Criptomoeda: o Bitcoin

Pedro Ramos Brandão
Universidade de Évora – CIDHEUS
pb@pbrandao.net

Resumo

A síntese da moeda Bitcoin, a história da criptomoeda e do Bitcoin, o movimento Cyberpunk, as primitivas das tecnologias das criptomoedas, criptografia assimétrica, encriptação de chave pública, assinaturas digitais, Blockchain, endereços digitais, administração de consenso, prova de trabalho (PoW), mineração e impossibilidade de gastos duplicados.

Palavras-chave: Cadeia de Bloco, Bitcoin, Moeda Criptográfica, Nakamoto, Criptomoeda, Mineração de Bitcoins.

Title: Cryptocurrency: Bitcoin

Abstract: The synthesis of the Bitcoin currency, the history of cryptocurrency and Bitcoin, the Cyberpunk movement, the primitives of cryptocurrency technologies, asymmetric cryptography, public key encryption, digital signatures, Blockchain, digital addresses, consensus management, proof of work (PoW), mining and the impossibility of duplicate expenses.

Keywords: Block Chain, Bitcoin, Crypto Currency, Nakamoto, Cryptocurrency, Bitcoin Mining.

1. Introdução

O Bitcoin é uma coleção de conceitos e tecnologias que formam a base de um ecossistema monetário digital.

Unidades de moeda denominadas Bitcoin são usadas para armazenar e transmitir valor entre os participantes da rede Bitcoin. Os utilizadores do Bitcoin comunicam entre si usando o protocolo Bitcoin, principalmente via Internet, embora outras redes de transporte também possam ser usadas. A pilha de protocolos do Bitcoin, disponível como software de código aberto, pode ser executada numa ampla gama de dispositivos de computação, incluindo laptops e smartphones, tornando esta tecnologia facilmente acessível.

Os utilizadores podem transferir Bitcoins pela rede para fazer praticamente qualquer coisa que possa ser feita com moedas convencionais, incluindo comprar e vender mercadorias, enviar dinheiro para pessoas ou organizações ou conceder crédito. O Bitcoin pode ser comprado, vendido e trocado por outras moedas em trocas de moeda especializadas. O

Bitcoin, em certo sentido, é a forma perfeita de dinheiro para a Internet, porque é rápido, seguro e sem fronteiras.

Ao contrário das moedas tradicionais, o Bitcoin é totalmente virtual. Não há moedas físicas nem moedas digitais em si. As moedas estão implícitas em transações que transferem valor do remetente para o destinatário. Os utilizadores do Bitcoin possuem chaves criptográficas que lhes permitem provar a propriedade do Bitcoin na rede Bitcoin. Com essas chaves, eles podem assinar transações para desbloquear o valor e gastá-lo transferindo-o para um novo proprietário. As chaves são frequentemente armazenadas numa carteira digital no computador ou no smartphone de cada utilizador. A posse da chave criptográfica que pode assinar uma transação é o único pré-requisito para gastar Bitcoin, colocando o controle inteiramente nas mãos do utilizador.

O Bitcoin é um sistema distribuído, *peer-to-peer*. Como tal, não há servidor central ou ponto de controle. O Bitcoin é criado através de um processo chamado mineração, que envolve competir para encontrar soluções para um problema matemático durante o processamento de transações Bitcoin. Qualquer participante da rede Bitcoin pode operar como um mineiro, usando o poder de processamento de seu computador para verificar e registar transações. A cada 10 minutos, em média, um minerador de bitcoin é capaz de validar a transação dos últimos 10 minutos e é recompensado com um novo Bitcoin. Essencialmente, a mineração Bitcoin descentraliza as funções de emissão e compensação de moeda de um banco central e substitui a necessidade de qualquer banco central.

O protocolo Bitcoin inclui algoritmos integrados que regulam a função de mineração em toda a rede. A dificuldade da tarefa de processamento que os mineiros devem executar é ajustada dinamicamente de modo a que, em média, alguém consiga a cada 10 minutos, independentemente de quantos mineiros estejam competindo a qualquer momento, processar transações e obter partes de um Bitcoin. O protocolo também reduz pela metade a taxa em que o Bitcoin novo é criado a cada 4 anos, e limita o número total de Bitcoins que serão criados, para um total fixo abaixo de 21 milhões de “moedas”. O resultado é que o número de Bitcoins em circulação acompanha de perto uma curva facilmente previsível que se aproxima de 21 milhões até o ano 2140. Devido à taxa de emissão decrescente do Bitcoin, no longo prazo, é uma moeda Bitcoin deflacionária. Além disso, o Bitcoin não pode ser inflacionado "imprimindo" dinheiro novo, acima e além da taxa de emissão esperada.

Nos bastidores, o Bitcoin é também o nome do protocolo da rede *peer-to-peer* e uma inovação de computação distribuída. A moeda Bitcoin é realmente apenas a primeira aplicação desta invenção. O Bitcoin representa o culminar de décadas de pesquisa em criptografia e sistemas distribuídos e inclui quatro inovações-chave reunidas numa combinação única e poderosa. O Bitcoin consiste em:

a) Uma rede descentralizada *peer-to-peer*;
b) Uma transação razão pública (a Blockchain);
c) Um conjunto de regras para validação de transações independentes e emissão de moeda (regras de consenso);
d) Um mecanismo para alcançar o consenso global descentralizado sobre a *blockchain* válido (algoritmo de Prova de Trabalho).

2. História da Criptomoeda

A história das criptomoedas assenta principalmente em dois fundamentos. O primeiro é a dos sistemas distribuídos, em geral, a segunda é a história dos sistemas de dinheiro eletrónico. No início, estas duas áreas de investigação tinham muito poucas ligações uma com a outra, apesar da utilização comum de determinadas primitivas criptográficas. Ambos os campos de investigação estão relacionados com a investigação e avanços da criptografia, e em particular, com pesquisas na área do dinheiro eletrónico, área esta que foi impulsionada na investigação por invenções na área da criptografia assimétrica.

O termo "moeda virtual" foi definida pelo Banco Central Europeu, em 2014, como um representante digital de moedas-valores que não são emitidos por um banco central ou autoridade pública, nem necessariamente conectada a uma moeda fiduciária, mas é aceite por pessoas singulares ou coletivas, como meio de pagamento e podem ser transferidas, armazenadas ou trocadas por via eletrónica. [1] O Bitcoin insere-se neste tipo de moeda definido pelo Banco Central Europeu.

A história das moedas criptográficas começou na década de 1980, com o trabalho de David Chaum [2, 3]. Ele ficou conhecido como o inventor de sistemas seguros digitais em termos de primitivas criptográficas aplicadas a moeda digital. [4] Propôs um novo esquema de criptografia para tornar secreto o conteúdo de uma mensagem, antes de esta ser assinada. Estas assinaturas secretas podiam ser verificadas publicamente apenas como uma simples assinatura digital. A proposta de Chaum baseia-se numa caixa digital que permite aos utilizadores gastarem a moeda digital de tal forma que não seja detetável pela outra parte. Numa publicação posterior melhorou a ideia, permitindo transações offline, adicionando mecanismos de deteção de despesas duplas. No entanto, o sistema exige partes confiáveis para emissão e disponibilização do dinheiro eletrónico. [5] Para comercializar as suas ideias de dinheiro digital, Chaum fundou a DigiCash, em 1990. Essa primeira geração de moedas criptográficas não conseguiu chegar a uma larga audiência, apesar dos vários esforços de comercialização. [3]

O MOVIMENTO CYBERPUNK

Com os avanços de David Chaum neste campo, nasceu o movimento Cypherpunk. O grupo informal comunicava por meio da lista de discussão eletrónica: Cypherpunks, e defendia o uso de tecnologias de criptografia e melhoria de privacidade. Entre outros, o trabalho de David Chaum inspirou o grupo de ativistas a promover o uso generalizado destas tecnologias. Anterior a este movimento a criptografia não estava publicamente disponível aos consumidores, de uma forma geral, era maioritariamente usada pelas forças armadas e agências de informação. O movimento Cypherpunk abordou temas como o anonimato, o pseudoanonimato, privacidade na comunicação e ocultação de dados, mas também censura e monitorização. Uma questão importante, em meados da década de 1990, foi o *chipset* Clipper, desenvolvido pela NSA, que foi duramente criticado pelos Cypherpunks pela sua *backdoor* embutida. Em 1994, Matt Blaze publicou um artigo sobre vulnerabilidades no sistema de custódia do Clip-per Chip. [6] Ele descobriu que o chip transmitia informações que poderiam ser exploradas para recuperar a chave de criptografia num LEAF (Law Enforcement Access Field) específico. Este LEAF continha um *hash* de 16 bits para provar que a mensagem não era modificada, no entanto, os 16 bits, não eram suficientes como uma medida de integridade confiável, já que um invasor poderia facilmente forçar outro Valor de um LEAF, pois daria o mesmo *hash*, mas não as chaves corretas após uma tentativa de depósito. foram detetadas outras

vulnerabilidades, em 1995, por Moti Yung e Yair Frankel, que no seu trabalho mostraram que o rastreamento de dispositivos de garantia de chaves podia ser explorado anexando ao LEAF mensagens de dispositivos diferentes do original, para ignorar o depósito em tempo real. [7] Vários outros ataques têm sido publicados desde então, [4] e grupos ativistas, como a Electronic Frontier Foundation, também expressaram as suas preocupações sobre o chip Clipper e os esforços do governo para limitar o uso de criptografia aos utilizadores da Internet. Isso é comumente chamado de guerras criptográficas.

O inventor do *Hashcash*, Adam Back, foi pioneiro no uso do ultra-compactcode com seu RSA de 3 linhas no arquivo de assinatura Perl, que na altura foi impresso em T-Shirts para protestar contra os regulamentos de exportação de criptografia dos Estados Unidos. Devido à falta de adoção do Clipperchip pelos fabricantes de smartphones, o design foi abandonado em 1996. No entanto, o debate sobre chaves de depósito e *backdoors* controlados pelo governo persiste até esta data. As revelações de Snowden, em 2013, desencadearam uma onda de preocupação pública que resultou numa maior procura de aplicações criptográficos por utilizadores finais e fornecedores.

A ascensão das criptomoedas

Antes da primeira criptomoeda descentralizada, o Bitcoin e seus sucessores, surgiram várias abordagens que melhoraram a ideia original de David Chaum. Esses conceitos representaram melhorias incrementais, mas como ainda continham elementos centralizados, eles não se qualificam como moedas completamente descentralizadas.

Em 1998, Wei Dai propôs o b-money [8], um sistema de dinheiro eletrónico anónimo e distribuído. Na sua proposta, ele descreveu dois protocolos baseados na suposição de que existia uma rede não rastreável onde os remetentes e destinatários eram identificados apenas por pseudônimos digitais e pelas suas chaves públicas, em que toda mensagem é assinada pelo remetente e criptografada para envio ao preceptor. O b-Money também permitiu a criação de dinheiro digital com base em quebra-cabeças criptográficos, anteriormente não resolvidos.

Em 1998, Nick Szabo desenvolveu uma nova moeda digital chamada *goldbit*. O seu sistema era baseado em enigmas criptográficos que, depois de resolvidos, eram enviados a um registro público bizantino tolerante a falhas e atribuídos à chave pública do solucionador. Isso permitiu que fosse obtido o consenso da rede sobre novas moedas. Para resolver o problema do gasto duplo sem uma autoridade central, o esquema de Szabo foi projetado para imitar as características de confiança do ouro. Em 2002, Szaboalso apresentou uma teoria dos "colecionáveis" baseada nas origens do dinheiro. [9]

Adam Back propôs o *Hashcash* [10], um sistema de prova de trabalho (PoW) baseado em funções hash criptográficas para derivar a prova probabilística do trabalho computacional como um mecanismo de autenticação. Os requisitos deste sistema eram a dificuldade em encontrar uma solução válida, mas, por outro, ser fácil verificar qualquer solução dada. Com o *Hashcash*, o objetivo do PoW era garantir a dificuldade para um *spammer* transmitir e-mails por meio de uma transmissão anónima de e-mails [10]. Como a identidade do remetente devia ser protegida, nenhuma verificação de autenticação tradicional é possível nesse cenário. Portanto, o servidor de e-mail exigia a solução para um desafio computacional como um método de autenticação para aceitação da mensagem para retransmissão. No caso do *Hashcash*, isso foi realizado através de um cabeçalho de

e-mail adicional. O esquema de PoW de Back foi reutilizado conceptualmente na mineração de Bitcoin.

Baseado em trabalhos anteriores, em 2004, Hal Finney apresentou o primeiro sistema monetário baseado numa prova de trabalho reutilizável (RPOW) [11] e na teoria dos colecionáveis de Szabo [9]. Semelhante ao bit de ouro de Szabo, o esquema de Finney introduziu dinheiro em tokens, alinhado com o conceito do valor de ouro. Mais tarde, após o lançamento do Bitcoin, Hal Finney tornou-se o primeiro utilizador desta nova criptografia, pós Satoshi Nakamoto. Ele recebeu a primeira transação Bitcoin a partir do criador do Bitcoin, Satoshi Nakamoto.

BITCOIN
Entre 2008 e 2009, o Bitcoin foi a primeira criptomoeda descentralizada desenvolvida por Satoshi Nakamoto [12]. Nakamoto, em 2008, publicou um *whitepaper* sobre o Bitcoin e logo depois, em 3 de janeiro de 2009, criou o protocolo para o Bitcoin, baseado na cadeia de blocos (Blockchain), marcando o início do Bitcoin como uma criptomoeda descentralizada. Até á data, é a criptomoeda mais bem-sucedida em termos de capitalização de mercado. Mais de 700 *altcoins* com base no Bitcoin foram propostas desde o lançamento do Bitcoin (por exemplo, Litecoin, Peercoin).

3. Primitivas das tecnologias de criptomoedas

Neste tópico, descrevemos as primitivas criptográficas necessárias para entender os princípios das atuais criptomoedas baseadas em PoW. Os dois blocos básicos da estrutura, nesse contexto, são funções *hash* criptográficas e a criptografia assimétrica.

3.1 Funções Criptográficas Hash
As primitivas mais importantes no contexto das criptomoedas baseadas em PoW são funções *hash* criptográficas. Portanto, focamo-nos nas propriedades exigidas a tais funções, bem como nas construções que podem ser baseadas a partir dela, por exemplo, árvores Merkle.

Uma função *hash* W transporta uma mensagem x de tamanho arbitrário, mas finito, e gera um *hash* w de tamanho fixo (também chamado de *digest*). Quando não explicitamente declarado diferentemente, referimo-nos a uma função *hash* criptográfica sempre que o termo função *hash* for utilizado neste trabalho.

Têm de existir quatro propriedades adicionais numa função *hash* para que a função seja qualificada como uma função *hash* criptográfica [13]:

a) Ser computacionalmente fácil calcular o *hash* de qualquer mensagem finita,

$$w = W(x), \text{ onde } w \text{ é de comprimento fixo}$$

b) Ser inviável gerar uma mensagem que tenha um determinado valor de *hash*. Inviável neste contexto significa que não pode ser alcançado por um adversário desde que a segurança da mensagem seja importante. Em termos de teoria da complexidade, isto é definido como não sendo possível em tempo polinomial. Devido a esta propriedade, as funções *hash* criptográficas também são chamadas de funções unidirecionais.

Dado um *hash* h é inviável encontrar qualquer mensagem x tal que $w = W(x)$

c) É inviável encontrar duas mensagens diferentes que produzem saídas idênticas, isto é, uma colisão, quando dadas como entrada para a função hash.

Dada a mensagem m é inviável encontrar outra mensagem m' de tal modo que

$$y \neq y' \text{ e } W(y) = W(y')$$

d) Resistente a colisões: é inviável encontrar quaisquer duas mensagens diferentes que produzam saídas idênticas, isto é, uma colisão, quando dadas como entrada para a função hash.

É impossível encontrar duas mensagens m,m' onde

$$y \neq y' \text{ e } W(y) = W(y')$$

Merkle introduziu o conceito de um esquema de assinatura única que se baseia numa "árvore infinita de assinaturas únicas". Esse conceito subjacente ficou conhecido posteriormente como uma árvore Merkle, árvore de *hash* ou árvore de autenticação [13]. As árvores Merkle são árvores binárias nas quais os nós "folha" são rotulados com os valores que necessitam de ser autenticados e cada nó "não-folha" é rotulado com o *hash* dos rótulos ou valores de seus nós filhos, a Imagem 1 mostra um exemplo da árvore Merkle com n = 4 e o hash de raiz resultante ou a raiz da árvore de Merkle r. Para autenticar um valor x_1 e provar que era parte de uma árvore Merkle com raiz hash r, são necessários os valores w_2 e w_6. [14]

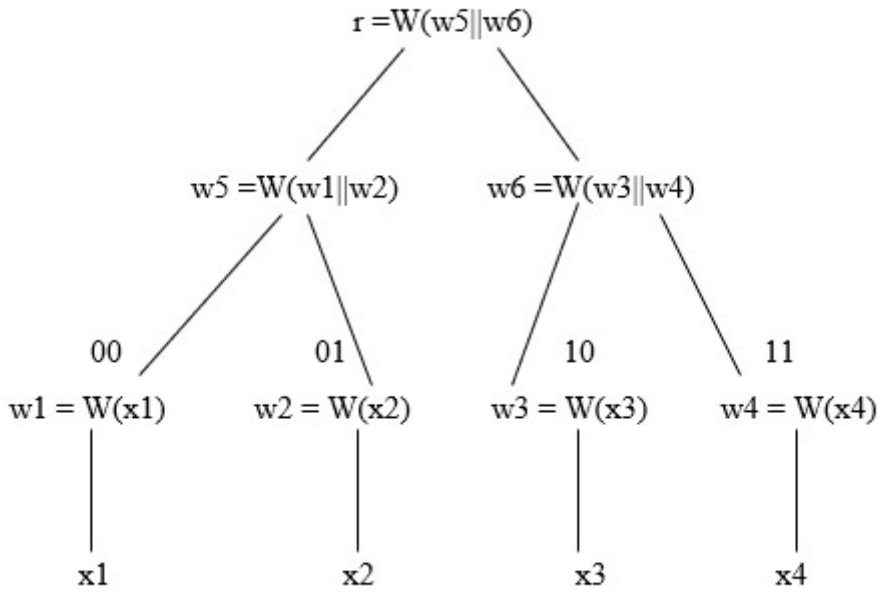

Imagem 1: exemplo de uma árvore de Merkle em que n = 4.

Algumas das propriedades da árvore de Merkle são:

a) O comprimento do caminho de qualquer folha até a raiz de uma árvore binária (balanceada) com n folhas é aproximado por $\log_2(n)$,

b) Dado um hash de raiz r e um valor x, para provar que x é realmente uma folha de uma árvore binária de Merkle (balanceada) requer cálculos de computação de aproximadamente $\log_2(n)$.

3.2 Criptografia Assimétrica

A segunda primitiva mais importante na qual as moedas criptográficas se baseiam é a criptografia assimétrica.

A criptografia assimétrica, mais conhecida como criptografia de chave pública, acompanha o problema de distribuição de chaves à medida que cada utilizador cria suas próprias chaves:

a) a chave privada que é mantida segura e nunca é distribuída,

b) a chave pública que pode ser enviada para qualquer pessoa com quem se queira trocar informações criptografadas.

Ao contrário da criptografia simétrica, as duas chaves comportam-se de maneira diferente; a chave pública é a única chave que pode decifrar o texto cifrado/criptografado usando a chave privada correspondente, a chave privada é a única chave capaz de decifrar os arquivos criptografados com a chave pública correspondente. Crucialmente, o valor de uma chave não pode ser facilmente determinado a partir da outra, portanto, mesmo que a chave pública "caia" em mãos hostis, o valor da chave privada não pode ser determinado. [14]

As chaves públicas podem ser distribuídas através de anexos de email ou através de servidores de chave de cadeia pública que atuam como distribuidores para um grande número de chaves públicas. A entidade criadora de uma chave pública faz o *upload* da sua chave para o servidor de distribuição e ficará disponível gratuitamente para qualquer pessoa que deseje utilizá-la.

Embora a matemática que está na base da criptografia de chave pública ser incrivelmente complexa, o processo de utilização é relativamente simples. Enviar uma mensagem usando criptografia de chave pública é simples. O remetente obtém uma cópia da chave pública do destinatário, por e-mail ou de um servidor de distribuição, e utiliza-a para criptografar a mensagem. O texto cifrado resultante é então enviado ao destinatário que usa a sua chave privada correspondente para decifrar o texto original. [14]

A criptografia de chave pública é popular porque não é necessária nenhuma troca segura inicial de chaves secretas para que uma mensagem criptografada seja enviada. No entanto, geralmente é muito mais lenta do que a criptografia simétrica; as técnicas tradicionais de criptografia de chave pública exigem que chaves sejam muito mais longas e ofereçam o mesmo nível de proteção que a criptografia simétrica. Um novo tipo de criptografia de chave pública, conhecido como "criptografia de curva elíptica", [14] pode ser tão seguro quanto a criptografia simétrica usando comprimentos de chave semelhantes.

ENCRIPTAÇÃO DE CHAVE PÚBLICA

Um esquema de criptografia de chave pública é definido como um triplo de algoritmos eficientes $\mathscr{E}$ = (A,B,C) onde:

a) A é um algoritmo de geração de chaves que não recebe nenhuma entrada e gera um par de chaves (xf; wf), onde xf é chamado de chave pública, que pode ser compartilhada publicamente, e wf é chamado de chave secreta, que deve ser mantido em sigilo.

$$(xf, wf) \leftarrow A()$$

b) B é um algoritmo de criptografia que recebe como entrada um pacote de chave pública, bem como uma mensagem m € Y e gera um texto cifrado t € T criptografado sob o xf de chave pública associado ao par de chaves pública/secreta (xf; wf) do destinatário pretendido.

$$t \leftarrow B(xf, y)$$

c) C é um algoritmo de decodificação (determinístico) que toma como entrada uma chave secreta wf, bem como a cifra o texto c € T e emite a mensagem m € Y, que foi criptografada sob a chave pública xf associada com wf, ou $\perp$ se as chaves erradas foram usadas.

$$Y \leftarrow C(wf, t)$$

Segue-se que se as operações respetivas são reversíveis $\forall$(xf; wf) de A afirma que:

$$\forall\ m \in Y : C(wf, B(xf, y) = y$$

ASSINATURAS DIGITAIS

Uma assinatura digital é uma técnica matemática usada para validar a autenticidade e integridade de uma mensagem, software ou documento digital. O equivalente digital de uma assinatura manuscrita ou selo carimbado, uma assinatura digital oferece muito mais segurança inerente, e destina-se a resolver o problema de adulteração e representação nas comunicações digitais.

As assinaturas digitais funcionam bem porque a criptografia de chave pública depende de duas chaves criptográficas mutuamente autenticadas. O indivíduo que cria a assinatura digital usa sua própria chave privada para criptografar dados relacionados à assinatura; a única maneira de decifrar esses dados é com a chave pública do próprio. A tecnologia de assinatura digital exige que todas as partes acreditem que o indivíduo que criou a assinatura conseguiu manter sua própria chave privada em segredo. Se a outra pessoa tiver acesso à chave privada do assinante, essa parte poderá criar assinaturas digitais fraudulentas em nome do detentor da chave privada. [14]

Um esquema de assinatura digital é definido como um triplo de algoritmos eficientes: $\wp$ = (D, E, F) onde:

a) D é um algoritmo de geração de chaves que não recebe nenhuma entrada e gera um par de chaves (xf; wf), onde xf é chamado de chave pública, que pode ser compartilhada publicamente, e wf é chamado de chave secreta, que deve ser mantido em sigilo.

$$(xf, wf) \leftarrow D()$$

b) E é um algoritmo de assinatura que recebe como entrada uma chave secreta wf, bem como uma mensagem m € Y e gera uma assinatura ð € $\sum$ que pode ser comunicada publicamente juntamente com a mensagem. E é invocado como:

$$E : ð \leftarrow B(wf, y)$$

c) F é um algoritmo (determinístico) que toma como entrada uma chave pública xf como uma mensagem m € Y bem como uma assinatura ð € $\sum$ e saídas do tipo: aceitar ou rejeitar, dependendo da validade da assinatura ð na mensagem m.

$$\{aceite, rejeitada\} \leftarrow F(xf, y, ð)$$

Então uma assinatura gerada por S é aceita por F se e só se (xf; wf) for um par válido da chave pública/secreta. Então ∀ (xf; wf) de D determinará que:

$$\forall y \in : \in(xf, y, E(wf, y)) = \text{aceite}$$

4. Bitcoin

Em 2016, a capitalização de mercado da Bitcoin alcançou mais de 10 bilhões de dólares [15], provando que projetar e manter uma moeda criptográfica distribuída é tecnicamente viável hoje em dia. Embora as primitivas técnicas, que são essencialmente funções *hash* criptográficas, e a criptografia assimétrica existam há muito tempo, o Bitcoin foi o primeiro conceito a combinar estes componentes técnicos com um sistema de incentivo, criando assim a primeira moeda criptográfica distribuída da história. Neste tópico, descrevemos o Bitcoin como o arquétipo das *blockchains* modernas baseadas em provas de trabalho distribuídas.

4.1 Perspetiva geral

O Bitcoin e outras criptomoedas dependem de dois tipos diferentes de estruturas de dados: transações e blocos. As transações são agrupadas em blocos. Os blocos estão encadeados através de *hashes* dos seus predecessores, formando assim uma estrutura de dados autenticada, a *blockchain* [16]. Transações e blocos são disseminados entre todos os nós participantes usando um protocolo de rede do tipo *peer-to-peer* (P2P). É adicionado um novo bloco á *blockchain* se um nó da rede puder fornecer uma prova de trabalho (PoW) para isso. O PoW age como um mecanismo de defesa contra-ataques de Sybil [17] e fornece uma forma de assinatura sem chave para autenticar novos blocos, bem como o blockchain como um todo [18]. Os nós honestos concordam que, em qualquer momento, apenas a maior *blockchain* é considerada válida. Embora comumente referido como regra de cadeia mais longa, é na verdade a *blockchain* mais difícil de calcular em termos de PoW, ou seja, a cadeia mais pesada. Se um nó não considerar um bloco válido, então o bloco não é adicionado á sua blockchain. Este consenso implícito pode ser considerado como um processo de uma "eleição de líder aleatório" em cada PoW resolvido. Ao líder é permitido propor um novo bloco e implicitamente concordar em todos os blocos antes desse, acrescentando um novo bloco ao final da respetiva *blockchain* [16]. Em suma, o Bitcoin pode ser descrito como um sistema distribuído que usa PoW e uma *blockchain* como um mecanismo de consenso probabilístico para concordar com o conjunto contido de transações, bem como o seu pedido. Assim, o sistema garante que todos os pares concordem com o atual *status* de propriedade dos bitcoins. Isso é necessário para manipular corretamente as transições de estado na propriedade de um bloco para o próximo bloco. Neste trabalho este consenso para alcançar esse objetivo é referido como consenso Nakamoto. Assim, o líder tem a permissão para decidir num bloco, depois outro líder é eleito baseado na solução de um quebra-cabeça PoW. Os líderes sinalizam a sua aprovação dos blocos anteriores, acrescentando-a ao legítimo, na blockchain. A probabilidade de concordar com um prefixo comum de blocos na cadeia mais pesada aumenta em direção a P r (1) à medida que as cadeias se tornam maiores [19].

Para motivar as pessoas a fornecerem os seus recursos computacionais e executar os nós Bitcoin, os chamados mineiros são recompensados com unidades monetárias (ou seja, bitcoins) para cada PoW válido fornecido para um bloco e suas transações associadas.

Como resultado, a segurança e a descentralização do Bitcoin não vêm apenas de aspetos técnicos, mas também da inteligente engenharia de incentivos [16].

4.2 Estruturas principais e conceitos

Endereços, transações e blocos são as três estruturas básicas de dados usadas no Bitcoin. A necessidade destas estruturas de dados específicas surgiu do fato do Bitcoin ter sido projetado como uma moeda digital distribuída. Todas as moedas criptográficas baseadas no Bitcoin, sejam elas garfos diretos (por exemplo, Namecoin, Litecoin, Zcash) ou apenas conceptualmente baseadas neles (por exemplo, Ethereum), também incluem variantes destas estruturas de dados centrais com algumas pequenas modificações. Este subtópico descreve essas estruturas e mostra como elas se interligam de forma a delinearem os conceitos básicos de uma moeda criptográfica. Para simplificar, assumimos neste subtópico que a ordem dos blocos na cadeia é acordada por cada cliente e que cada cliente conhece pelo menos o atual líder da cadeia. Durante a vida útil do Bitcoin, houve pequenas alterações na representação e interpretação exatas das estruturas de dados principais, por exemplo, a interpretação do valor da Versão (nVersão) do cabeçalho do bloco, que originalmente representava apenas um número de versão crescente e agora é interpretado como vetor de bits, para que os mineradores possam indicar se suportam recursos que exigem um garfo simples.

BLOCO

A estrutura de dados mais fundamental no Bitcoin é um bloco. Um bloco consiste num cabeçalho nas transações associadas ao respetivo bloco. Esses blocos são encadeados, incluindo hashes criptográficos dos seus antecessores para formar uma lista vinculada comumente chamada de *blockchain*. O estado atual da moeda é representado pela ordem dos blocos na cadeia. Eles representam um *ledger* de todas as transações realizadas, nas quais as transações são processadas sequencialmente dependendo de sua posição no bloco em que ocorrem.

BLOCKCHAIN

O termo blockchain, embora não seja diretamente introduzido por Satoshi Nakamoto no artigo original [12], é comumente usado como um termo genérico para se referirem conceitos relacionados com a criptografia aplicada a tecnologias monetárias. Podemos defini-la como uma estrutura de dados de lista vinculada, que usa somas de *hash* sobre os seus elementos como ponteiros para os respetivos elementos. Se considerarmos esta definição, a construção de uma *blockchain* garante que, contanto que alguém tenha armazenado ou recuperado o bloco correto na ponta da cadeia, ele seja capaz de verificar os os outros blocos da corrente quando fornecidos na sua totalidade, como é ilustrado na Imagem 2.

ENDEREÇOS

Os endereços Bitcoin, como os endereços de muitas outras moedas criptográficas, são *hashes* criptográficos de chaves públicas. Portanto, cada endereço na verdade consiste numa parte pública e outra parte privada. A parte pública é o endereço, que pode ser comparado a um número de conta num banco on-line. A parte privada é a chave secreta correspondente, que pode ser comparada à senha ou assinatura exigida para retirar dinheiro de uma conta de poupança comum. Os endereços podem ser gerados por qualquer pessoa tão facilmente quanto os pares de chave pública/privada. Isto permite que todos aceitem Bitcoins distribuindo o endereço público sem qualquer conhecimento mais profundo do próprio protocolo Bitcoin ou dos seus mecanismos de consenso.

No Bitcoin, os endereços são um par de chaves pública/privada do Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA) [20]. Mais precisamente, o Bitcoin usa a curva elíptica secp256k1 especificada e recomendada pela Certicom [21]. Para criar um endereço Bitcoin processável, a parte pública é codificada conforme descrito no Algoritmo ABC (exemplificado a seguir a este parágrafo). No processo, a chave pública é dividida várias vezes. Deste modo, são utilizadas duas funções *hash* diferentes, isto é, RIPEMD160 e SHA256 [22].

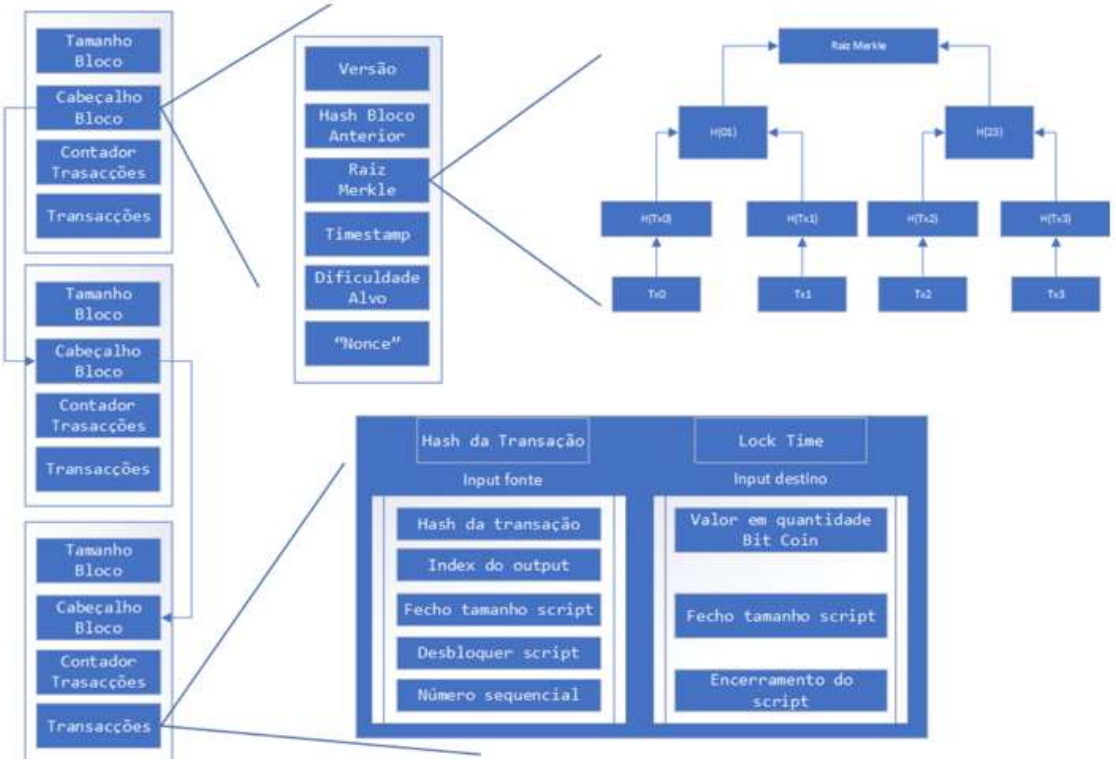

Imagem 2: Composição da Blockchain

Algoritmo ABC (exemplificação), construção de endereços Bitcoin de chaves públicas ECDSA: [22]
Input: ECDSA chave pública pk
Output: endereço Bitcoin A e.g., 1DR8mXZpK75q7Vipkb1tmp8Wyjz6gDHZBL
1: a = 0x00 || RIPEMD160(SHA256 8pk))
2: h = SHA256(SHA256(a))
3: A = Base58(a || H[251 : 255])

TRANSAÇÃO
As transações são usadas para transferir unidades monetárias de um endereço para outro. Elas podem ser criadas por qualquer entidade que possua unidades monetárias, ou seja, Bitcoins. Posse neste contexto significa controlar a chave privada do respetivo endereço que no momento detém as unidades monetárias que devem ser transferidas, isto é, um endereço que tenha recebido transações no passado.

Uma transação no Bitcoin consiste numa ou várias entradas e uma ou várias saídas. Uma entrada desbloqueia uma saída anterior, fornecendo uma assinatura criptográfica válida. Deste modo, as entradas servem como prova de que o portador do respetivo endereço Bitcoin que recebeu anteriormente os Bitcoins também está na posse da chave privada requerida. A chave privada é necessária para gerar a assinatura que desbloqueia os fundos para que eles possam ser usados, ou seja, transferidos para outro endereço de Bitcoin.

Por exemplo, se Joana quiser transferir 5 bitcoins para João, ela primeiro necessita do endereço Bitcoin do João. Para o nosso exemplo, supomos que esse endereço é transferido por algum canal de comunicação confiável, por exemplo, exibido como informações de pagamento ao fazer compras num website que usa um certificado válido para criptografia TLS [23]. A Joana coloca o endereço do João na saída da transação que está construindo junto com o número de moedas que deseja transferir para essa conta, ou seja, 5. Na etapa seguinte, a Joana precisa provar que está na posse do número necessário de moedas Bitcoins e que ela realmente quer transferi-los para o João. Portanto, a Joana pesquisa no *blockchain* por transações anteriores em que os Bitcoins foram enviados para endereços que estão sob seu controle, ou seja, onde ela está na posse das chaves privadas correspondentes. Em seguida, ela desbloqueia o número de transações anteriores necessárias para cobrir a saída desejada de 5 bitcoins. No nosso exemplo, ela usa duas transações (saídas) anteriores para isso, consistindo de 4 e 3 bitcoins. Referindo-se às respetivas transações anteriores, Joana cria uma entrada na transação atual para cada saída que deseja desbloquear. Essas entradas identificam exclusivamente as saídas anteriores pelo seu ID e número de transação. Para desbloquear essas saídas, ela precisa de provar que é a legítima proprietária, o que ela faz fornecendo assinaturas criptográficas e todas as entradas.

A Joana, agora, adiciona uma saída à transação que transfere 5 Bitcoins para o endereço Bitcoin do João. Como as duas entradas desbloqueadas somam mais do que o valor desejado de 5 Bitcoins, a Joana acrescenta outra saída para transferir a mudança de 2 Bitcoins de volta para um endereço Bitcoin que está sob o seu controle. Assim que a transação é construída, a Joana transmite-a para a rede *peer-to-peer* Bitcoin e aguarda até que seja incluída num bloco recém-gerado. Depois da transação ser incluída na cabeça do *blockchain*, a transação é chamada como confirmada. O número de confirmações é definido pelo número de blocos criados em cima do bloco que contém a transação.

Uma transação em Bitcoins é considerada válida se cumprir os seguintes critérios:
a) Todas as entradas desbloqueadas não foram gastas (isto é, desbloqueadas e usadas) numa transação anterior.
b) Todas as assinaturas criptográficas nos inputs são válidas.
c) A soma de todos os valores desbloqueados nas entradas é maior ou igual à soma de todos os valores especificados nas saídas da transação.

4.3 Administração do Consenso

Este subsistema contém todas as partes críticas do consenso, ou seja, as regras nas quais a maioria dos nós participantes tem que concordar para chegar a um consenso sobre o estado da *blockchain*. Por outras palavras, se houver um acordo sobre a validade e ordem dos blocos na cadeia, então há também um acordo sobre a ordem das transações. Isso é necessário para determinar se uma determinada transação é válida, isto é, se usa apenas saídas de transação que não foram gastas até ao momento.

O consenso aleatório no Bitcoin é baseado na prova de trabalho para selecionar aleatoriamente o nó na rede que será o líder da próxima "rodada" (ou seja, o próximo bloco). Ao líder é permitido propor o próximo bloco, então outro líder é escolhido de acordo com o mesmo princípio e assim por diante. Após este processo, o líder atual pode implicitamente concordar com a cadeia a que estava conectado anteriormente, anexando o seu *bock* recém-criado à frente da cadeia ou discordando escolhendo um bloco diferente, ou seja, criado anteriormente, para anexar. A chance de um nó ser selecionado como líder depende de seu poder de *hashing* relativo em comparação com todos os outros nós.

Portanto, qualquer nó pode aumentar suas chances de ser selecionado aumentando a sua participação computacional. De acordo com as estimativas atuais, esse mecanismo pode ser considerado seguro contra um nó malicioso participante no consenso, desde que sua participação não aumente acima de 25% da taxa global de *hash*. Este valor assemelha-se a uma estimativa atual e é o resultado de um processo ainda em curso para modelar e avaliar as garantias de segurança da *blockchain* PoW [24], sob certos ataques [25, 26] e combinações destes [27]. Além da seleção aleatória, a prova de trabalho também atua como uma proteção contra ataques de Sybil [17] em Bitcoins. Isto é necessário desde os nós possam entrar (e sair) da rede Bitcoin P2P e iniciar (ou parar) a participação no protocolo.

A partir dessa perspetiva, a prova de trabalho garante que um invasor necessita efetivamente do respetivo poder computacional para gerar novos blocos e, portanto, influenciar diretamente o processo de consenso.

4.4 Prova de trabalho

Uma prova de trabalho (PoW) no contexto da ciência da computação é um mecanismo que permite que um sistema de teste forneça evidências para um verificador em como ele investiu recursos computacionais (por exemplo, CPU e memória) numa determinada tarefa. Existem diferentes definições e requisitos relativos à construção de tais provas [28, 29, 30, 31]. Concentramos nos aspetos mais relevantes no contexto das tecnologias de moeda criptográfica. Neste domínio, este tipo de quebra-cabeças são, às vezes, também denominados de quebra-cabeças de *hash* [16], quebra-cabeças computacionais, quebra-cabeças moderadamente difíceis ou quebra-cabeças arranhados [32]. Num nível abstrato, as principais características que um PoW, no contexto de moedas criptográficas, deve cumprir podem ser resumidas da seguinte forma:

a) Qualquer dado PoW é fácil de verificar.
b) O PoW gera-se dificilmente.
c) A dificuldade da PoW é parametrizável.
d) Não deve ser possível reutilizar PoWs gerados anteriormente.
e) Não deve ser possível gerar PoWs antecipadamente e usá-los posteriormente.

.

Os três primeiros são os requisitos básicos para um PoW, e também são altamente relevantes para outros cenários de aplicação. Os requisitos 4 e 5 são particularmente relevantes no contexto de moedas criptográficas, como demonstraremos neste subtópico. Os requisitos 1, 2 e 3 são cumpridos devido às propriedades da função *hash* criptográfica subjacente. O PoW é fácil de verificar, pois dado o valor PoW ser o resultado da função *hash* subjacente e, portanto, poder ser verificado executando novamente a função *hash* na mesma entrada (fácil de calcular). O PoW é difícil de gerar, isto é, apenas através da pesquisa de força bruta, porque é inviável gerar mensagens que correspondam a uma saída

específica de uma função *hash* criptográfica (resistência de pré-imagem). A dificuldade do PoW é parametrizável porque existe um intervalo de valores de *hash* permitidos que são aceites como PoW válida. Expandir ou reduzir este intervalo torna o PoW mais fácil ou mais difícil. A reutilização de PoWs gerados anteriormente é dificultada pela imposição da estrutura da linha de cabeçalho no lado do servidor. O cabeçalho deve conter um registro de data e hora, o destinatário e um valor aleatório exclusivo. Além disso, o servidor deve verificar o valor aleatório e confirmar que ele não foi usado antes. Se este for o caso, um PoW válido não poderá ser reutilizado nem mesmo para o mesmo endereço de destinatário. Para minimizar o requisito de armazenamento no servidor para valores aleatórios já utilizados, o servidor só pode guardar os valores aleatórios para um determinado intervalo de tempo e descartar todas as mensagens que tenham um *timestamp* antigo como inválido. A última propriedade (5) também é preenchida pelo *hashslash*. É possível gerar uma PoW válida antes do tempo e usá-los mais tarde. Infelizmente é possível pré-gerar arbitrariamente muitos cabeçalhos válidos simplesmente configurando o *timestamp* para o valor desejado no futuro no qual as mensagens devem ser enviadas para o servidor. Dessa forma, um invasor pode pré-calcular quantos PoW desejar e usá-los no momento desejado, inundando o servidor com mensagens válidas. Embora tal ataque seja teoricamente possível, o invasor não pode evitar investir consideráveis recursos computacionais na computação desses cabeçalhos. Portanto, o envio de muitas mensagens de *spam* ainda é uma tarefa computacionalmente intensa. [32]

4.5 Mineração

Mineração é o processo de solução e disseminação de soluções PoW como um meio de chegar a um consenso sobre o estado atual do blockchain. Os nós que estão ativamente envolvidos na busca e que fornecem uma solução para o PoW são chamados de mineiros. Os mineiros são recompensados com unidades da Criptomoeda minada (por exemplo, Bitcoins) como uma compensação pelos seus esforços e por investirem poder computacional na segurança geral da Criptomoeda. Os mineiros podem entrar ou sair da rede a qualquer momento, aumentando ou diminuindo o poder de mineração. Portanto, a PoW *no blockchain* necessita ajustar a dureza do PoW para garantir que novos blocos sejam gerados em intervalos regulares. Quanto maior o número T, menor o número de soluções possíveis, resultando que a PoW seja mais difícil de encontrar. O valor máximo possível para T é definido em Bitcoin como $Tmax = 2^{224}$.

Isto assemelha-se a 32 bits de zero iniciais e, portanto, um número médio de 32 tentativas para encontrar uma solução.

Em dezembro de 2016, a meta era de $Tc = 2^{224}$ /254620187304. O alvo atual requer aproximadamente 2^{69} tentativas, em média, para encontrar uma solução. Para sustentar um intervalo de blocos de aproximadamente 10 minutos, um novo alvo Tn é definido a cada 2.016 blocos como uma função do tempo decorrido t:

$$Tn = Tc * \frac{t}{2{,}016 * 10 minutos}$$

A probabilidade de encontrar um novo bloco é distribuída exponencialmente e as recompensas de mineração são pagas em intervalos irregulares, uma vez que a *blockchain* não pode contabilizar todas as ações dos mineiros enquanto ajusta a dificuldade. O tempo médio necessário para encontrar um bloco (MTTB), ou seja, um PoW válido, pode ser calculado dependendo da ação p da taxa *hash* total. Quando o intervalo de bloco é de 10 minutos e se recebe uma percentagem de p em comparação com a taxa de *hash* total da

rede, o tempo médio para o próximo bloco encontrado é calculado como mostrado na Equação seguinte:

$$MTTB = 10 \text{ minutos} / p$$

4.6 Gastos em duplicado

Num sistema central, o gasto duplo pode ser facilmente detetado, uma vez que existe apenas uma entidade central responsável pela contabilidade. No domínio das moedas criptográficas distribuídas, a mitigação de ataques com gastos duplos é um problema central.

Vamos supor um cenário por exemplo em que Maria quer lançar um ataque de gasto duplo no ecossistema Bitcoin. De um modo geral, um ataque duplo de sucesso seria permitir que a Maria gastasse as mesmas unidades de moeda duas vezes. Para executar o ataque, Maria requeria alguns fundos, que ela podia tentar dobrar em gastos e um comerciante aceitaria Bitcoin em troca pelas mercadorias. Para o nosso exemplo, suponhamos que Manuel é um comerciante que administra um serviço de troca em que aceita Bitcoins em troca de dólares americanos (USD). Num cenário de gastos duplos o objetivo de Maria é convencer Manuel em como ela recebeu o número necessário de bitcoins, de modo a que ela envie o equivalente número de dólares em troca, enquanto convence o resto da rede Bitcoin que esta transação para Manuel nunca aconteceu. Para conseguir isso, Maria cria duas transações conflituantes que fazem referência à mesma saída de transação não utilizada (UTXO). Para o nosso exemplo, basta saber que uma transação Bitcoin é composta por um número variável de entradas e um número variável de saídas. Cada entrada desbloqueia a saída de uma transação anterior que ainda não foi usada, isto é, desbloqueada.

Uma transação no Bitcoin é válida se: [33]

a) Todas as suas entradas ainda não foram gastas, isto é, pertencem ao conjunto de UTXOs;

b) A soma de todas as unidades monetárias (Satoshis) desbloqueadas nas entradas é menor ou igual á soma de Satoshis nas saídas; e

c) o código do programa *Script* em todas as entradas é avaliado corretamente, ou seja, todas as assinaturas criptográficas fornecidas nessa transação estão corretas.

As propriedades de segurança do Bitcoin são baseadas na suposição de que a maioria do poder de mineração pertence aos mineiros honestos. Os primeiros trabalhos em modelagem de segurança em Bitcoin concluíram que o poder de mineração de todos os mineiros honestos tem que ser estritamente superior a 50%, de modo a sustentar a segurança do blockchain [33, 12, 34]. Se os mineiros desonestos têm a maioria do poder de mineração, eles podem controlar a inserção de novas transações na *blockchain* e na transação da taxa de mercado, portanto, o fornecimento de moedas recém-minadas. Por outras palavras, todas as propriedades de um sistema projetado para funcionar sem um terceiro elemento confiável é substituído por um monopólio de mineração.

Trabalhos mais recentes encontraram estratégias de ataque que podem ser bem-sucedidas mesmo sem controle da maioria do poder de mineração. Exemplos incluem o bloqueio de retenção [26] de ataques como mineração egoísta [35], ataques de eclipse [36], bem como combinações dos mesmos, denominada mineração teimosa [24, 27]. Esses ataques estão relacionados com a disseminação de informações e visam isolar a rede e particioná-la em

clusters desconectados. Retendo ou reprimindo de outra forma a propagação de informação de novos blocos gerados, alguns nós maliciosos podem enganar os participantes honestos em "desperdiçar" o seu poder computacional através da mineração em blocos obsoletos ou antigos que já têm sucessores. A probabilidade de sucesso de tais ataques aumenta com a quota de energia mineira (a) e o nível de conectividade (y) do atacante. Abaixo de um certo limite para estes parâmetros, a mineração honesta supera essas estratégias de ataque. Um atacante mal conectado ($y \approx 0,1$) requer um $a \geq 0,33$ para executar com sucesso um ataque de mineração egoísta [120]; um atacante conectado a metade dos nós ($y \approx 0: 5$) precisaria de um número ainda menor a $\geq 0,25$. Portanto, 25% é atualmente considerado um limite inferior conservador no poder de mineração exigido para que um atacante obtenha uma vantagem usando essas estratégias de ataque. [24, 27,35, 36]

5. Conclusão

O protocolo Bitcoin é uma mistura inteligente de tecnologias e conceitos de diferentes áreas que em combinação criou algo notável. A maioria das primitivas usadas, como o encadeamento de funções *hash* criptográficas, criptografia assimétrica ou prova de trabalho, eram conhecidas e foram estudadas antes do aparecimento do Bitcoin. A novidade do Bitcoin está na fusão dessas tecnologias com um sistema de incentivo baseado na teoria dos jogos e num caso de uso prático, ou seja, numa moeda digital. Isto criou um novo tipo de sistema de consenso distribuído probabilístico apelidado de consenso Nakamoto. A novidade deste mecanismo é que ele permite que o anonimato e a participação no processo de consenso através do processo de mineração sem a necessidade de algum tipo de procedimento prévio de configuração confiável. O Bitcoin não é a resposta para tudo, mas sem dúvida teve impacto em muitas áreas e comunidades: criou uma nova classe de sistemas de consenso aleatórios e reacendeu a pesquisa no campo de consenso distribuído e sistemas tolerantes a falhas bizantinos, em geral. É uma comunidade viva e diversificada que está impulsionando o desenvolvimento desse conjunto de tecnologias.

A publicação on-line do original, a implementação de *software* e o desenvolvimento posterior da comunidade nos seus primórdios superaram a pesquisa académica tradicional e os ciclos de publicação. Isto demonstrou que se pode implementar e executar um sistema digital descentralizado com uma capitalização de mercado de milhões de milhões de dólares, antes mesmo de ter um modelo teórico a funcionar a cem por cento. Mostrou que o pensamento interdisciplinar pode levar a novas abordagens e soluções com aplicações práticas.

Enquanto o Bitcoin e a *blockchain* dificilmente são a resposta para a vida, o universo ou a medicina, a fusão das suas tecnologias subjacentes e os métodos utilizados abriram novos caminhos e delinearam novas possibilidades em diferentes áreas de pesquisa.

Além disso, as tecnologias da moeda criptográfica também têm uma dimensão sociológica e prática com potencial disruptivo. Nunca antes foi tão fácil criar uma moeda que pode ser usada em todo o mundo sem a absoluta necessidade de um terceiro elemento confiável (exemplo: bancos) ou a exigência de distribuir moedas e notas físicas. Esta mudança de paradigma obriga-nos a repensar o conceito de dinheiro e moedas e permite-nos imaginar um futuro em que uma infinidade de diferentes criptografias podem permitir

a existência de uma criptomoeda mais justa para as sociedades. Contanto que existam métodos para usar facilmente diferentes moedas criptográficas e também para trocar ativos entre elas, não será necessário contar com apenas com uma criptomoeda para tudo. Por último, é inquestionável que a investigação criptográfica permitiu, pelo menos, apresentar uma solução alternativa ao modelo clássico e monopolista dos bancos, e apresentar uma solução exequível mais justa para o uso do dinheiro. Logo mais vantajosa para a Humanidade.

Que os grandes bancos vão fazer tudo para que as moedas criptográficas não vinguem, é um facto que damos como certo.

REFERÊNCIAS

[1] E. B. Authority. Eba opinion on virtual currencies. http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf,2014.

[2] Namecoin. https://namecoin.org/

[3] Requiem of a Bright Idea. http://www.forbes.com/forbes/1999/1101/6411390a.html

[4] D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology, pages 199–203. Springer, 1983. DOI: 10.1007/978-1-4757-0602-4_18.

[5] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In Proc. on Advances in Cryptology, pages 319–327. Springer-Verlag, New York, 1990. DOI: 10.1007/0-387-34799-2_25.

[6] M. Blaze. Protocol failure in the escrowed encryption standard. In Proc. of the 2nd Conference on Computer and Communications Security, pages 59–67. ACM, 1994. DOI:10.1145/191177.191193.

[7] Y. Frankel and M. Yung. Escrow encryption systems visited: Attacks, analysis and designs. In Annual International Cryptology Conference, pages 222–235. Springer, 1995. DOI: 10.1007/3-540-44750-4_18.

[8] W. Dei. B-money. http://www.weidai.com/bmoney.txt

[9] N. Szabo. Shelling out: The origins of money. http://nakamotoinstitute.org/shelling-out/, 2002. Accessed: 2017-06-09.

[10] A. Back et al. Hashcash-a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf, 2002.

[11] H. Finney. Reusable proofs of work (RPOW). http://web.archive.org/web/20071222072154/http://rpow.net/, 2004.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[13] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996. DOI: 10.1201/9781439821916.

[14] G. Becker. Merkle signature schemes, merkle trees and their cryptanalysis. Ruhr-University Bochum, Technical Report, 2008.

[15] Coinmarketcap. http://coinmarketcap.com/

[16] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. Bitcoin and cryptocurrency technologies. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf ?a=1, 2016.

[17] J. R. Douceur. The sybil attack. In International Workshop on Peer-to-peer Systems, pages 251–260. Springer, 2002. DOI: 10.1007/3-540-45748-8_24.

[18] R. Pass, L. Seeman, and A. Shelat. Analysis of the blockchain protocol in asynchronous networks. http://eprint.iacr.org/2016/454.pdf, 2016. DOI: 10.1007/978-3-319-56614-6_22.

[19] J. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology-EUROCRYPT, pages 281–310. Springer, 2015. DOI: 10.1007/978-3-662-46803-6_10.

[20] Certicom Research. SEC 1: Elliptic Curve Cryptography, Version 2.0. http://www.secg.org/sec1-v2.pdf, 2009.

[21] Certicom Research. SEC 2: Recommended elliptic curve domain parameters, version 2.0. http://www.secg.org/collateral/sec2_final.pdf, 2010

[22] NIST. FIPS 180-4: Secure hash standard (SHS), 2012.

[23] T. Dierks and E. Rescorla. The transport layer security (TLS) protocol, version 1.2. RFC 5246 (proposed standard), 2008. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568,7627, 7685. DOI: 10.17487/rfc5246.

[24] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. https://eprint.iacr.org/2016/555.pdf, 2016. DOI: 10.1145/2976749.2978341.

[25] I. Eyal. The miner's dilemma. In Security and Privacy (SP), Symposium on, pages 89–103. IEEE, 2015. DOI: 10.1109/sp.2015.13.

[26] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography and Data Security, pages 436–454. Springer, 2014. DOI: 10.1007/978-3-662-45472-5_28.

[27] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In 1st European Symposium on Security and Privacy, IEEE, 2016. DOI: 10.1109/eurosp.2016.32.

[28] L. Chen, P. Morrissey, N. P. Smart, and B. Warinschi. Security notions and generic constructions for client puzzles. In International Conference on the Theory and Application of Cryptology and Information Security, pages 505–523. Springer, 2009. DOI: 10.1007/978-3-642-10366-7_30.

[29] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In Annual International Cryptology Conference, pages 139–147. Springer, 1992. DOI: 10.1007/3-540-48071-4_10.

[30] B. Groza and B. Warinschi. Cryptographic puzzles and dos resilience, revisited. Designs, Codes and Cryptography, 73(1):177–207, 2014. DOI: 10.1007/s10623-013-9816-5.

[31] D. Stebila, L. Kuppusamy, J. Rangasamy, C. Boyd, and J. G. Nieto. Stronger difficulty notions for client puzzles and denial-of-service-resistant protocols. In Cryptographers Track at the RSA Conference, pages 284–301. Springer, 2011. DOI: 10.1007/978-3-642-19074-2_19.

[32] A. Miller, A. Kosba, J. Katz, and E. Shi. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In Proc. of the 22nd Conference on Computer and Communications Security (SIGSAC), pages 680–691. ACM, 2015. DOI: 10.1145/2810103.2813621.

[33] A. Miller and L. JJ. Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin. https://socrates1024.s3.amazonaws.com/consensus.pdf, 2014.

[34] M. Rosenfeld. Analysis of hashrate-based double spending. http://arxiv.org/abs/1402.2009, 2014.

[35] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. http://arxiv.org/pdf/1507.06183.pdf, 2015.

[36] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. In 24th Security Symposium (USENIX Security 15), pages 129–144, 2015.

Pedro Ramos Brandão: Presidente do Conselho Científico do ISTEC. Coordenador do Mestrado em Informática no ISTEC. Diretor da Pós-Graduação em Virtualização e Cloud Computing no ISTEC. Professor Coordenador do ISTEC. Investigador Integrado na Universidade de Évora (CIDEHUS). Doutorado em História Política Contemporânea (FOS: História), ISCTE; Doutoramento em Ciências da Informação (FOS: Ciências da Computação e da Informação), Universidade de Évora; Mestrado em Segurança da Informação e Crime no Ciberespaço (Instituto Superior Técnico), Mestrado em História Moderna e Contemporânea (ISCTE), Licenciado em História (UL), Licenciado em Engenharia Multimédia (ISTEC), *Post Graduate Training - Cybersecurity: Technology, Application and Policy (Massachusetts Institute of Technology - MIT), Post Graduate Training - Cybersecurity Risk Management (Rochester Institute of Technology – RIT).* Diretor da Revista com Arbitragem Científica: Kriativ-Tech. Scientific Reviewer at "International Journal of Information and Communication Sciences – USA. Scientific Reviewer at "International Scientific Conference Theoretical and Practical Aspects of Distance Learning", University of Silesia in Katowice (Poland). Editorial Board Member of Journal of Computer, USA. Scientific Committee Member of International Conference on Virtual and Networked Organizations Emergent Technologies and Tools.