Faculdade de Engenharia da Universidade do Porto

Blockchain e criptomoedas

Uma breve análise das suas implicações sociais

Projeto FEUP 2018/19 – Mestrado Integrado em Engenharia Informática e Computação:

Manuel Firmino da Silva Torres José Manuel de Magalhães Cruz

Equipa 1MIEIC05_4:

Supervisor: João Correia Lopes Monitora: Sara Fernandes

Estudantes & Autores:

Amanda Silva up201800698@fe.up.pt Francisco Borralho up201806242@fe.up.pt

Diogo Rodrigues up201806429@fe.up.pt Miguel Silva up201806388@fe.up.pt

Diogo Almeida up201806630@fe.up.pt Tiago Rocha up201406679@fe.up.pt

Resumo

As criptomoedas têm vindo a conquistar a atenção pública por razões diversas. Enquanto decorre o debate entre o sistema financeiro "clássico" e o "Tecno-Leviatã" das criptomoedas, tanto no campo ideológico como nas questões técnicas e práticas, a verdade é que a indiferença é improvável, tendo em conta o potencial de um profundo impacte social. O objetivo deste trabalho é explorar a vertente tecnológica e sociológica das criptomoedas e da *blockchain*, a estrutura de dados que as suporta. Para isso, foram analisados relatórios e obras contemporâneas de forma a fundamentar os aspetos expostos. Neste trabalho, são explorados alguns aspetos técnicos das criptomoedas e da blockchain, sendo de seguida apresentados os principais pontos favoráveis e desfavoráveis às duas tecnologias. Por fim, é exposto um conjunto de aplicações, perspetivas e propostas, particularmente direcionadas à tecnologia de *blockchain*, que se espera que persista além de qualquer criptomoeda, das quais será legado, pela sua utilidade transversal a áreas tão relevantes como as finanças, a saúde, a indústria e a investigação científica na criptografia.

Palavras-Chave

Bitcoin; Blockchain; Criptografia; Peer-to-Peer; Moeda; Sistema fracional de reserva; Double Spending; Sociedade; Privacidade

Índice

Lista de figuras

Lista de acrónimos

DDoS	Distributed Denial of Service
P2P	Peer-to-Peer
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Distributed Proof of Work

Glossário

Altura (de um bloco): Número de blocos que precedem esse bloco na *blockchain*. O *genesis block* tem altura zero.

Contrato social: Teoria de organização social que afirma que os indivíduos numa sociedade consentem, implícita ou explicitamente, em perder algumas liberdades e submeter-se a determinada autoridade, em troca da proteção dos seus restantes direitos.

***Dark web*:** Conteúdos da WWW que não estão indexados nos principais motores de busca, e que requerem software, configurações ou autorizações específicas.

DDoS: Ataque informático a uma rede ou máquina, efetuado com um grande conjunto de máquinas que inundam o alvo de solicitações às quais não é capaz de responder.

Moeda *fiat*: Moeda sem valor intrínseco e que não representa propriedade de um bem. Possui valor devido à confiança das pessoas numa entidade (governo ou grupo de pessoas) que assegura a manutenção desse valor.

Moeda-mercadoria: Moeda que possui valor intrínseco, derivado da escassez natural do material de que é constituída e da dificuldade de colocar em circulação (ex.: ouro, prata, sal, e neste caso bitcoins).

Protocolo criptográfico: Protocolo que utiliza métodos criptográficos para providenciar segurança aos interlocutores.

Protocolo de comunicação: Sistema de regras que permite transmitir informação entre duas entidades através da variação de uma quantidade física.

***Ransomware*:** Software malicioso que ameaça publicar ou bloquear de forma permanente o acesso à informação privada da vítima a não ser que um resgate (*ransom*) seja pago.

Reserva bancária: Conjunto de ativos líquidos de um banco, que lhe permite corresponder à necessidade de levantamentos dos depositantes.

SHA256: Função criptográfica de *hashing* que pertence à família de funções SHA-2 (*Secure Hash Algorithm 2*), desenvolvida pela NSA (*National Security Agency*). Para qualquer input, produz uma *hash* de 256 bits.

***Stack*:** Estrutura de dados abstrata sequencial, em que cada elemento possui uma referência ao elemento anterior. Suporta as operações de remoção e inserção de elementos numa das pontas (de forma eficiente) e acesso sequencial aos elementos.

1. Introdução

O presente trabalho tem por objetivo constituir uma revisão bibliográfica sobre os conceitos de *blockchain*, criptomoedas e Bitcoin em particular, reportando-se aos aspetos técnicos de cada uma das tecnologias com a profundidade necessária à compreensão das temáticas subsequentes, nomeadamente das vantagens e desvantagens de cada tecnologia, assim como reflexões, aplicações atuais, potencialidades e perspetivas sobre as mesmas, com especial foco sobre a *blockchain*. Uma vez que se tratam de assuntos relativamente recentes (especificamente, de entre os três conceitos como os conhecemos hoje, a *blockchain* é o conceito mais "antigo", datando de 2008), a bibliografia utilizada é constituída principalmente por publicações em conferências e revistas científicas, notícias de jornais *online*, relatórios e teses. Este relatório foi realizado no âmbito da unidade curricular Projeto FEUP.

2. As criptomoedas

Criptomoedas não são nada mais do que meios de troca; uma forma de realizar uma transação digitalmente.

São, portanto, moedas virtuais completamente independentes do controlo dos governos, ou qualquer autoridade central, entidade, servidor, etc.

Mas se elas são completamente descentralizadas, como é que as transações são mantidas e verificadas? Porque é que elas são tão valiosas? E de onde é que vem o fornecimento dessas moedas?

Para responder a essas perguntas é preciso perceber a tecnologia inerente às criptomoedas: Blockchain. Uma blockchain é uma espécie de livro público que regista e guarda todas as transações que alguma vez aconteceram na rede Peer-to-Peer dessa criptomoeda. E enquanto as transações forem uma constante e continuarem a acontecer esse registo continuará a crescer e a reconstruir-se. Essa é a razão pela qual se chama uma cadeia.

Como esse livro de registos é público para toda a gente, a sua informação vai ser continuamente distribuída e sincronizada digitalmente por todo o mundo. Ela irá partilhar sempre da mesma informação.

Quer isto dizer que, sempre que ocorre uma nova transação, ela irá ser publicamente guardada nesse livro de registos e, quando essa transação acontecer, todos os utilizadores que tiverem uma cópia desse livro serão informados da ocorrência de uma nova transação na rede.

Às pessoas que mantêm o controle de tudo o que se passa na cadeia e que procuram verificar se as transações efetuadas são válidas e reais, chamamos *miners*, ou em português "mineiros". Porquê?

Vejamos o exemplo do que se passa na Bitcoin.

Para que uma transação aconteça é necessário que se tenha uma carteira virtual na rede Bitcoin. Esta carteira incluirá duas chaves: uma privada e uma pública. Uma transação só é dada como verdadeira se for assinada pela chave privada do remetente e uma vez assinada ela está pronta para ser enviada para a cadeia de blocos com a chave pública do mesmo. Esta chave atua como um mecanismo de verificação que confirma que a mensagem do remetente foi, de facto, marcada com a sua chave privada e que esta chave está associada à sua chave pública.

Quando a transação for enviada para a rede Bitcoin, e subsequentemente anunciada a todas as pessoas que fazem a sua manutenção, estes *miners* têm agora a tarefa de usar algoritmos computacionais para verificar a validade de cada transação individual.

Este processo assegura que nenhuma transação fraudulenta está a acontecer. Também

é um processo extremamente complexo em que mesmo as máquinas mais poderosas podem demorar algum tempo a resolver. O primeiro nodo a resolver essa operação recebe uma recompensa – Bitcoins – que são geradas aquando da resolução de uma das funções *hash* criptográfica que validam uma transação, daí a metáfora da "mineralização" das Bitcoins.

Assim que uma transação é verificada ela é acrescentada à cadeia e o processo repete-se sucessivamente.

Porém, o número de Bitcoins que um *miner* recebe por recompensa não é de todo fixo, elas vão reduzindo logaritmicamente à medida que são introduzidas na cadeia, por forma a limitar o número de moedas existentes e prevenir a sua inflação. Apenas 21 000 000 de Bitcoins podem estar em circulação na rede.

3. A *blockchain*

3.1. Aspetos técnicos da blockchain

A *blockchain* é uma tecnologia que permite a transferência de bens entre usuários. Funciona como uma base de dados que armazena informação, organizando-a em blocos (*blocks*). À medida que a informação é armazenada, são criados novos blocos para armazenar a informação recente, que serão posteriormente ligados ao bloco anterior, formando, assim, uma corrente, daí o seu nome. Um dos exemplos reais do uso da *blockchain* é a sua utilização para armazenar o histórico de transações de bitcoins entre entidades (Prathyusha, Kavya, e Akshita 2018).

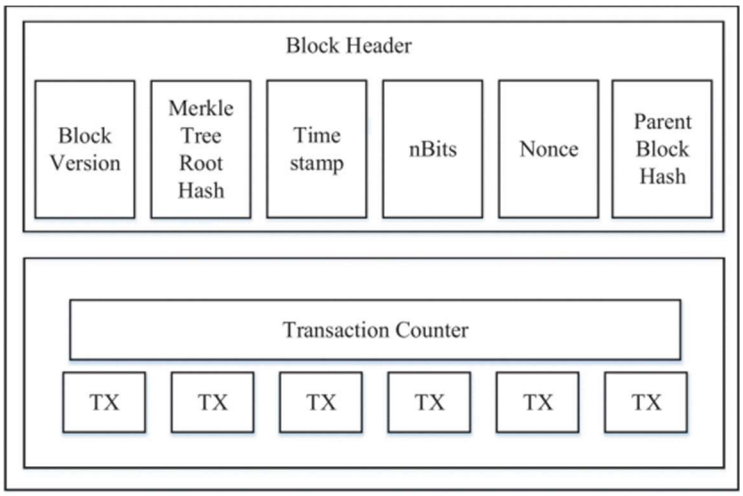

Figura 1. Constituição de um bloco da *blockchain* (Zheng et al. 2017).

Cada bloco nesta corrente é constituído por 2 partes essenciais: o *block header* e o bl*ock body*. O *block header* contém: a versão do bloco; a sua *hash* especifica; a data da sua criação; uma *nonce*; um *nBits* e a *hash* do bloco anterior de forma a permitir a ligação deste bloco à corrente. O *block body*, por sua vez, contém toda a informação armazenada no bloco (Zheng et al. 2017).

Como vimos, no *block header* encontra-se presente uma *hash* especifica desse bloco. Essa *hash* é gerada utilizando o algoritmo SHA256, e serve como identificadora do bloco. Está aqui também presente a *hash* referente ao bloco anterior. É a presença desta *hash* que permite validar o bloco criado e ligá-lo aos blocos anteriormente formados. Portanto, se essa *hash* corresponder à *hash* do bloco imediatamente anterior, valida-se esse bloco, juntando-o à corrente (Antonopoulos 2014).

Assim, uma *blockchain* é muitas vezes visualizada como uma *stack* de blocos por ordem cronológica, em que cada bloco se refere ao bloco anterior através de *hashes*, criando uma corrente que liga todos os blocos, desde o mais recente, até ao bloco original ou *genesis block* (Antonopoulos 2014).

3.2. Ideologia da *blockchain*

A *blockchain* usa o sistema ***peer-to-peer*** (P2P). Este sistema é baseado numa rede onde não há hierarquias nem servidores centrais para onde são direcionadas informações ou dados. Neste sistema, os computadores ligados à rede (nodos) são independentes, mas interligados entre si, realizando todos as mesmas funções, recebendo e partilhando dados ao mesmo tempo. Assim, ao usar uma rede P2P, a *blockchain* é descentralizada, não existindo um servidor central para onde flui toda a informação, mas sim um conjunto de computadores com acesso total a toda a informação presente na *blockchain* (Antonopoulos 2014).

Numa rede centralizada, a validação de uma dada transação dá-se por meio de uma entidade intermediária confiável. Por outro lado, num sistema descentralizado, cada transação é validada através do consenso entre nodos em relação à validade ou não de um bloco, conseguida com o uso de alguns protocolos. Alguns desses protocolos são o *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS), *Delegated Proof-of-Stake* (DPoS) e *Ripple*.

O PoW é o protocolo usado no sistema da Bitcoin, pelo que será aprofundado mais adiante.

De acordo com Mingxiao et al. (2017) e Zheng et al. (2017), o protocolo PoS pode ter em conta um dos seguintes fatores: o *coin age*, ou seja, o tempo que um nodo mantém a moeda em sua posse; ou a quantidade de posses que um nodo tem. No primeiro caso, quanto mais tempo um nodo mantém bens em sua posse, mais direitos tem, sendo as suas transações consideradas seguras. No segundo, acredita-se que quanto mais bens um utilizador tem, menor a chance de ele atacar a rede, daí ser considerado mais confiável.

Na DPoS os nodos que geram e validam blocos são eleitos democraticamente. Este protocolo permite uma rápida criação e validação de blocos (Mingxiao et al. 2017).

3.3. *Blockchain* associada às criptomoedas

A Bitcoin utiliza a tecnologia *blockchain* como forma de armazenar todas as transações realizadas. De acordo com o sistema da Bitcoin, a validação de transações/blocos é realizada pelos nodos conectados à rede através do protocolo de PoW.

Assim, quando ocorre uma transação, esta é incorporada num bloco que, após estar completo, será enviado para todos os nodos da rede para que este seja validado e posteriormente ligado à *blockchain*. Esta avaliação é conhecida como *mining*, e é efetuada pelos *miners*. Para conseguir provar a validade de determinado bloco, os *miners* têm que descobrir a *hash* do bloco sobre verificação através de um problema matemático baseado num algoritmo, cuja resolução é de elevada dificuldade, mas de fácil verificação. O *miner* que conseguir determinar a *hash* envia-a para os outros *miners* para que estes possam verificar se essa é a solução correta. Caso isso aconteça, o bloco é validado e adicionado à *blockchain*. A solução do problema (*hash*) é então incluída no *header* do novo bloco e serve como prova

(PoW) de que o *miner* resolveu o problema, permitindo-lhe receber uma recompensa em bitcoins. Após ser incluído na *blockchain*, todas as transações incluídas no bloco são consideradas válidas, permitindo o uso ou troca das bitcoins pelos novos donos (Antonopoulos 2014).

Muitas vezes, vários blocos são validados ao mesmo tempo, integrando a *blockchain* na mesma altura. Isto pode causar um ***blockchain fork***, ou seja, uma bifurcação da *blockchain*, causando a formação de duas correntes às quais vão sendo adicionados blocos.

> "A *blockchain* literalmente dividiu-se em dois, com uma parte da rede a adicionar blocos a uma versão da *chain*, e a outra parte a adicionar à outra. Nas seis horas subsequentes, existiram efetivamente duas redes Bitcoin a operar ao mesmo tempo, cada uma com a sua própria versão do histórico de transações." **(Buterin 2013)**[1]

Na maioria das vezes, este problema é resolvido rapidamente: a *chain* mais longa é considerada a principal, e os blocos presentes na *chain* mais curta são removidos e reintegrados na *blockchain*. Mas, em alguns casos, estes *forks* podem durar até algumas horas, criando várias bifurcações e correntes inválidas de blocos, tendo como consequência perdas de informação e de blocos que, noutros casos, seriam validados.

3.4. Segurança e imutabilidade da *blockchain*

A tecnologia da *blockchain* funciona com base na criptografia, permitindo um sistema seguro. Para além do uso de criptografia, a presença no *block header* da *hash* referente ao bloco imediatamente anterior permite aumentar a segurança e a imutabilidade dos dados, principalmente à medida que são adicionados novos blocos.

Como foi visto anteriormente, a forma de descobrir a *hash* de um determinado bloco é resolvendo um problema matemático de grande dificuldade, sendo necessário um grande poder computacional para o fazer. Assim, com a modificação da informação presente num dado bloco, a *hash* referente a esse mesmo bloco irá mudar. Vimos também que os blocos contêm a *hash* dos blocos imediatamente anteriores. Desta forma, com a alteração dos dados de uma dada transação e com a consequente mudança da *hash*, os blocos serão incompatíveis entre si, sendo então detetada uma falha pelos nodos, um indicador de que foram realizadas alterações num dado bloco, permitindo a sua correção. Para que a alteração ocorra sem ser detetada, seria necessário recalcular as *hashes* de todos os blocos posteriores ao que foi alterado, o que é praticamente impossível dada a necessidade de capacidade computacional extremamente elevada para que esse cálculo fosse realizável antes da deteção da falha.

[1] Em relação à *fork* de março de 2013 (ver secção 5.4).

4. Vantagens das criptomoedas

As criptomoedas têm uma vasta vantagem sobre as moedas físicas em diversos aspetos. Os mais relevantes são:

- Liberdade financeira
- Moeda descentralizada
- Menor número de taxas aplicadas

Sendo uma moeda descentralizada, por ser gerida por um *software open-source*, a *blockchain* que suporta a Bitcoin é

> "armazenada num ficheiro num computador pessoal, e o acesso ao ficheiro é permitido apenas ao dono do ficheiro. Apenas o dono possui as chaves que permitem o acesso à Bitcoin e a sua transferência para outros utilizadores através de um *software* especial *open-source*, sobre o qual a informação está disponível de forma gratuita." **(Danilina, Podlinnova, e Silaev 2015)**

O uso da moeda digital pretende que movimentos sejam realizados diretamente entre as pessoas, sem que sejam obrigados a passar por terceiros como bancos.

> "Não existem impostos, e as taxas de transação são mais baixas: devido à sua natureza descentralizada e anonimidade dos utilizadores, não existe uma forma viável de implementar um sistema de impostos na Bitcoin." **(Conti et al. 2017)**

Além disso, a moeda é internacional, o que significa que pode ser usada em qualquer parte do globo, sendo bem mais prático do que o câmbio de moeda, o que inclui taxas por sua vez.

A Bitcoin tem como objetivo substituir as moedas físicas e tornar o uso do dinheiro pragmático e acessível a todos.

5. A ideologia Bitcoin

5.1. Teoria do dinheiro

Apesar da teoria do dinheiro não se enquadrar em grande parte no âmbito deste relatório, a compreensão de alguns conceitos fundamentais desta área é essencial ao desenvolvimento do tópico da Bitcoin como motivo de alteração do paradigma económico.

Num *sistema de reserva total*, a reserva de um banco corresponde à totalidade dos depósitos, prestando apenas serviços de segurança aos depositantes (Abel, Bernanke, e Croushore 2011).

Mas supondo que os montantes de depósitos e levantamentos se equilibram aproximadamente, e que é improvável que os depositantes pretendam levantar uma grande parte dos depósitos num curto intervalo de tempo (*corrida aos bancos*), o banco necessita de apenas uma fração dos depósitos em reserva (*reserva mínima*) de forma a satisfazer os levantamentos[2]. No *sistema de reserva fracional*, o banco pode utilizar a maior parte dos depósitos para conceder empréstimos com juros a clientes com baixo risco de incumprimento, aumentando os seus lucros (Abel, Bernanke, e Croushore 2011). Assim, (1) os depositantes têm a 'garantia' de poder efetuar levantamentos[3], e (2) os devedores recebem dinheiro após contraírem empréstimos. Assim, considera-se que o banco "criou dinheiro a partir do nada", uma vez que processa (2) enquanto se compromete com (1) (Rothbard 1995).

5.2. Cripto-utopia

O sucesso da "revolução Bitcoin" sobre a teoria do dinheiro apoia-se no falhanço do sistema económico-financeiro, tanto do ponto de vista moral, como do ponto de vista prático.

A própria noção de moeda *fiat*, cuja produção se encontra sistematicamente associada à **produção de dívida** e ao binómio devedor-credor, prejudica a sua imagem na perspetiva da igualdade de direitos (o credor exige ao devedor a restituição do valor da dívida), assim como incomoda quem considera a dívida um problema moral, económico e político (Dodd 2017).

De acordo com Dodd (2017), a utilização da Bitcoin visa, além da substituição do atual sistema financeiro, a remoção de dois principais intermediários: bancos, e estado. Em termos mais gerais, o objetivo é remover completamente a política da produção e gestão do dinheiro.

Para Rothbard (1995), **o sistema de reserva fracional é inerentemente insolvente**, uma vez que um banco depende da ignorância dos depositantes para os convencer de que o dinheiro depositado se encontra de facto "no banco". Se os depositantes se apercebessem

[2] Por exemplo, a Reserva Federal dos EUA exige uma reserva mínima de 10% a bancos com total de operações >$122,3M (Federal Reserve 2017), e o BCE exige 1% (European Central Bank 2018).

[3] Mesmo que um banco declare insolvência, o banco central possui um fundo de garantia de depósitos, para o qual contribuem todos os bancos, que garante o pagamento aos depositantes.

da realidade, ocorreria uma corrida aos bancos e consequente insolvência de múltiplos bancos. Nessa situação, seria impossível resgatar o sistema financeiro com todo o dinheiro que existe, forçando o banco central a emitir moeda suficiente para pagar a todos os depositantes, provocando hiperinflação.

Conferindo autoridade a cada nodo da rede, a Bitcoin não requer a confiança de pessoas em pessoas; a **confiança** é depositada **em máquinas e algoritmos** que não são tão facilmente corrompíveis como especialistas, políticos ou banqueiros.

Através da Bitcoin, é satisfeito o objetivo de remover os bancos do sistema financeiro, uma vez que se extinguem as funções de salvaguardar dinheiro ou produzi-lo ("do nada") através de criação de dívida. A Bitcoin possui **valor real** na medida em que representa o custo de hardware, computacional, e energético de a produzir (Maurer, Nelms, e Swartz 2013), pelo que não precisa de, nem pode, ser criado da mesma forma que as moedas *fiat*. Além disso, é dinheiro totalmente desligado de dívida, espelhando características apontadas ao ouro como moeda-mercadoria (Dodd 2017). O vocabulário da Bitcoin traduz um certo paralelismo com o ouro (ex.: *miners*/*mining*, *rigs*), e inclusive Nakamoto estabelece essa comparação:

> "A adição gradual de moeda [Bitcoin] é análoga ao gasto de recursos pelos mineiros de ouro para colocar mais ouro em circulação. No nosso caso, são gastos tempo de CPU e eletricidade." **(Nakamoto 2009)**

O facto da Bitcoin utilizar o sistema de *distributed ledger* confere à rede um caráter distribuído em termos de processamento de operações e de autoridade, concetualmente impossibilitando hierarquias. Por um lado, esvazia-se por completo a última função que restava às instituições financeiras: **os bancos privados e o estado/banco central como topo de uma hierarquia de autoridade/centralidade**. Por outro, é satisfeita outra linha (uma das únicas quase desligável da teoria do dinheiro associada) do esquema ideológico que suporta as criptomoedas: a visão utópica do **horizontalismo social** por distribuição da autoridade, através da concretização de um sistema sem hierarquias e no qual as pessoas podem entrar por vontade própria ao compactuarem com o protocolo; nas palavras de Scott (2014), um "Tecno-Leviatã", por analogia ao Contrato Social de Hobbes (1651).

Ligada à questão da remoção do estado do sistema financeiro está ainda associado o medo de **interferência excessiva do estado em assuntos privados/pessoais**, que culmina na possibilidade última de controlar a vida dos cidadãos através do sistema financeiro[4]. Ao permitir o afastamento das instituições (principalmente do governo), a Bitcoin remove-lhes o controlo do dinheiro, sobrepondo-se às teses do anarquismo, liberalismo/extrema-direita e autores de teorias de conspiração (Dodd 2017).

[4] Apesar de ser difícil de provar que algum estado é capaz desse nível de controlo dos cidadãos, sabe-se que alguns estados utilizam o sistema financeiro para efetuar vigilância por razões de segurança (Goede 2012).

A Bitcoin pode ser utilizada simultaneamente como meio de troca e como investimento, sendo que os apoiantes ideológicos preferem sublinhar a vertente de meio de troca, uma vez que é a vertente que fundamentalmente permite justificar a substituição das moedas *fiat*.

5.3. Contradições da ideologia Bitcoin

Mesmo quando os seus partidários pretendem fazer crer que a adoção da Bitcoin permitirá operar uma alteração fundamental do sistema financeiro e da sociedade, nem sequer as criptomoedas podem fugir a determinados vícios que afetam as moedas que buscam substituir.

Transferência da confiança

A transferência da confiança de pessoas para máquinas não implica confiança total no sistema; pelo contrário, continua a ser necessário que os utilizadores sejam maioritariamente ignorantes em relação ao funcionamento das criptomoedas, fundamentando a sua confiança na 'fé' em protocolos e nas pessoas que os criam, em vez de na 'fé' em bancos e estados. De acordo com Dodd (2017), em entrevista a um negociante de Bitcoin, a mesma pessoa foi capaz de afirmar que (1) a Bitcoin era superior ao ouro na medida em que existe uma quantidade máxima bem conhecida de Bitcoins (₿21M) fixada pelo software, assim como que (2) seria possível ao "chief scientist" da Bitcoin aumentar ou remover esse limite. A forma atual de funcionamento da Bitcoin admite ambas as afirmações, aparentemente contraditórias. Em (1), o negociante confirma que a ignorância das pessoas é a "ficção necessária" para manter a rede a funcionar. Já em (2), é explicitada a condição real da Bitcoin: a maior parte do software dedicado a essa criptomoeda é fornecido pela Bitcoin.org e por outros grupos, e que o limite não é alterado apenas para não quebrar a confiança em (1) (Dodd 2017).

Concentração de poder e horizontalismo social

Apesar da Bitcoin transparecer ideias anarquistas e liberais de horizontalismo social, fracassa na implementação prática. No mundo da Bitcoin, não importa quem detém mais bitcoins (são poderosos dentro dos pressupostos do sistema); quem detém o poder são os maiores produtores de bitcoins, pois controlam a produção de moeda, e podem concertar posições para alterar a *blockchain*[5]. Além disso, a Bitcoin, por *design*, promove a concentração da produção da moeda nas *mining pools* (como explicado em mais detalhe em 5.5), constituindo, assim, o exemplo supremo de hierarquização do sistema financeiro. As *mining pools* podem controlar a Bitcoin sem a confiança dos utilizadores, quando do lado das moedas *fiat* existe um banco central, que as pessoas sabem ser responsável pela gestão do sistema financeiro e na qual as pessoas confiam (Dodd 2017).

[5] Aquando da *fork* de março de 2013 (secção 5.4), ficou evidente a capacidade de concertação das *pools* entre si e com entidades supervisoras da Bitcoin.

De acordo com Dodd (2017), "é fácil exagerar o impacto da Bitcoin fora dos círculos de aficionados". O relatório de (Agrawal 2015) sobre os resultados da sondagem do Coin Center (até março de 2015) revelaram que 35% dos inquiridos estavam familiarizados com a Bitcoin, e que apenas 4,5% tinham usado a moeda digital. A análise de (Brown 2018) aos resultados da sondagem da LendEDU (agosto de 2017), salienta o crescimento da consciência pública sobre a Bitcoin (78,6%), apesar da reduzida utilização reportada pelos inquiridos (11,0%)[6].

Apesar do objetivo da Bitcoin de estabelecer o paradigma de dinheiro como 'coisa' em substituição da interpretação como fenómeno social, foi crescendo em sua volta uma comunidade totalmente desenvolvida com forte espírito de grupo, que cultiva a confiança no protocolo Bitcoin, promotora de determinadas ideologias políticas, claramente organizada e hierarquizada, na qual as assimetrias de riqueza e poder são claras (Dodd 2017). Em suma, a Bitcoin deu origem a uma entidade à qual claramente se opõe do ponto de vista ideológico e dos (supostos) objetivos práticos, mas da qual depende de forma indispensável a sua sobrevivência, mostrando claramente que o dinheiro é um fenómeno social (Dodd 2017).

5.4. Problemas técnicos da Bitcoin

É importante frisar que, apesar de dependente de tecnologia e vigiada por um conjunto de supervisores e programadores, a *blockchain* utilizada pela Bitcoin não é infalível. A história da Bitcoin encontra-se marcada por **incidentes** relacionados com *blockchain forks* acidentais e *bugs* que poderiam ter implicações gravíssimas no protocolo, Figura 2.

Incidente/Data	Descrição
Value overflow 2010, 15/Ago	O bloco 74638 continha uma transação que criou Ƀ$2^{64}/10^8$ para dois endereços, devendo ser rejeitado por ultrapassar o limite de Ƀ21M. O bloco foi validado por erro de *overflow*. Resolvido com uma *soft fork*, a *chain* 'boa' retomou liderança no bloco 74691 [+53]. (Buterin 2013, Harding 2016)
2013 Bitcoin fork 2013, 11/Mar	Durante o período de atualização do bitcoind0.7 para 0.8, foi criado o bloco válido 225430, anormalmente grande. O bloco foi rejeitado pelos nodos pre-0.8 e aceite pelos nodos 0.8, provocando uma *hard fork* durante 6 horas. Algumas *mining pools* foram requisitadas a regressar a pre-0.8, a *chain* 'boa' retomou liderança no bloco 225454 [+24] (Buterin 2013).
CVE-2018-17144 2018, 18/Set	Detetado um *bug* crítico que permitia ataques DDoS a nodos da rede, provocando risco de inflação devido a *double-spending*. Corrigido em 20/Set com o *patch* BitcoinCore0.16.3 (BitcoinCore 2018, Gola 2018).

Figura 2. Incidentes relacionados com o protocolo Bitcoin (lista selecionada).

Apesar de não diretamente relacionadas com o protocolo Bitcoin, as empresas cambistas de Bitcoin constituem uma parte essencial do sistema, pelo menos enquanto a Bitcoin não for

[6] Note-se que (Agrawal 2015) e (Brown 2018) se reportam a sondagens *online*, pelo que existem limitações na generalização das inferências de ambas as sondagens à população em geral. A utilização de uma metodologia de correção de resultados é referida explicitamente apenas na sondagem do Coin Center por (Valkenburgh 2015).

uma moeda de circulação corrente. Desde a criação da Bitcoin que existem as cambistas, e desde essa altura que se repetem **ataques informáticos** a estas empresas que possuem grande volume de transações e de depósitos, Figura 3.

Data	**Cambistas atacadas**	**Valor roubado (₿)**	**Valor (US$)** (aprox.)
Dec 2017	NiceHash (Eslovénia)	4 736	51,2M
Abr 2017	Yapizon (Coreia do Sul)	3 816	5,1M
Out 2016	Bitcurex (Polónia)	2 300	1,5M
Ago 2016	Bitfinex (Hong Kong)	119 756	70,1M
Fev 2015	Bter (China)	7 170	1,8M
Fev 2014	Mt. Gox (Japão)	650 000	547,3M

Figura 3. Ataques informáticos a empresas cambistas, que resultaram no roubo de bitcoins (lista selecionada). (CoinDesk 2018, Higgins 2017, Khatwani 2018)

5.5. Problemas de *design* e económicos da Bitcoin

A moeda possui valor quando é escassa, mas a escassez das moedas *fiat* é relativa, dependendo da vontade dos bancos e do estado; já a Bitcoin é escassa em termos absolutos, limitada à quantidade de ₿21M, o que significa que, com crescimento económico real, a Bitcoin é **inerentemente deflacionária** (Correia 2017, Dodd 2017), encontrando-se a deflação associada à falta de liquidez e redução do consumo devido ao incentivo à poupança (Correia 2017, Tucker 2017), condições que se encontram historicamente ligadas a um desempenho económico muito fraco (Abel, Bernanke, e Croushore 2011).

Devido a questões do seu próprio *design* e natureza, a Bitcoin dá origem a vários problemas que se alimentam de forma cíclica: (1) a Bitcoin como ativo de investimento, (2) a volatilidade do seu valor e (3) a reduzida adoção da moeda.

Afeta ↱	**(1) Investimento**	**(2) Volatilidade**	**(3) Reduzida adoção**
(1) Investimento	Como a deflação incentiva a poupança, os donos de ₿ logicamente pretendem guardá-las para poderem adquirir mais bens mais tarde, quando a moeda for mais valiosa (Tucker 2017).	A interpretação da ₿ como investimento de risco faz com que as pessoas considerem 'normais' eventuais oscilações, ignorando a necessidade de ter cuidado com o sistema financeiro.	Se a ₿ é um investimento de risco, não faz sentido utilizar em transações de bens essenciais; o risco de perda de dinheiro por desvalorização da ₿ afasta pessoas normais e investidores de baixo risco.
(2) Volatilidade	Reduz a ₿ ao nível de ações em bolsa (investimento de risco).	Nenhuma entidade controla a quantidade de dinheiro em circulação e a inflação/deflação (Alstyne 2014).	A tabelação de preços em ₿ torna-se difícil, por implicar atualizações frequentes.
(3) Reduzida adoção	A ₿ torna-se pouco prática como meio de troca em comércio, logo prevalece a vertente do investimento (que exige menos movimentos).	A base de utilizadores é pequena, logo algumas transações podem provocar grandes oscilações.	Todos os fatores acabam por dificultar a adoção, de forma rentável e generalizada, da aceitação de ₿ como método de pagamento.

Figura 4. Alguns problemas da Bitcoin (₿) que se alimentam de forma cíclica. Os problemas nas linhas afetam os problemas nas colunas. A cinza, é descrita a forma como a natureza da Bitcoin afeta esse problema.

Mesmo nos casos em que a Bictoin é utilizada na aquisição de bens, os preços encontram-se geralmente tabelados em moedas *fiat* (Dodd 2017); e até em casos em que serve como investimento, o objetivo é que a Bitcoin se valorize face a outras moedas para permitir um câmbio para moedas *fiat* que permita lucro. Em ambos os casos, a Bitcoin faz parte do processo como mera intermediária da transação.

A Bitcoin utiliza *proof-of-work* por *design*, um tipo de certificação que promove a concentração da produção de moeda, uma vez que a única máquina recompensada é a que resolver o puzzle criptográfico primeiro. Como o poder computacional das *mining pools* é muito elevado, estas acabam por minar ainda mais bitcoins do que era suposto tendo em conta o seu poder computacional. Além de resolverem mais *puzzles* em menos tempo, ultrapassam de longe máquinas menos poderosas que tenham começado a resolver o mesmo *puzzle* ao mesmo tempo, coletando toda a recompensa para si (Dodd 2017).

5.6. Problemas legais associados à Bitcoin

O caráter tecnológico da Bitcoin configura uma grande dificuldade de legislação, uma vez que os legisladores não possuem o conhecimento necessário, nem são aconselhados o suficiente, sobre as criptomoedas para elaborarem leis razoáveis. Além disso, ocorrem complicações ao nível da aplicação da lei, uma vez que se trata de uma moeda transnacional e descentralizada; atualmente, não existe uma política internacional de regulação da Bitcoin e a sua legalidade depende fundamentalmente de país para país (Norry 2018).

Como referido na secção 5.2, a Bitcoin pode ser simultaneamente considerada um investimento e uma moeda de troca. Se for considerada a primeira, então traduz-se numa espécie de ação em bolsa (logo semelhante a um bem), o que torna proibida a sua utilização como moeda na maior parte dos países (que não permitem **comércio em géneros**), além de forçar a **taxação** da mesma forma que ações ou investimentos. Quando é considerada uma moeda que aspira a substituir as outras moedas, coloca diretamente em causa a soberania dos países (cuja *razão de ser* é a possibilidade de influenciar o mercado e a sociedade) e a legitimidade do sistema fracional de reserva; por uma questão de sobrevivência, ambas as instituições utilizariam todos os meios à sua disposição para neutralizar a Bitcoin.

Mesmo que o objetivo da Bitcoin seja apenas complementar o sistema financeiro existente (como acontece maioritariamente na atualidade), surge outro tipo de problemas, nomeadamente ligados à atividade criminosa. Pouco depois da sua criação, a Bitcoin atraiu a atenção dos reguladores em resultado da sua utilização na *Dark Web* em virtude do género de produtos e serviços que podem ser adquiridos nesta parte da *Web* (nomeadamente armas de fogo, drogas ilícitas (Norry 2018), pornografia ilegal e cartões e contas bancárias roubadas, além de operações de lavagem e contrafação de dinheiro (Moore e Rid 2016)).

6. Aplicações da blockchain em outros domínios

A blockchain surgiu em 2008, durante uma das maiores crises financeiras mundiais, para realizar transações monetárias com Bitcoin. O seu intuito inicial era retirar o intermediário de transações onde era necessário os envolvidos confiarem uns nos outros ou em terceiros para mediar transações e garantir que os valores são efetivamente transferidos (Ferreira 2017). Um *distributed ledger* permite evitar a centralização e criar um P2P global seguro (Cavalcante Neto et al. 2017). Desta forma, o seu uso difundiu-se para diversos outros setores. Alguns dos benefícios são apresentados na Figura 5.

Transações seguras, rápidas e sem intermediário	Reduz/elimina o risco da desconfiança entre as partes e custos de transação
Utilizadores com poderes	Os utilizadores controlam todas as suas transações e informações
Dados de alta qualidade	Os dados da blockchain são intrinsecamente completos, consistente, precisos e amplamente disponíveis no momento que forem necessários
Segura e amplamente disponível	Ausência de ponto único de falha
Processos íntegros	Tudo é executado conforme o protocolo, sem intermediários
Transparência e imutabilidade	Todas as transações estão disponíveis publicamente e não podem ser alteradas ou apagadas
Simplificação do registo	Um único livro de registo (blockchain) é criado, reduzindo a desordem e complicações

Figura 5. Benefícios de um *distributed ledger* (Leal).

6.1. Moeda soberana em formato digital

Com a expansão dos meios eletrónicos, diversos bancos centrais (Canadá, Inglaterra e Singapura) estão a estudar a possibilidade da emissão de uma moeda soberana em suporte virtual, com vantagens como (Burgos e Batavia 2018):

- Redução do custo de transações financeiras
- Monitorização em tempo real
- Maior eficiência de pagamentos e proteção do consumidor
- Descentralização de sistemas de pagamento
- Democratização e integração social de sistemas financeiros

Moedas virtuais particulares, como a Bitcoin, possuem valor monetário não controlado. As criptomoedas privadas "não são emitidas, garantidas ou reguladas por Banco Central. Possuem forma, denominação e valor próprios" (Banco Central do Brasil 2017). Ou seja, não são moedas oficiais. Ao contrário do modelo aqui retratado, trata-se de um dinheiro digital emitido pelo banco central, ao qual é concedido o estatuto de moeda oficial, tal como o Euro ou outras moedas soberanas.

Com a sua oficialização, a população teria amplo acesso às moedas *tokenizadas*, baseado em *tokens* e no mecanismo de transferência P2P, sem juros, com a privacidade de saldo e transações garantida pelo sigilo bancário tal como nos bancos de hoje, e com custos muito mais baixos (Cavalcante Neto et al. 2017).

A escolha da instituição responsável pelo *mining* de novas moedas seria uma decisão política (Cavalcante Neto et al. 2017), que permitiria um melhor controlo da inflação/deflação num mercado dominado por essa moeda, ao contrário do que ocorre com a maior parte das criptomoedas privadas.

Este projeto teria foco na venda a retalho. Atualmente já há manipulações digitais de valores monetários. No entanto, os principais meios de pagamento na venda a retalho continuam a ser notas e moedas físicas, cujo ciclo de vida curto implica grandes despesas aos cofres públicos. De acordo com (Cavalcante Neto et al. 2017), cerca de 30% das moedas metálicas ficam fora de circulação.

Os cartões bancários possuem operações com um custo mais alto, uma vez que exigem o controlo de cobranças, que é feito por um mediador, o emissor do cartão. De qualquer forma, se não se tratasse de uma criptomoeda seria mesmo assim necessário um mediador, o que implica custos adicionais nas transações (Martins 2018).

6.2. Autenticação de documentos com *blockchain* (cartórios)

Um cartório serve como mediador para autenticar testemunhos, como casamentos, contratos de compra/venda ou acordos judiciais. A credibilidade desses documentos é devido ao poder governamental dado ao estabelecimento, que propõe um valor proferido pelo mesmo para conferir autenticidade ao registo. Porém, este processo é corruptível dado que se baseia na confiança entre indivíduos (Martins 2018)

Com transações feitas por blockchain, cada registo é armazenado numa 'página' de um registo (*ledger*), tornando-se quase impossível adulterá-lo passado algum tempo (Martins 2018).

No caso de se pretender modificar uma informação do registo, deve-se proceder a alterações em toda a página e em todas as páginas anteriores, o que pode implicar a necessidade de um poder de processamento computacional exorbitante, o que na prática se traduz na credibilidade e imutabilidade dos arquivos.

Num sistema de autenticação por *blockchain*, todos os registos são armazenados no *distributed ledger*, onde não estão sujeitos ao risco de deterioração (danos físicos) como em documentos de papel, e podem ser consultadas a qualquer momento. Com este sistema, deixa de ser necessário um mediador confiável, reduzindo-se assim o custo de escrituração (Martins 2018).

6.3. Smart contracts

A Bitcoin foi a primeira criptomoeda a suportar *smart contracts* básicos, na medida em que permitem à rede transferir um montante de uma pessoa para outra, sendo que a rede só validará as transações quando determinadas condições forem cumpridas.

O Ethereum, considerada a segunda geração de *blockchain*, não possui linguagem restritiva e limitada somente à moeda. Com linguagem mais flexível e extensível, os desenvolvedores podem redigir os seus próprios programas (Hertig).

São inúmeros os motivos que tornam um *smart contract* superior a um contrato comum. Há um ganho em eficiência notável, nomeadamente tendo em conta que os diversos resultados e implicações podem ser calculados rapidamente, sem a necessidade de advogados, cartórios e transferências bancárias (Ferreira 2017).

O benefício mais importante da *blockchain* é que, sem a necessidade de uma entidade central com o papel de conciliadora, permite a duas partes que não se conhecem confiem uma na outra, possibilitando a troca de informações. Vantagem desejável uma vez que pode haver deslealdade do árbitro, favorecendo uma das partes. No caso de uma *blockchain*, não é possível corromper o mediador a seu favor, uma vez que é necessário a prevalência do consenso da maior parte (Ferreira 2017). Assim, a realização de *smart contracts* permite diminuir a burocracia e simplificar as etapas do processo.

7. Implicações sociais da blockchain

7.1. Vantagens de privacidade da blockchain

De forma a entender os verdadeiros benefícios da *blockchain* na melhoria da privacidade, precisamos inicialmente de entender o conceito de privacidade. O dicionário Merriam-Webster (2018) define privacidade como o "estado de separação/distância de companhia ou observação", situação que não ocorre frequentemente na proteção de dados pessoais.

Atualmente, a *blockchain* é uma das melhores soluções para a melhoria da privacidade de dados online, visto que o armazenamento da informação não é realizado numa só base de dados, mas sim num potencialmente infinito número de lugares e de forma encriptada como garantia de segurança. A incorporação desta tecnologia em diversos sistemas modernos (por exemplo de pagamento), fornece um maior controlo ao usuário relativamente à informação que partilha e com quem a partilha (Hall 2018).

Estas técnicas de *blockchain* já estão a ser aplicadas em vários países. Por exemplo, o governo da Estónia moveu gradualmente todos os dados e informações acerca dos seus cidadãos para um sistema de *blockchain* distribuído; no estado americano do Illinois, estão também a ser efetuados testes em sistemas baseados em *blockchain*, que incluem um registo de nascimento. Em Singapura, está a ser considerada a implementação de um *blockchain* que visa fornecer aos seus cidadãos uma maneira simples de interagir com os serviços do governo (Hall 2018).

Assim, há ainda muito trabalho a fazer para desviar o foco da tecnologia *blockchain* das criptomoedas e direcionar a sua atenção para aplicações no mundo real, como a garantia de privacidade e soluções de armazenamento (Hall 2018).

7.2. Desafios sociais na utilização dos sistemas de criptomoeda (*blockchain*)

Ainda que tenha inúmeros benefícios, uma das grandes barreiras à *blockchain* é também uma das maiores razões para a sua popularidade: a falta de suporte e controlo por parte das autoridades. De facto, é o carácter social da *blockchain*, em que cada utilizador da rede tem um papel, que provoca, ocasionalmente, a fraca gestão e manuseamento de dados, tendo como consequências, por exemplo, a perda de dinheiro por parte de certos utilizadores e falhas de segurança no caso do sistema de moedas virtuais.

Perda da *wallet*

Uma vez que não atuam terceiros confiáveis na gestão de carteiras virtuais de Bitcoin, se um utilizador perder a chave privada associada à sua carteira, todas as bitcoins contidas nesta serão perdidas para sempre, uma vez que não existe nenhum método que permita a recuperação desta moeda. A perda desta chave associada à *wallet*, muitas vezes associada a danos no disco rígido ou vírus que corrompem dados, pode facilmente levar à falência um investidor de Bitcoin em meros segundos (Conti et al. 2017).

Facilitação de atividade criminal

O nível de anonimato e privacidade fornecido pelo sistema de Bitcoin, ainda que não inquebrável (como irá ser exposto mais à frente), é considerável, o que justifica a elevada utilização desta moeda nas transações e atividades ilícitas, como o mercado negro, lavagem de dinheiro, evasão fiscal (Conti et al. 2017) e ainda, como relatado recentemente, com o vírus informático WannaCry, em ataques de *ransomware* (Mathews 2018).

7.3. Falhas de segurança nos sistemas de criptomoeda (*blockchain*)

Apesar da grande quantidade de benefícios que advêm do uso do Blockchain, este está também exposto a diversas ameaças que afetam, especialmente, os sistemas reguladores de moedas virtuais.

É o modelo descentralizado e o ambiente incontrolável que garantem a popularidade de moedas como a Bitcoin e Ethereum, porém, estas são também algumas das razões pelas quais hackers e ladrões conseguem tão facilmente encontrar métodos para burlar transações realizadas nestes sistemas de cripto moeda (Conti et al. 2017).

Desta maneira, há diversas vulnerabilidades associadas à tecnologia *blockchain*, que são evidenciadas pelos vastos tipos de ataque que ocorrem, nomeadamente: *double spending* (existindo também vários métodos para o facilitar), ataques à rede da moeda, ataques às *mining pools* e ataques ao cliente (Conti et al. 2017).

Double spending

Como o nome indica, *double spending* é o ato de gastar as mesmas bitcoins em múltiplas transações, e é realizado ao enviar rapidamente duas transações sucessivas, de modo a enganar o destinatário do pagamento, que consequentemente não será capaz de resgatar as moedas, perdendo, assim, o produto vendido. Atualmente, *double spending* é um dos grandes problemas de segurança do sistema de bitcoin, e, devido ao modo como a *blockchain* funciona, é e sempre será possível realizar, mesmo com a rigorosa identificação e ordenação nas transações (Conti et al. 2017).

7.4. Problemas de privacidade e anonimato na *blockchain*

No sistema bancário tradicional, é atingido o nível de privacidade requerido através da restrição de acesso às transações, ou seja, apenas as entidades envolvidas nestas transferências têm acesso às informações associadas a estas (Conti et al. 2017).

Devido à natureza do funcionamento da tecnologia *blockchain*, não é possível atingir privacidade e anonimato total, uma vez que, ao efetuar uma transação de dados, toda a informação relativa a essa transferência é revelada a qualquer utilizador conectado à rede, ainda que esta não especifique a origem da transação e que esteja encriptada. Na rede Bitcoin, por exemplo, uma transação representa um pagamento, que é certificado por uma chave digital privada pertencente ao dono anterior dessa quantidade de bitcoin; após a transação, a posse da moeda é especificada numa outra chave, agora pública (Möser 2013).

Estas chaves, utilizadas na *blockchain* (neste caso no sistema Bitcoin) são endereços pseudónimos que tentam desvincular a transação da identidade do utilizador; porém, as transações têm que ser identificadas, de modo a evitar *double spending*. Desta maneira, a ligação entre o utilizador e a transação pode ser rastreada através destas chaves, levando à origem da transferência e expondo a identidade desse mesmo utilizador (Conti et al. 2017).

7.5. Propostas de melhoria de privacidade na *blockchain* (e na Bitcoin)

Perante todos os problemas de privacidade que surgem devido à estrutura natural pública do *blockchain*, existem tecnologias que melhoram e aperfeiçoam os aspetos de privacidade desta corrente de dados, que podem ser divididos em três categorias: *peer-to-peer mixing protocols*, que se baseiam na utilização de um serviço de *mixing* anónimo para misturar o rasto de transferências/transações de modo a confundir eventuais rastreadores; *distributed mixing networks*, que usam também protocolos de *mixing*, facilitando também as transações; e, finalmente, Altcoins, que podem ser moedas alternativas ou extensões à própria Bitcoin, frequentemente mais seguras, oferecendo mais privacidade e anonimato nas transferências (Conti et al. 2017).

8. Conclusões

Uma blockchain é uma estrutura de dados dinâmica e sequencial constituída por blocos, cada um contendo alguma informação e uma *hash* criptográfica que identifica o bloco anterior. Adicionalmente, a informação dos blocos pode ser encriptada para maior segurança. Quando um novo bloco é criado à *chain*, este é adicionado apenas após ser validado pelo sistema P2P, através do qual um conjunto de máquinas/nodos hierarquicamente iguais efetuam a verificação, votando depois a inclusão ou rejeição do bloco.

As criptomoedas são moedas virtuais, cujas transações são guardadas numa *blockchain*. Nas transações com estas moedas, não existe um intermediário com autoridade. O sistema financeiro de criptomoedas não é regulado por nenhuma instituição central, dependendo essencialmente do protocolo da criptomoeda (apesar de casos em que o protocolo é elemento intermédio para *mining pools* e organizações controlarem as criptomoedas, como na *fork* de 2013 da Bitcoin). A verificação de um bloco é realizada principalmente através de PoW ou PoS, no caso em que nenhum nodo em particular é confiável, mas a rede é razoavelmente confiável. A atividade de participar na rede ou verificar blocos é conhecida como *mining*, e é geralmente premiada com recompensas monetárias na moeda do sistema utilizado. Um nodo só pode provar que um bloco é válido após resolver um problema matemático e criptográfico de elevada dificuldade, o que limita a quantidade de blocos adicionados à *blockchain* (no caso da Bitcoin, cerca de um bloco a cada 10 minutos) e bloqueia possíveis ataques do tipo DoS.

A utilização da Bitcoin, a criptomoeda mais popular atualmente, traz várias vantagens, como a remoção de intermediários (bancos e estados) por transferência da confiança de pessoas para máquinas e protocolos, além de permitir transações (principalmente internacionais) sem custos acrescidos ou taxas, constituindo-se como uma ferramenta para aumentar a igualdade social por razões fundamentadas no próprio *design* da moeda.

Apesar disso, a Bitcoin, assim como outras criptomoedas, possui na sua própria ideologia ou na forma como funciona na prática várias contradições e desvantagens, como o facto da verificação da *blockchain* por PoW promover a concentração de produção da moeda e de poder, ou os problemas técnicos inerentes à tecnologia, evidentes pelos vários incidentes na rede e ataques informáticos às *mining pools*. Para os estados, as criptomoedas constituem não só uma ameaça à lei (por permitirem aquisição de produtos e serviços ilegais, e operações de lavagem e contrafação de dinheiro.

Por estas razões, as criptomoedas não deverão experienciar grande aderência das pessoas, pelo menos nos próximos anos. Por outro lado, o caráter multifacetado da *blockchain* como uma base de dados abstrata deverá permitir a sua aplicação em diversas áreas, herdando os benefícios que lhe são inerentes e mitigando as desvantagens de experiências passadas.

Referências bibliográficas

Abel, Andrew B., Ben S. Bernanke, e Dean Croushore. 2011. *Macroeconomics*. 7 ed, *The Pearson Series in Economics*. Boston: Pearson Education, Inc.

Agrawal, Neeraj. 2015. "Coin Center releases March 2015 Bitcoin Public Sentiment Survey Data." Coin Center, Atualizado em 31 de março de 2015, acedido em 14 de outubro de 2018. https://coincenter.org/entry/coin-center-releases-march-2015-bitcoin-public-sentiment-survey-data.

Alstyne, Marshall Van. 2014. "Why Bitcoin has value." *Communications of the ACM* 57 (5):30-32. doi: 10.1145/2594288.

Antonopoulos, Andreas M. 2014. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies (Early Release)*. Sebastopol, CA: O'Reilly Media, Inc.

Banco Central do Brasil. 2017. "Moedas Virtuais (FAQ)." Banco Central do Brasil, Atualizado em novembro de 2017, acedido em 19 de outubro de 2018. https://www.bcb.gov.br/pre/bc_atende/port/moedasvirtuais.asp?idpai=FAQCIDADAO.

BitcoinCore. 2018. "CVE-2018-17144 Full Disclosure." Atualizado em 20 de setembro de 2018, acedido em 16 de outubro de 2018. https://www.ccn.com/new-core-patch-fixes-bitcoin-network-vulnerability-to-ddos-attacks/.

Brown, Mike. 2018. "Bitcoin's Present (and Future) Role in the American Economy." LendEDU, Atualizado em 23 de agosto de 2018, acedido em 10 de outubro de 2018. https://lendedu.com/blog/bitcoins-role-in-the-american-economy/.

Burgos, Aldênio, e Bruno Batavia. 2018. O Meio Circulante na Era Digital. Brasília, Brasil: Banco Central do Brasil.

Buterin, Vitalik. 2013. "Bitcoin Network Shaken by Blockchain Fork." *Bitcoin Magazine*.

Cavalcante Neto, Aristides Andrade, Aldênio de Vilaça Burgos, José Deodoro de Oliveira Filho, Marcus Vinicius Cursino Suares, Rafael Sarres de Almeida, e Marcelo José Oliveira Yared. 2017. Distributed ledger technical research in Central Bank of Brazil. Brasília, Brasil: Banco Central do Brasil.

CoinDesk. 2018. "Bitcoin (USD) Price." Atualizado em 16 de outubro de 2018, acedido em 16 de outubro de 2018. https://www.coindesk.com/price/.

Conti, Mauro, Sandeep Kumar E, Chhagan Lal, e Sushmita Ruj. 2017. "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, Piscataway, NJ. Acedido em 18 de outubro de 2018. https://arxiv.org/abs/1706.00916.

Correia, Guilherme Canedo. 2017. "BITCOIN: As inconsistências do modelo." Mestrado em Estratégias de Investimento e Internacionalização, Instituto Superior de Gestão.

Danilina, M. V., A. G. Podlinnova, e A. S. Silaev. 2015. "'E-Gold': The Advantages and Disadvantages." *Global Scientific Potential* 46 (1):101-103.

Dodd, Nigel. 2017. "The Social Life of Bitcoin." *Theory, Culture and Society* 35 (3):35-56. doi: 10.1177/0263276417746464.

European Central Bank. 2018. "How to calculate the minimum reserve requirements." Atualizado em 2018, acedido em 15 de outubro de 2018. https://www.ecb.europa.eu/mopo/implement/mr/html/calc.en.html.

Federal Reserve. 2017. "Policy Tools: Reserve Requirements." Atualizado em 3 de novembro de 2017, acedido em 15 de outubro de 2018. https://www.federalreserve.gov/monetarypolicy/reservereq.htm.

Ferreira, Frederico Lage. 2017. "Blockchain e Ethereum: Aplicações e Vulnerabilidades." Bacharelado em Ciência da Computação, Instituto de Matemática e Estatística, Universidade de São Paulo.

Goede, Marieke de. 2012. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN: University of Minnesota Press.

Gola, Yashu. 2018. "New Core Patch Fixes Bitcoin Network Vulnerability to DDoS Attacks." *CryptoCoinsNews*, Bitcoin Technology. https://www.ccn.com/new-core-patch-fixes-bitcoin-network-vulnerability-to-ddos-attacks/.

Hall, Josh. 2018. "How Blockchain could help us take back control of our privacy." *The Guardian*, 21 de março de 2018, Opinion. Acedido em 18 de outubro de 2018. https://www.theguardian.com/commentisfree/2018/mar/21/blockchain-privacy-data-protection-cambridge-analytica.

Harding, David A. 2016. "Value overflow incident." BitcoinWiki, Atualizado em 22 de julho de 2016, acedido em 16 de outubro de 2018. https://en.bitcoin.it/wiki/Value_overflow_incident.

Hertig, Alyssa. "How Do Ethereum Smart Contracts Work?". CoinDesk, acedido em 19 de outubro de 2018. https://www.coindesk.com/information/ethereum-smart-contracts-work/.

Higgins, Stan. 2017. "Cryptocurrency Mining Market NiceHash Hacked." *CoinDesk*. https://www.coindesk.com/62-million-gone-cryptocurrency-mining-market-nicehash-hacked/.

Hobbes, Thomas. 1651. *LEVIATHAN, or the matter, forme & power of a common-wealth ecclesiastical and civill*. Londres: Andrew Crooke.

Khatwani, Sudhir. 2018. "Top 5 Biggest Bitcoin Hacks Ever." *CoinSutra*. https://coinsutra.com/biggest-bitcoin-hacks/.

Leal, Rodrigo Lima Verde. Blockchain e Internet das Coisas: Aplicações e Iniciativas. Campinas, Brasil: CPqD.

Martins, Thiago Fonseca. 2018. "Prova de existência de arquivos digitais utilizando a tecnologia blockchain do protocolo Bitcoin." Bacharel em Engenharia da Computação, Instituto de Informática, Universidade Federal do Rio Grande do Sul.

Mathews, Lee. 2018. "Boeing Is The Latest WannaCry Ransomware Victim." *Forbes*, 30 de março de 2018. Acedido em 18 de outubro de 2018. https://www.forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim/#5efc53626634.

Maurer, Bill, Taylor C. Nelms, e Lana Swartz. 2013. "'When perhaps the real problem is money itself!': the practical materiality of Bitcoin." *Social Semiotics* 23 (2):261-277. doi: 10.1080/10350330.2013.777594.

"Privacy." 2018. In *Merriam-Webster*. Springfield, MA, Acedido em 18 de outubro de 2018. https://www.merriam-webster.com/dictionary/privacy.

Mingxiao, Du, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, e Chen Qijun. 2017. "A Review on Consensus Algorithm of Blockchain." IEEE International Conference on Systems, Man, and Cybernetic, Banff, Canadá, 5-8 de outubro de 2017.

Moore, Daniel, e Thomas Rid. 2016. "Cryptopolitik and the Darknet." *Survival* 58 (1):7-38. doi: 10.1080/00396338.2016.1142085.

Möser, Malte. 2013. "Anonymity of Bitcoin Transactions: An Analysis of Mixing Services." Münster Bitcoin Conference, Münster, 17-18 de julho de 2013.

Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Cryptography Mailing list at https://metzdowd.com*.

Norry, Andrew. 2018. "An In-depth Look at Bitcoin Laws & Future Regulation." Blockonomi, Atualizado em 2 de julho de 2018, acedido em 18 de outubro de 2018. https://blockonomi.com/bitcoin-regulation/.

Prathyusha, T., M. Kavya, e P. Sree Laxmi Akshita. 2018. "Block Chain Technology." *International Journal of Computer & Mathematical Sciences* 7 (3):232-237.

Rothbard, Murray N. 1995. "Fractional Reserve Banking." *The Freeman* 45 (10):624-627.

Scott, Brett. 2014. "Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain." E-International Relations, Atualizado em 1 de junho de 2014, acedido em 17 de outubro de 2018. https://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/.

Tucker, Jeffrey A. 2017. "In Defense of Bitcoin Hoarding." *Foundation for Economic Education*. Acedido em 17 de outubro de 2018. https://fee.org/articles/in-defense-of-bitcoin-hoarding/.

Valkenburgh, Peter Van. 2015. "Coin Center's new Bitcoin Public Sentiment Survey." Coin Center, Atualizado em 27 de janeiro de 2015, acedido em 14 de outubro de 2018. https://coincenter.org/entry/coin-center-s-new-bitcoin-public-sentiment-survey.

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, e Huaimin Wang. 2017. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." IEEE 6th International Congress on Big Data, Honolulu, HI, 25-30 de junho de 2017.