FIAP ON

BLOCKCHAIN ADVANCED

BLOCKCHAIN X *CRIPTOMOEDAS*

HENRIQUE POYATOS

5

LISTA DE FIGURAS

SUMÁRIO

5 BLOCKCHAIN X CRIPTOMOEDAS

Falemos de outros Criptoativos além do Bitcoin e como eles estão propondo novos modelos de funcionamento, algoritmos de consenso e até mesmo de *blockchains*, em busca de modelos mais escalonáveis e eficientes.

O bitcoin é apenas a primeira entre as várias experiências econômicas a ser bem-sucedida em três coisas: conseguir simular uma escassez artificial de um bem digital, impedir que algo digital pudesse ser duplicado e resolver o problema do gasto duplo em uma rede descentralizada. No entanto, sua origem é libertária e baseada em software livre (seu código-fonte está publicado no GitHub, em <https://github.com/bitcoin/bitcoin>), permitindo a qualquer um baixá-lo, fazer mudanças no código de acordo com suas necessidades e redistribuí-lo, o princípio básico da filosofia do software livre.

Sendo assim, aqueles que por alguma razão discordam das regras estabelecidas pela rede Bitcoin podem, simplesmente, usar seu código-fonte como referência, fazer as mudanças que julgar necessárias e começar seu próprio criptoativo e sistema financeiro.

E isso já aconteceu, centenas ou talvez milhares de vezes. Existem hoje milhares de criptoativos no mercado, embora nem todos tenham o código-fonte do Bitcoin como origem. Na verdade, o *blockchain* do Bitcoin possui limitações reconhecidas, como:

- **Pouco espaço em cada bloco para armazenar transações:** por armazenar um número limitado de transações por vez (cada bloco pode armazenar apenas 1MB em transações), o alto interesse pelo criptoativo provocou grandes “congestionamentos” na rede, e uma transação que não pagasse uma taxa de rede significativa (uma espécie de cobrança de DOC/TED) aos mineradores, poderia ter a validação de sua transação adiada em muitas horas ou até mesmo dias.
- **Tempo alto para a validação de cada bloco:** por ser fixado em dez minutos, impossibilitaria seu uso para, como dizem os críticos, “pagar um cafezinho na cafeteria”, ou seja, ele é inviável em usos que precisem de uma confirmação em poucos segundos;

- **Pouca performance ou escalabilidade:** o próprio modelo de *blockchain* não foi concebido para ter alta performance como bancos de dados que funcionem de maneira distribuída; na verdade, foi concebido para fazer o oposto: uma rede de *blockchain* possui milhares de computadores fazendo as mesmas tarefas e realizando cópias dos mesmos dados, sendo assim, jamais atingirá a performance de redes de transações dos cartões de crédito. Segundo Vermeulen (2017), enquanto a rede Bitcoin é capaz de processar até quatro transações por segundo, a **Paypal** seria capaz de processar 193 no mesmo tempo, enquanto a **Visa** é capaz de processar 1.667 transações por segundo, em média.
- **Sigilo parcial:** embora a segurança do sistema seja garantida pela criptografia, os dados presentes no bloco não são criptografados. As informações são armazenadas em aberto, sendo possível acompanhar o bitcoin desde sua geração, passando por todas as carteiras até o presente momento. Sendo assim não existe, nesse caso, “sigilo bancário”: todas as movimentações são públicas, para quem quiser olhar. O que é mantido em segredo é a identidade dos donos das carteiras, que são identificados com um identificador alfanumérico longo, a chave pública do par de chaves. O sigilo na rede bitcoin é, portanto, parcial, pois o proprietário da carteira é anônimo, mas suas transações são todas conhecidas. É possível identificar o dono da carteira ao cruzar informações adicionais: por exemplo, um e-commerce no qual tenha feito compras pagando diretamente com bitcoins; para o e-commerce, portanto, a minha identidade como dono de carteira é revelada.
- **Alto custo para a validação do bloco:** o algoritmo baseado em prova de consenso, em que o *hash* que valida o bloco deve ser “adivinhado” após milhões de tentativas por milhares de fazendas de mineração diferentes, faz com que a energia elétrica dispendida para essa tarefa ultrapasse o gasto energético da maioria das nações africanas, ou seja, a rede de *bitcoin* consome mais energia elétrica do que países inteiros. Minerar bitcoins não é exatamente sustentável do ponto de vista ecológico, digamos assim.

Vários grupos que considerem um ou mais desses cincos fatores levantados como problemas sérios a serem resolvidos estão criando seus próprios criptoativos

com propostas diferentes: blocos com mais espaço para a validação de transações, tempos mais curtos para a validação dos blocos, *blockchain* com arquiteturas diferentes que podem “embaralhar” as transações para que seus participantes tenham mais sigilo, outras iniciativas visando aumentar o número de transações por segundo e até outros grupos propondo novos algoritmos de consenso, como é o caso do *proof of stake* (POS), cujo modelo dispensa ASICs que gastam tanta energia elétrica.

Dentre os milhares de criptoativos, existem várias iniciativas tecnologicamente interessantes que propõem mudanças como as relatadas, enquanto outras (provavelmente 90% delas) representam apenas esquemas fraudulentos de pirâmide que visam gerar riqueza aos seus criadores, lesando centenas de milhares de pessoas no processo. Nas próximas páginas, vamos abordar alguns criptoativos que merecem destaque.

5.1 Bitcoin Cash

O Bitcoin Cash (BCH) é um excelente exemplo de liberdade de ações que projetos abertos mantidos por comunidades proporcionam. O criptoativo nasceu de um desacordo da comunidade sobre os rumos que o projeto do Bitcoin deveria tomar para resolver os problemas de congestionamento da rede e as altas taxas de rede que os usuários estavam pagando como consequência disso.

O Bitcoin enfrenta um sério problema de escalabilidade, pois o volume de transações que consegue processar em cada bloco (que demora 10 minutos) é muito baixo dado o crescente interesse no uso desse criptoativo. O tamanho de seu bloco é de 1MB (um megabyte) e qualquer tentativa de aumento necessitaria um consenso de todos os participantes de rede, ou seja, milhares de partes interessadas. Se o consenso não for atingido, há um risco de a rede partir em duas (*splits*), fazendo com que a moeda se torne duas, perdendo força computacional e valor de mercado.

Uma parte razoável da comunidade acreditava que o tamanho do bloco de transações do Bitcoin deveria ser radicalmente aumentado, passando de 1MB para 2MB, 4MB ou até mesmo 8MB. No entanto, tal alteração não seria compatível com a versão de 1MB que a rede roda normalmente, exigindo um ***hardfork*** e a necessidade de consenso mencionada.

Embora pareça banal, tal mudança poderia trazer outras consequências para o delicado equilíbrio da rede, e a maior parte da comunidade preferiu a implementação do *Segregated Witness*, um ***softfork*** que retirou parte das informações transacionais do corpo do bloco e, na prática, possibilitou aumentar o armazenamento de 1MB para 1.4MB. Além do SegWit, a abordagem das ***sidechains*** para resolver o problema de escalabilidade foi o desejo da maioria, como a iniciativa da ***Lightning Network***.

O conservadorismo da maioria irritou uma parte da comunidade que resolveu pegar o código-fonte original do Bitcoin, fazer as alterações que julgava necessárias e, diferentemente de outros criptoativos que começam seu "*blockchain* do zero" ou de um bloco gênese, decidiram que o Bitcoin Cash seria um *fork* do *blockchain* do Bitcoin: a partir do bloco 478558, o *blockchain* bifurcou, minerando **Bitcoin** em uma direção e **Bitcoin Cash** em outra.

Figura 5.1 – Logo do Bitcoin Cash
Fonte: HUFFMAN (2017)

Na prática, as "moedas" foram duplicadas: quem tinha 1 bitcoin em uma carteira naquele momento, também tinha um 1 bitcoin cash no mesmo endereço de carteira. Curiosamente, não houve uma desvalorização expressiva do Bitcoin na época, cujo preço se manteve mais ou menos estável.

Como alteração imediata, o tamanho do bloco do Bitcoin Cash é de 8MB, oito vezes mais do que do projeto original. Além disso, alterações no algoritmo de ajuste de dificuldade da mineração foram necessárias, permitindo que mineradores pudessem migrar facilmente de Bitcoin para Bitcoin Cash.

Em novembro de 2018, houve novamente um impasse, dessa vez na comunidade do Bitcoin Cash. De um lado, parte da comunidade liderada por **Roger**

Ver, conhecido como ***Bitcoin Jesus,*** e, de outro lado, o polêmico **Craig Wright**, australiano que alega ser Satoshi Nakamoto (e foi apelidado pela comunidade de Faketoshi). O *fork* deu origem ao Bitcoin ABC de Roger Ver (que posteriormente ganhou o direito de continuar sendo chamado de Bitcoin Cash) e ao Bitcoin SV (*Satoshi Vision*) de Craig Wright.

5.2 Bitcoin Gold

Uma outra parte da comunidade Bitcoin acredita que, com o aumento crescente do *hashrate* e a necessidade de se minerar com ASICs cada vez mais poderosas, a rede de mineração está cada vez mais concentrada em poucas partes que possuem recursos financeiros para tal. Dessa maneira, tais partes poderiam impor seus interesses políticos e econômicos, arruinando assim a característica mais importante de um *blockchain*, a descentralização e o equilíbrio de forças dos participantes.

Figura 5.2 – Logo do Bitcoin Gold
Fonte: BITCOINGOLD (2018)

Vencida pela vontade da maioria, essa parte da comunidade repetiu o processo feito pelo Bitcoin Cash, alterando o código-fonte para atender a suas necessidades e minerando um bloco do *blockchain* do Bitcoin de número 491407 em outra direção, bifurcando novamente a rede de blocos. Mais uma vez, as carteiras foram duplicadas e quem tinha bitcoins na ocasião possuía também Bitcoin Gold (BTG).

Segundo BitcoinGold (2017) em seu *paper*, a principal mudança realizada é a troca do algoritmo de prova de trabalho de SHA256 (usado no Bitcoin e BitcoinCash) para EquiHash. Tal mudança tira a obrigatoriedade de minerar usando ASICs, dando uma chance real àqueles que queiram minerar com GPUs (placas de vídeo) como nos velhos tempos, tornando o processo de mineração mais democrático.

5.3 Litecoin

O tempo de confirmação de transações dos blocos de Bitcoin sempre foi fixado em dez minutos, o que impossibilita que seja usado para pequenas transações. O alto tempo para confirmação não permite pagar um cafezinho com bitcoins, por exemplo. O volume máximo de 21 milhões de bitcoins torna a moeda deflacionária, fazendo com que pontos de centavos tenham muito poder de compra, tornando difícil trabalhar com frações dela (o bitcoin pode ser fracionado até a oitava casa decimal mas, convenhamos, é difícil usá-lo como unidade de medida quando algo vale 0,00000001 bitcoin ou 1 satoshi).

Se o Bitcoin é o ouro digital, o projeto do Litecoin (LTC) iniciado apenas dois anos depois pelo ex-funcionário da Google, Charles Lee, se propõe a ser a prata. Criado a partir do código-fonte do Bitcoin, a principal mudança foi no algoritmo de prova de trabalho e o tempo de confirmação fixado em dois minutos e meio.

Figura 5.3 – Logo do Litecoin
Fonte: LITECOININFO (2018)

A substituição no algoritmo de prova de trabalho também tornou mais difícil e caro criar ASICs para minerar a moeda, diminuindo a escalada de equipamentos para essa tarefa e, assim, inibindo os altos investimentos e a necessidade de taxas de rede, embora ela, segundo a BitinfoCharts (s.d.), tenha chegado a uma média recorde de 1,5 dólar no final de 2017.

Diferente do Bitcoin cujo limite foi fixado em 21 milhões de unidades, o projeto Litecoin estabeleceu como limite 84 milhões de unidades, ou seja, 4 vezes mais.

Por ser uma comunidade menor e mais ousada, o projeto se tornou um excelente piloto para melhorias que posteriormente foram incorporadas no Bitcoin. O projeto foi o primeiro entre os principais criptoativos a implementar o SegWit e, segundo Russell (2017), foi a primeira a realizar uma transação na *Lightning Network*.

5.4 Ripple

O Ripple é uma proposta muito diferente das demais sob diversos aspectos. Para começar, seu controle é centralizado na empresa que o criou, a Ripple Labs, Inc. Seu real valor é ter estabelecido um sistema de pagamentos do tipo RTGS (*Real-time gross settlement*), que são sistemas que transferem remessas de dinheiro de um banco a outro em tempo real com segurança e de maneira irrevogável. O sistema da empresa se coloca como uma opção de transferência financeira muito mais rápida, barata e confiável do que Western Union (o sistema de correio dos EUA) e a rede SWIFT, usada tradicionalmente para remessas internacionais.

Figura 5.4 – Logo do Ripple
Fonte: WIKIMEDIA COMMONS (2014)

No sistema de pagamentos Ripple, trafegam *tokens* chamados de ripples (XRP). Segundo AZIZ (s.d.), a diferença entre uma “criptoativo” (também chamado de criptomoeda ou *altcoin*) e o token é estrutural: enquanto “criptoativos” possuem seu próprio *blockchain* em separado, *tokens* operam no topo de uma *blockchain* e podem ser gerados mais facilmente, compartilhar um mesmo *blockchain* com outros *tokens* e são utilizados na criação de aplicações descentralizadas.

Outra controvérsia é o fato de que os *tokens* ripples (XRP) são “pré-minerados”; eles não são gerados pelo processo de mineração e gradualmente colocados em uso, eles já estão disponíveis. De acordo com a CoinMarketCap (2018b), existem mais de 39 bilhões de ripples disponíveis.

A empresa e seu token XRP ganhou o noticiário de 2018 com algumas notícias ao fazer generosas doações a ONGs nos EUA. Segundo Elkins (2018), o próprio site da **DonorsChoose.org**, a ONG DonorsChoose.org, responsável por intermediar doações de pessoas para professores e salas de aulas em todo o território dos Estados Unidos, recebeu uma doação em XRP equivalente a 29 milhões de dólares, sendo a maior doação nos 18 anos de funcionamento da ONG.

Além de um ator muito bem-sucedido em Hollywood, **Ashton Kutcher** também é um notório investidor em tecnologias. Tendo financiado no passado empresas como o Airbnb, Uber, Foursquare, Skype e Soundcloud, seu atual fundo de investimento em tecnologia, o **Sound Ventures**, está agora financiando a Ripple. O ator surpreendeu a todos ao doar ao vivo no EllenShow o equivalente a quatro milhões de dólares em XRP para a **The Ellen DeGeneres Wildlife Fund**.

Figura 5.5 – Kutcher e Oseary, da Sound Ventures, no momento da doação
Fonte: DAILY MAIL (2018)

Kutcher ironiza o momento da doação, mencionando que “geralmente as pessoas doam com aqueles cheques gigantes”, mas que ele iria fazer digitalmente, mostrando o quanto era fácil e rápido transferir dinheiro de ponta a ponta. Percebe que, além de apoiador de causas nobres, o ator também é capaz de uma brilhante jogada de *marketing* – os usuários de criptoativos também agradecem.

5.5 Dash

Por se tratar de um *blockchain* aberto, o Bitcoin mantém apenas a identidade de seus usuários em sigilo, pois cada carteira é identificada com um número hexadecimal. No entanto, os saldos de todas as carteiras e transações realizadas ficam totalmente abertos para quem quiser ver.

O criptoativo Dash (DASH) propõe um tipo diferente de *blockchain* que mantém o saldo e histórico de transações em sigilo, além de transações que podem ser instantaneamente confirmadas. Outro diferencial é um modelo de incentivo que não recompensa apenas os mineradores, mas também os *masternodes* responsáveis por validar e armazenar o *blockchain* e desempenhar um papel importante no ecossistema.

Figura 5.6 – Logo do Dash
Fonte: DASH (2018)

5.6 Monero

O criptoativo Monero (XMR) também preza pelo sigilo das transações feitas, como o Dash, realizando o chamado ofuscamento de *blockchain*: uma única transação ponto a ponto é substituída por várias transações e o dinheiro muda de mãos diversas vezes, mesmo entre carteiras que possuam seu dinheiro "estacionado". Esse "embaralhamento" de transações torna a rastreabilidade quase impossível, em um processo muito parecido com a rede Onion utilizada pelo navegador Tor.

Tais moedas possuem fungibilidade, ou seja, suas unidades podem ser facilmente substituídas por outras; diferentemente do Bitcoin cujas unidades podem ser rastreadas facilmente desde sua criação e podem ser marcadas para serem rejeitadas por outros usuários envolvidos em atividades suspeitas, isso não pode ser realizado no Dash ou Monero, tornando-as mais atraentes para pessoas envolvidas em atividades ilícitas.

Figura 5.7 – Logo do Monero
Fonte: MONERO (2018)

5.7 Iota

Poucos criptoativos estão propondo mudanças tão ousadas quanto a IOTA. Sua rede foi concebida para viabilizar um conceito conhecido como *Machine Economy*, um futuro no qual teremos transações M2M (*machine-to-machine*, ou máquina para máquina) de maneira totalmente autônoma.

Pegue como exemplo a geração de energia elétrica: já se estuda no Brasil o que é uma realidade em alguns países, onde temos pequenos produtores de energia elétrica (com seus painéis solares ou outras fontes renováveis de energia) gerando sua própria energia e, quando há energia excedente, devolvendo essa energia ao *grid* energético, fazendo o relógio de consumo girar ao contrário.

Vislumbra-se, no entanto, uma realidade diferente, na qual fosse possível contratar essa energia elétrica excedente diretamente do pequeno produtor, que está praticando um preço de quilowatts por hora (kWh) diferenciado. No entanto, isso aconteceria de maneira totalmente automatizada: o painel solar do pequeno produtor que possui uma carteira de dinheiro integrada (para receber as receitas de venda de energia), enquanto o relógio de minha residência também possui sua própria carteira e, com uma certa inteligência artificial, aproveita esses “preços dinâmicos” da energia, contratando e pagando por ela de maneira autônoma.

O que o projeto IOTA defende é que essas “microtransações” realizadas entre os sensores seriam totalmente inviáveis na rede do Bitcoin, em que o incentivo financeiro pela mineração e o modelo de prova de trabalho exigindo cada vez mais processamento e energia elétrica gerou uma escalada nos custos, e as transações na rede Bitcoin exigindo taxas de rede cada vez mais dispendiosas.

Além disso, a arquitetura atual do *blockchain* em uma única corrente em que todos os mineradores validam os mesmos blocos não teria a escalabilidade necessária para uma rede de sensores que, segundo a Gartner (2017), deve ultrapassar 11 bilhões de sensores em 2018 e outras previsões (EICHMANN, 2018) falam em 50 bilhões de dispositivos conectados à Internet em 2020.

Figura 5.8 – Logo do IOTA
Fonte: WIKIMEDIA COMMONS (2018)

A IOT propõe uma arquitetura totalmente revolucionária para validação das informações. Em vez de um *blockchain* de uma única corrente sequencial, os blocos formam um “emaranhado”, conhecido como *The Tangle*:

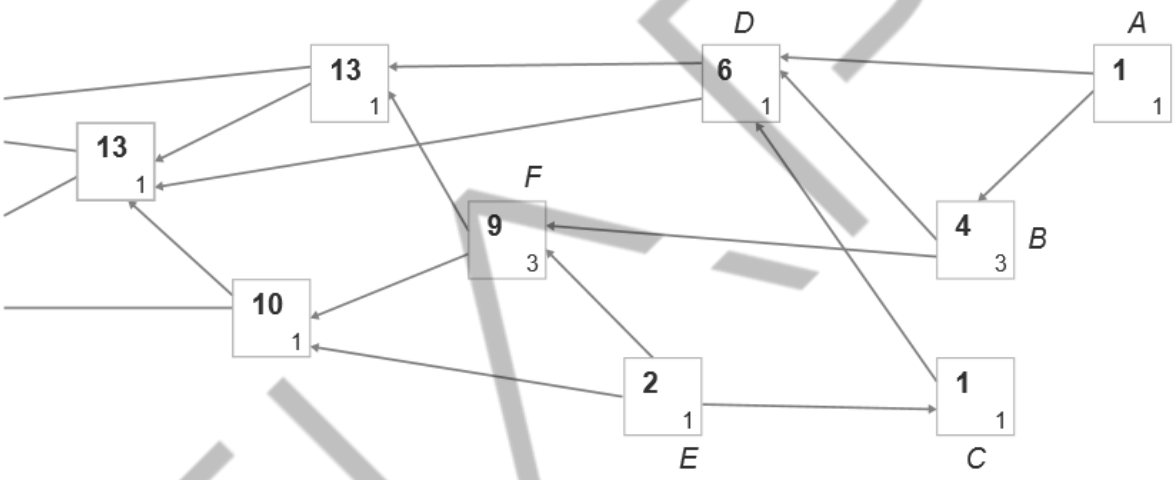

Figura 5.9 – Blockchain no formato Tangle ou “emaranhado”
Fonte: POPOV (2018)

Sua estrutura é baseada em um grafo acíclico dirigido (*Directed Acyclic Graph* ou DAG) em que, para qualquer vértice v, não há nenhuma ligação dirigida começando e acabando em v. Na prática, esse tipo de estrutura permite que quanto mais pessoas estejam usando a rede, mais validações aconteçam, trazendo a desejada escalabilidade; não há um gargalo como no *blockchain* tradicional, em que um número maior de mineradores não aumenta a performance da rede de consenso; no IOTA, quanto mais participantes, maior a performance.

Outra grande quebra de paradigma é a eliminação do papel dos mineradores. Na rede IOTA, para realizar transações na rede, o participante precisa fazer uma pequena quantidade de trabalho computacional, verificando duas transações anteriores, ou seja, o papel de validação de blocos é intrinsicamente ligado ao usuário da rede.

Cada participante possui os mesmos incentivos e recompensas: para realizar uma transação no Tangle, duas transações anteriores precisam ser validadas para que eu ganhe o direito de ter minha própria transação validada por outros. Ao implementar esse sistema de validação "*pay-it-forward*", não há a necessidade de recompensas financeiras, tornando todas as transações de IOT livre de taxas, o que torna as "microtransações" entre máquinas viável.

Portanto, não há a necessidade de um minerador, aliás, como acontece com a Ripple, todos os *tokens* IOTA já foram gerados no bloco gênese (o primeiro bloco da rede) e existem para todo e sempre 2,779,530,283,277,761 tokens.

A seguir, as vantagens do IOT segundo seus desenvolvedores:

- **Alta escalabilidade:** ao aumentar a atividade da rede, se diminui o tempo de validação dos blocos;
- **Requisitos de hardware baixos:** a rede foi desenvolvida para sensores IoT participarem;
- **Transações livre de taxas:** um centavo enviado sempre será um centavo recebido;
- **Segurança das informações:** os dados são codificados para garantir segurança;
- **Transações *off-line*:** não há necessidade de conectividade constante, uma realidade para vários sensores IoT;
- **Imunidade quântica:** o IOT usa assinaturas especiais que seriam imunes à próxima geração da computação (o processamento quântico);

Como é o caso de vários criptoativos, o IOTA está em fase de prova de conceito e seus desenvolvedores preveem que a viabilidade seja atingida em meados de 2018.

5.8 Zcash

O criptoativo ZCASH (ZEC) tem uma proposta de *blockchain* que mantém o sigilo do saldo nas carteiras e do histórico de transações, algo que não difere muito

de outras como DASH ou Monero. Seu destaque aqui se dá graças ao seu relacionamento com o povo venezuelano.

Figura 5.10 – Logo do ZCASH
Fonte: ZCASH (2018)

Quando a economia de um país vai mal, sua moeda fiduciária sofre uma violenta desvalorização que impacta diretamente no dia a dia de sua população. Rapidamente os indivíduos começam a se proteger fazendo reserva de valor em outro tipo de ativo, como o ouro e o dólar.

O Brasil sofreu com o problema por anos durante boa parte das décadas de 1980 e 1990; mais recentemente a Argentina passa por um processo parecido e é sabido que muitos argentinos procuraram proteger seus patrimônios convertendo pesos argentinos em dólares, reais ou mesmo em bitcoins.

Para o povo venezuelano, no entanto, essas opções não são viáveis. A crise do país se mostra mais aguda que a da Argentina e a moeda estatal, o bolívar, passa por uma desvalorização ainda mais violenta. Embora não seja ilegal para um venezuelano possuir dólares, na prática a moeda americana é de difícil acesso a eles.

Embora o governo venezuelano tenha criado seu próprio criptoativo lastreado em petróleo (chamado de **petro**) como uma maneira de contornar as sanções impostas pelos Estados Unidos ao país, o povo venezuelano não confia mais nesse ativo do que confia no bolívar, pois ambos possuem controle estatal e estão sujeitos aos interesses do regime.

Segundo Del Castillo (2018), por meio de uma Exchange conhecida como AirTM, 168 mil venezuelanos têm usado a moeda ZCASH como intermediária na conversão entre bolívares e dólares americanos. Sua propriedade de não rastreabilidade das transações a torna ideal para os venezuelanos se protegerem de seu regime autoritário.

5.9 Ethereum

Desde sua concepção, a proposta da rede Ethereum é audaciosa. A ideia seria responder à pergunta: e se o dinheiro fosse programável? E se uma nota de dinheiro pudesse vir atrelada às suas próprias regras ou condições?

Mantido pela Ethereum Foundation, uma organização sem fins lucrativos na Suíça, o Ethereum é uma plataforma descentralizada que roda contratos inteligentes, permitindo que aplicações rodem exatamente conforme foram programadas previamente, sem a possibilidade de atraso, censura, fraude ou interferência de terceiros (ETHEREUM, s.d.).

Figura 5.11 – Logo do Ethereum
Fonte: ETHEREUM (s.d.)

Para manter o incentivo de mineração da rede, foi criado um token chamado ether para viabilizar seu funcionamento. Atualmente, o ether é o segundo maior criptoativo em participação de mercado, segundo o CoinMarketCap.com.

Não vamos nos estender muito nesse assunto no momento: nosso terceiro capítulo será inteiramente dedicado ao **Ethereum** e seus *Smart Contracts*.

5.10 Dogecoin

O criptoativo Dogecoin (DOGE) merece uma menção honrosa não por possuir um diferencial como os outros destacados por aqui, mas justamente por não possuir nenhum. A moeda foi criada em 2013 e seu mote era... ter como mascote um meme de um cachorro da raça Shiba Inu. Apenas isso. Alguma dúvida? Visite o site oficial do projeto (http://dogecoin.com/) e comprove você mesmo.

Figura 5.12 – Logo do Dogecoin
Fonte: DOGECOIN (2018)

Apesar de sua mediocridade e não receber qualquer contribuição de seus desenvolvedores por mais de um ano, segundo a CoinMarketCap (2018a), durante a "corrida do final de 2017" sua unidade chegou a quase dois centavos de dólar, com um valor de mercado que chegou a dois bilhões de dólares. Seu valor saltou de US$ 0,003641 de 15 de dezembro de 2017 para o pico de US$ 0,01753 em 8 de janeiro de 2018, ou seja, o criptoativo passou a valer quase cinco vezes mais em apenas 24 dias de maneira puramente especulativa, sem qualquer razão sustentável para sua valorização.

O Dogecoin é um de milhares de criptoativos que provam que as pessoas não fazem a menor ideia de onde estão colocando seu dinheiro. Seu próprio criador, o australiano Jackson Palmer escreveu três dias após o recorde da cotação um artigo intitulado "***My Joke Cryptocurrency Hit $2 Billion and Something Is Very Wrong***" (em tradução livre "minha 'criptomoeda' de zoeira atingiu dois bilhões e tem algo muito errado nisso", vide Palmer (2018)).

Conforme sua reflexão, muitos investidores inexperientes compraram outros ativos de baixo custo como o Dogecoin na esperança que eles acompanhassem a trajetória meteórica do Bitcoin e esse “efeito manada” resultou na escalada de preços insustentáveis, mesmo para projetos sólidos como o Bitcoin. Quando a correção veio (e ela sempre vem), o resultado foram muitos mortos e feridos.

Conforme já dito antes neste conteúdo, procure conhecer o criptoativo no qual pretende investir. Poucos deles possuem valor tecnológico e razões reais de existência, e são esses que possuem as melhores chances de vingar no futuro; os demais são apenas esquemas de pirâmide que podem desmoronar a qualquer momento.

DICA: Não invista no que você não conhece!

REFERÊNCIAS

AZIZ. **Coins, Tokens & Altcoins: What's the Difference?** Disponível em: <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>. Acesso em: 21 jul. 2020.

BITCOINGOLD. **BITCOINGOLD – Make Bitcoin decentralized again.** 2015. Disponível em: <https://bitcoingold.org/>. Acesso em: 21 jul. 2020.

BITCOINGOLD. **BITCOINGOLD Roadmap.** 2017. Disponível em: <https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf>. Acesso em: 21 jul. 2020.

BITINFOCHARTS. **Litecoin Avg. Transaction Fee historical chart.** 2017. Disponível em: <https://bitinfocharts.com/comparison/litecoin-transactionfees.html>. Acesso em: 21 jul. 2020.

COINDANCE. **Bitcoin Block Details.** Disponível em: <https://coin.dance/blocks>. Acesso em: 21 jul. 2020.

COINMARKETCAP. **Dogecoin.** 2015. Disponível em: <https://coinmarketcap.com/currencies/dogecoin/>. Acesso em: 21 jul. 2020.

COINMARKETCAP. **Ripple.** 2015. Disponível em: <https://coinmarketcap.com/currencies/ripple/>. Acesso em: 21 jul. 2020.

DAILY MAIL. **What is Ripple? Cryptocurrency explained after Ashton Kutcher donates $4 million to Ellen DeGeneres.** 2015. Disponível em: <http://www.dailymail.co.uk/sciencetech/article-5767579/What-Ripple-Cryptocurrency-explained-Ashton-Kutcher-donates-4-million-Ellen-DeGeneres.html>. Acesso em: 21 jul. 2020.

DASH. **DASH.org**. 2015. Disponível em: <https://www.dash.org/>. Acesso em: 21 jul. 2020.

DEL CASTILLO, Michael. **The Anti-Petro? Zcash Throws Venezuelans a Lifeline.** 2015. Disponível em: <https://www.coindesk.com/anti-petro-zcash-throwing-venezuelans-lifeline/>. Acesso em: 21 jul. 2020.

ELKINS, Kathleen. **Ripple donates $29 million after nonprofit's founder 'dared' himself to ask.** 2015. Disponível em: <https://www.cnbc.com/2018/03/28/ripple-donates-29-million-after-donorschoose-org-founder-dared-himself-to-ask.html>. Acesso em: 21 jul. 2020.

ETHEREUM. **Ethereum Web Site.** Disponível em: <https://ethereum.org/>. Acesso em: 21 jul. 2020.

HANNAERT, Raphael. **IOTA: The Catalyst for a Powerful Machine-to-Machine Economy.** 2017. Disponível em: <https://medium.com/bitcoin-center-korea/iota-the-

catalyst-for-a-powerful-machine-to-machine-economy-aaecea7b1255>. Acesso em: 21 jul. 2020.

HUFFMAN, Zane. **Price of Bitcoin Cash Soars to All Time USD High of $2700.** 2017. Disponível em: <https://themerkle.com/price-of-bitcoin-cash-soars-to-all-time-usd-high-of-2700/>. Acesso em: 21 jul. 2020.

LITECOININFO. **File:Full Logo L.png.** 2015. Disponível em: <https://litecoin.info/index.php/File:Full_Logo_L.png>. Acesso em: 21 jul. 2020.

MCMILLAN, Robert. **Ex-Googler gives the world a better bitcoin.** 2013. Disponível em: <https://www.wired.com/2013/08/litecoin/>. Acesso em: 21 jul. 2020.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2005. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 21 jul. 2020.

PALMER, Jackson **My Joke Cryptocurrency Hit $2 Billion and Something Is Very Wrong.** 2015. Disponível em: <https://motherboard.vice.com/en_us/article/9kng57/dogecoin-my-joke-cryptocurrency-hit-2-billion-jackson-palmer-opinion>. Acesso em: 21 jul. 2020.

POPOV, Serguei. **The Tangle.** 2015. Disponível em: <https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.5.2.pdf>. Acesso em: 21 jul. 2020.

POPPER, Nathaniel. **Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.** Nova York: Harper Paperbacks, 2016.

REDMAN, Jamie. **Fork Watch: Block 478558 Initiates 'Bitcoin Cash' Split – First Blocks Now Mined**. 2017. Disponível em: <https://news.bitcoin.com/fork-watch-first-bitcoin-cash-block-mined/>. Acesso em: 21 jul. 2020.

RUSSELL, Rusty. **Major Milestone: The First Lightning Payment on Litecoin pays from Zurich to San Francisco.** 2017. Disponível em: <https://blockstream.com/2017/05/11/lightning-on-litecoin.html>. Acesso em: 21 jul. 2020.

VERMEULEN, Jan. **Bitcoin and Ethereum vs Visa and PayPal – Transactions per second.** 2017. Disponível em: <https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html>. Acesso em: 21 jul. 2020.

ZCASH. **ZCASH.** 2015. Disponível em: <https://z.cash/>. Acesso em: 21 jul. 2020.

GLOSSÁRIO

ICO	ICO significa Initial Coin Offerring, ou oferta de moedas inicial, um trocadilho com IPO, prática comum em bolsa de valores. A empresa gera *tokens* e realizada uma oferta pública destes ativos, como uma forma de levantar fundos rapidamente; pode ser usado para crowdfunding legítimos, mas tem sido utilizado frequentemente para fraudes e esquemas de pirâmide.
Rede Onion	Utilizada pelo navegador Tor, esta rede mascara a navegação web de seus usuários fazendo com que a requisição HTTP viaje por dezenas de nós ao redor do mundo, tornando quase impossível rastrear a real origem e destino de uma comunicação.