélio; MEDEIROS, Natalino.

Economia Neoschumpeteriana: expoentes evolucionários e desafios endógenos da indústria brasileira. Revista Economia Ensaios, v. 20, n. 1, 2005.

THE TRUST Machine. The Economist, Oct. 31st, 2015. Disponível em: <https://www.economist.com/leaders/2015/10/31/the-trust-machine>. Acesso em: 03 set. 2018.

TODD, Peter. [Bitcoin-development] Tree-chains preliminary summary. Mar 25, 2014. Disponível em: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-March/004797.html>. Acesso em: 03 set. 2018.

TWEED, David. Bitcoin Can't Save World's Autocrats From the Sanctions Squeeze. Bloomberg, Jan. 15, 2018. Disponível em: <https://www.bloomberg.com/news/articles/2018-01-15/bitcoin-can-t-save-world-s-autocrats-from-the-sanctions-squeeze>. Acesso em: 04 set. 2018.

VERGE. Site. Disponível em: <http://vergecurrency.com/>. Acesso em: 04 set. 2018.

VILLELA, Gustavo. Plano Collor confiscou a poupança, e Brasil mergulhou na hiperinflação. Acervo O Globo, 16 mar. 2015. Atualizado em 30 nov. 2017. Disponível em: <http://acervo.oglobo.globo.com/fatos-historicos/plano-collor-confiscou-poupanca-brasil-mergulhou-na-hiperinflacao-15610534>. Acesso em: 03 set. 2018.

WHITE, Gareth R. T. Future applications of blockchain in business and management: A Delphi study. Strategic Change, v. 26, n. 5, 2017, p. 439-451.

WHYTE, William Hollingsworth; NOCERA, Joseph. The Organization Man. New York: Simon and Schuster, 1956.

WILKINSON, Shawn. Migration from Counterparty to Ethereum. Storj, Mar. 23, 2017. Disponível em: <https://blog.storj.io/post/158740607128/migration-from-counterparty-to-ethereum>. Acesso em: 03 set. 2018.

WILLETT, J. R. The Second Bitcoin Whitepaper. vs. 0.5 (Draft for Public Comment). White paper, 2013. Disponível em: <https://bravenewcoin.com/assets/Whitepapers/2ndBitcoinWhitepaper.pdf>. Acesso em: 03 set. 2018.

WILLIANS-GRUT, Oscar. ‘Market manipulation 101’: ‘Wolf of Wall Street’-style ‘pump and dump’ scams plague cryptocurrency markets. Business Insider, Nov. 14, 2017. Disponível em: <http://uk.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11>. Acesso em: 03 set. 2018.

WILT, Jerom de. DAO, can it be viable?: An exploratory research on the viability of a blockchain based Decentralized Autonomous Organization. Radboud Universiteit, June 2017. Disponível em: <https://theses.ubn.ru.nl/bitstream/handle/123456789/4517/Wilt%2C_Jerom_de_ sequence=1>. Acesso em: 05 set. 2018.

WOOD, Gavin. Ethereum: A secure decentralised generalised transaction ledger. EPI-150 Revision. Disponível em: <http://gavwood.com/paper.pdf>. Acesso em: 01 nov. 2018.

WORLD ECONOMIC FORUM. The future of financial infrastructure. Aug. 2016. Disponível em: <http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.p Acesso em: 01 nov. 2018.

WORLD ECONOMIC FORUM. The Future of Jobs: employment, skills and workforce strategy for the fourth industrial revolution. WEF, jan. 2016.

WORLD INEQUALITY DATABASE. Site. Disponível em: <https://wid.world/>. Acesso em: 01 nov. 2018.

WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Mar. 10, 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664>. Acesso em: 03 set. 2018.

ZHENG, Zibin et al. Blockchain Challenges and Opportunities: a survey. Int. J. Web and Grid Services, Vol. 14, n. 4, 2018.

ZYNIS, Dominik. A Brief History of Mastercoin. Omni, Nov. 29, 2013. Disponível em: <https://blog.omni.foundation/2013/11/29/a-brief-history-of-mastercoin/>. Acessado em: 03 set. 2018.

Notas

Capítulo 1

[1] Fonte: MANKIW, 2009, p. 631. Após desenvolvido o texto, o autor encontrou analogias semelhantes ao povo Yap em portais jornalísticos como Coin Telegraph e Forbes, mas manteve o texto.

[2] RUSSIAN Quantum Center developed the first quantum blockchain. Russian Quantum Center, 25 maio 2017. Disponível em: <http://www.rqc.ru/news/?ELEMENT_ID=1270>. Acesso em: 30 ago. 2018.

[3] TAPSCOTT, Don. Dell Technologies World 2018 Conference. 2018. Citação oral.

[4] BITCOINWIKI. Proof of work. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_work>. Acesso em: 03 set. 2018.

[5] BITCOIN FORUM. Topic: Proof of stake instead of proof of work. Disponível em: <https://bitcointalk.org/index.php?topic=27787.0>. Acesso em: 03 set. 2018.

[6] BITCOINWIKI. Proof of Stake. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_Stake>. Acesso em: 03 set. 2018.

[7] NEM. General Information. Disponível em: <http://docs.nem.io/en>. Acesso em: 01 nov. 2018.

Capítulo 3

[1] Fonte: METALLICA x Napster aconteceu há 8 anos. Revista Rolling Stone, 12 abr. 2008. Disponível em: <http://rollingstone.uol.com.br/noticia/metallica-x-napster-aconteceu-ha-8-anos/#imagem0>. Acesso em: 03 set. 2018.

Capítulo 4

[1] ETHEREUM. History of Ethereum. Disponível em: <http://ethdocs.org/en/latest/introduction/history-of-ethereum.html>. Acesso em: 03 set. 2018.

[2] Termo derivado do inglês top flip, onde especuladores compram ações no IPO e as vendem no primeiro pregão dessas ações nas bolsas.

[3] Danilo Vaz, Community Manager da DAOStack, em entrevista ao autor em 23 de maio de 2018.

[4] BITCOIN MARKETING TEAM. Site. Disponível em: <https://bitcoinmarketingteam.com/>. Acesso em: 03 set. 2018.

[5] EOS. Frequently Asked Questions: here are some common questions about EOS and EOSIO. Disponível em: <https://eos.io/faq>. Acesso em: 03 set. 2018.

[6] De acordo com análise do mercado.

[7] Moedas fiats são moedas sem lastros, de curso legal. Sua aceitação é muitas vezes imposta por regulamentação governamental. Ex.: dólar, euro, real.

[8] COIN GOVERNANCE SYSTEM. Site. Disponível em: <https://cgs.vote/>. Acesso em: 05 set. 2018.

Capítulo 5

[1] Insutrtech são empresas do setor de seguros que, com uso intensivo da tecnologia em seus processos, visam desburocratizar, baratear o custo e aumentar a capilaridade dos serviços de seguros.

[2] Fonte: BRINKER, Scott. The Blockchain Marketing Technology Landscape. Chiefmartec, Sep. 26, 2017.

[3] Fonte: Coin Schedule. Cryptocurrency ICO Stats 2018. Disponível em: <https://www.coinschedule.com/stats.html>. Acesso em: 01 nov. 2018.

[4] <https://adhive.tv/#summary>.

[5] STACK EXCHANGE. How could the bitcoin protocol be changed? Has this ever occurred? Bitcoin questions, s.d. Disponível em: <https://bitcoin.stackexchange.com/questions/3945/how-could-the-bitcoin-protocol-be-changed-has-this-ever-occurred#comment4983_3948>. Acesso em: 03 set. 2018.

[6] BITCOIN WIKI. Economic majority. Disponível em: <https://en.bitcoin.it/wiki/Economic_majority>. Acesso em: 03 set. 2018.

[7] BITCOIN.ORG. Bitcoin Developer Guide. Consensus Rule Changes. Disponível em: <https://bitcoin.org/en/developer-guide#consensus-rule-changes>. Acesso em: 03 set. 2018.

[8] DECRED. Decred Documentation. Overview. Disponível em: <https://docs.decred.org>. Acesso em: 03 set. 2018.

[9] CARBONVOTE. Site. Disponível em: <http://carbonvote.com/>. Acesso em: 03 set. 2018.

[10] Termo derivado do Princípio da Composicionalidade, onde o significado de uma expressão complexa é totalmente determinado por sua estrutura e os significados de seus constituintes. Uma vez que se metodiza o que as partes significam e como elas são ordenadas juntas, não há mais margem para outro significado do todo.

[11] Entrevista de Dunbar à NPR, 2011. DON'T Believe Facebook; You Only Have 150 Friends. NPR, June 05, 2011. Disponível em: <https://www.npr.org/2011/06/04/136723316/dont-believe-facebook-you-only-have-150-friends>. Acesso em: 03 set. 2018.

[12] DIGIX. Site. Disponível em: <https://digix.zendesk.com/hc/en-us>. Acesso em: 03 set. 2018.

[13] NEM. Site. Disponível em: <https://nem.io/>. Acesso em: 03 set. 2018.

[14] DASH BUDGET PROPOSAL VOTE TRACKER. Site. Disponível em: <https://dashvotetracker.com>. Acesso em: 03 set. 2018.

[15] LEE, Charlie. Litecoin price, tweets, and conflict of interest. Reddit, jan. 2018. Disponível em: <https://www.reddit.com/r/litecoin/comments/7kzw6q/litecoin_price_tweets_and Acesso em: 05 set. 2018.

[16] Santos Dumont é reconhecido no Brasil e na França como o inventor do avião e esta é somente uma entre as inúmeras hipóteses que explicariam seu suicídio.

Capítulo 6

[1] ESTCOIN Backs Down as Banking Authorities Bully Estonia. Coinnews, Mar. 06, 2018. Disponível em: <http://www.coinnews.life/events/estcoin-backs-down-as-banking-authorities-bully-estonia/>. Acesso em: 03 set. 2018.

[2] HIGH Speed Traders Are Taking Over Bitcoin. Bloomberg, Jan. 16, 2017. Disponível em: <https://www.bloomberg.com/news/articles/2017-01-16/high-speed-traders-are-taking-over-bitcoin-as-easy-money-beckons>. Acesso em: 03 set. 2018.

[3] BLOCKGEEKS. 5 High Profile Cryptocurrency Hacks. Disponível em: <https://blockgeeks.com/guides/cryptocurrency-hacks>. Acesso em: 03 set. 2018.

[4] JAPANESE crypto exchange says US$400 million in NEM currency lost. South China Morning Post, Jan. 27, 2018. Updated Feb. 06, 2018. Disponível em: <http://www.scmp.com/business/banking-finance/article/2130804/japanese-crypto-exchange-says-us400-million-nem-currency>. Acesso em: 03 set. 2018.

[5] BINANCE Dexathon. Binance, Mar. 16, 2018. Disponível em: <https://medium.com/binanceexchange/binance-dexathon-845dc0cbfffe>. Acesso em: 03 set. 2018.

[6] CRYPTOECONOMICS. Site. Disponível em: <http://cryptoeconomics.com.au/>. Acesso em: 03 set. 2018.

[7] Fonte: COINMARKETCAP. Site. Disponível em: <https://coinmarketcap.com/>. Acesso em: 01 nov. 2018.

[9] Ibid.

[9] STEEM TOOLS. Site. Disponível em: <http://steemtools.com>. Acesso em: 04 set. 2018.

Capítulo 7

[1] Ataque 51% acontece quando o poder de consenso da rede se concentra em um participante ou grupo de poucos nodos, permitindo que essa capacidade computacional valide transações inválidas e afete a integridade do blockchain.

[2] GOING to War: Monero Sticks to Anti-ASIC Guns with emergency Software Update. CCN, Mar. 26, 2018. Disponível em: <https://www.ccn.com/monero-sticks-to-anti-asic-guns-with-emergency-software-update>. Acesso em: 04 set. 2018.

[3] GUSSON, Cassio. Vitalik Buterin é contra hard fork para impedir a Bitmain na Ethereum. Criptomoedas Fácil, 10 abr. 2018. Disponível em: <https://www.criptomoedasfacil.com/vitalik-buterin-e-contra-hard-fork-para-impedir-a-bitmain-na-ethereum/>. Acesso em: 04 set. 2018.

[4] Dados analisados do CoinmarketCap de abril de 2018. Em maio a Verge sofreu um ataque 51% e esses resultados foram alterados radicalmente. Foi mantido o texto para exemplificação dos objetivos das DOs.

[5] VERGE. Site. Disponível em: <http://vergecurrency.com/>. Acesso em: 04 set. 2018.