UM CAFÉ COM O PROTOCOLO BITCOIN

i2e

https://i2e.online

Título
Um café com o protocolo Bitcoin

Edição de autor
Outubro de 2021

Edição ebook e edição impressa

Design e composição gráfica
#legendavisual

ISBN 978-989-33-2523-0

Para:

To:

Índice

Parte 1
Contextualização

Nota Introdutória

Capítulo 1 – Blockchain e Bitcoin

- Enquadramento Tecnológico e Económico
  - Blockchain a Cadeia de Blocos
  - A Função Hash ou impressão digital do bloco
  - O Padrão Ouro, Bretton Woods e Bitcoin
  - Bitcoin e Satoshi Nakamoto
- Bitcoin como blockchain e moeda
  - Trilema das blockchains
  - Prova de trabalho. O Mining ou mineração de Bitcoins
  - Halvings e o modelo deflacionário
  - Economia do Bitcoin
  - Bitcoin a unidade. Satoshi a fração

Capítulo 2 - Conviver com Bitcoins

- Criptografia e Carteiras de Criptomoedas
  - Carteiras de criptomoedas
- Exchanges, Plataformas de aquisição.
- Como obter Bitcoins
  - Conta no Exchange
  - Programas de remuneração
- Já tenho Bitcoins e agora?
- Problema da escalabilidade
- Transações, mempool, taxas e gargalo no contexto da escalabilidade.
  - Transações
  - Mempool, taxas e gargalo

Parte 2
Construir o futuro, atualizando-se.

Capítulo 3 – BGV - Bitcoin à Grande Vitesse

- Bitcoin Cash - o Hard Fork
- SegWit - Segregated Witness
  - Problema da maleabilidade
  - Assinatura
- Lightning Network
  - Lightning (Relâmpago)
  - Contextualização
  - Invoice - Fatura
- Ligações entre os nós
  - Onion Routing
  - Source Routing (Cálculo da Rota)
- Taproot - Atualização e evolução
  - Sistema de Votação
  - Aprovação do Taproot
  - Taproot - O que muda
    - Assinaturas Schnorr
    - Linearidade como vantagem
    - MultiSig com Assinaturas Schnorr
    - Fungibilidade
    - Redução do peso de memória
    - Smarts contracts - Lightning Network e DeFi

Nota Final

Síntese

Sugestão: Assume esta secção como uma síntese do livro e não como parte integrante do mesmo.

Satoshi Nakamoto, o criador do Bitcoin, disse, um dia, que explicar ou descrever esta temática para o público geral era complexo, pois não havia, nem há nada com o que relacionar.

É verdade. A prova está no facto desta primeira secção ter sido a última a ser escrita. Após a leitura prévia à publicação, verificou-se a necessidade de escrever um resumo ainda mais simplificado de todo o conteúdo. A especificidade do assunto, a complexidade dos termos técnicos e a dificuldade em tornar o conteúdo ainda mais percetível, ao longo de cada capítulo, levaram a que adotasse esta estratégia.

Nestes parágrafos tento, com uma linguagem básica e dando exemplos do quotidiano, explicar o assunto descrito nas páginas seguintes. Esta abordagem inicial, mais descomplicada, permitirá uma melhor compreensão dos conteúdos abordados.

Satoshi Nakamoto é o criador do protocolo Bitcoin. Não se sabe quem é. É anónimo, contudo o seu legado é enorme e sem precedentes na história da economia moderna. Foi homenageado em Budapeste, em Setembro de 2021.

Ao criar um sistema de pagamento sem a necessidade de uma ou mais entidades, para além do utilizador que paga, do utilizador que recebe e do utilizador que valida a transação, revolucionou por completo o sistema financeiro. Bancos ou instituições como Visa, Mastercard, Paypal etc., deixam de ser necessários. No fundo, o protocolo Bitcoin é uma versão digital dos pagamentos em numerário (A paga diretamente a B), mas sem a entidade emissora/reguladora de moeda (Banco Central Europeu, Reserva Federal Americana, Banco do Japão, etc.). Neste sistema, tudo ocorre entre utilizadores da rede – quem paga, quem recebe e quem valida as transações (os mineradores).

A ideia disruptiva resultou de vários fatores, nomeadamente: perda na confiança do sistema financeiro, perda de confiança nas políticas governamentais de sustentabilidade económica, perda de confiança nas entidades emissoras de moeda e a contínua inflação e desvalorização do dinheiro ao longo dos anos.

Antes de 1971, os governos não imprimiam moeda sem existir uma proteção de um ativo finito e imune à desvalorização. O ouro era esse ativo, o padrão. Uma economia global tornava complexa a manutenção de reservas de ouro, em vários países. Optou-se, em 1944, pelo padrão dólar-ouro. Os Estados Unidos da América guardavam o ouro (a II Guerra Mundial não destruiu o seu território) e imprimiam dólares em função das reservas de ouro físico, existentes nos seus cofres. Por sua vez, os outros países emitiam as moedas nacionais consoante as suas reservas em Dólares. Isto terminou em 1971, passando a emitir-se dinheiro com base na confiança da economia de cada país.

Se há uma impressão sem limite, há desvalorização. A areia é mais barata que o ouro.

Anos mais tarde, em 2008, surgiu uma crise económica, em parte, também, resultante da perda de confiança nas entidades financeiras.

Em 2009, surge o protocolo Bitcoin, baseado na matemática e criptografia, num ativo com número finito de unidades e na descentralização da confiança. Um mecanismo de validação das transações (Algoritmo de Consenso) garante segurança e impede que as moedas criadas sejam duplamente gastas.

Servindo-se da capacidade da internet e associando conceitos e mecanismos de criptografia (Função Hash), Satoshi criou uma versão digital do dinheiro, com base numa tecnologia já existente, mas nunca antes utilizada – blockchain. Esta é a maravilha do protocolo Bitcoin – sistema financeiro descentralizado, virtualmente, impossível de alterar ou modificar.

A moeda não é impressa, mas sim, minerada. A sua mineração implica utilizar equipamentos informáticos dispendiosos, que garantam um processamento computacional, suficientemente grande para conseguir minerar Bitcoins.

Trata-se de um processo competitivo entre os mineradores. A recompensa, pela resolução de problemas matemáticos de elevada complexidade, é o crédito em Bitcoins. Depois de minerados, entram em circulação para compra e/ou utilização, ou seja, minerar e adquirir são as formas de se obter Bitcoins.

Por estar limitada a 21 milhões de moedas e a recompensa pela mineração ser reduzida ao longo do tempo (conceito de Halving), a tendência será valorizar e não desvalorizar. O protocolo Bitcoin é deflacionário e não inflacionário.

Ao aumentar o seu preço, como mostra a história, é cada vez mais caro comprar um Bitcoin (BTC), contudo, a sua fração Satoshi (SATS), ainda é acessível. Digamos que, será como comprar na frutaria 10 gomos de laranja, em vez de uma laranja. Chegará o tempo em que o nosso raciocínio será em SATS e não BTC. Tornar-se-á mais prático.

Numa perspetiva futura, acredito na convivência diária com o Bitcoin. Este fará parte do nosso quotidiano como faz a internet, o telemóvel ou a energia elétrica. Porém, ainda terá de superar a fase da negação, passar a fase de aceitação e chegar à fase de adoção, o que está muito próximo, a meu ver. Quando isso acontecer, passaremos a utilizar SATS como moeda de circulação, em alternativa à utilização de EUR ou USD.

A aquisição e convivência com Bitcoins é simples e fácil. Excluo nesta explicação a mineração.

As empresas especializadas - Exchanges - permitem adquiri-los, comprando com moeda nacional (EUR, USD, GBP) ou trocando por outras criptomoedas. Depois de obtidos, guardam-se numa carteira digital, um software que permite armazenar e transacionar Bitcoins. Com esta carteira, estamos ligados à blockchain (rede) onde circula o Bitcoin.

Quando escrevo um texto no Word, utilizo o software de processamento de texto. Esse documento pode ser enviado por e-mail, utilizando a internet, para alguém que o irá ler, abrindo-o num processador de texto. Simplifiquemos.

O Phill quer pagar à Ann um café em Bitcoins. Temos um emissor (Phill), uma recetor (Ann) e uma mensagem (pagamento em Bitcoins). Convertamos este exemplo no anterior. O Phill (emissor) quer enviar à Ann (recetor) um documento em formato DOC do Word (mensagem).

O Phill, para enviar Bitcoins, precisa de os deter na sua carteira digital, tal como necessita de ter um processador de texto e um documento DOC do Word. A Ann para receber os Bitcoins utiliza uma carteira digital, tal como usa o processador de texto para abrir o documento DOC do Word.

O Phill envia os Bitcoins, através da rede Blockchain, utilizando a internet, tal como envia o documento DOC do Word pelo sistema de e-mail (“rede”), utilizando a internet. Contudo, caso o Phil se engane no endereço de Ann, esta não recebe e o ficheiro é enviado para outra pessoa.

O processador de texto, sendo software, atualiza-se e sofre modificações, que implementam melhorias no seu funcionamento, garantindo a necessária adaptação à realidade, ao longo do tempo. O Word de 1998 não é igual ao Word de 2021.

O protocolo Bitcoin, sendo também software, é, constantemente, atualizado, permitindo uma melhor adaptação à nova realidade vivida em cada momento temporal. Porém, há uma grande diferença, todas essas atualizações, apenas, são implementadas, caso sejam aprovadas com grande consenso da comunidade de validadores.

Uma atualização do Word poderá ser útil na realidade Europeia, mas não na Asiática, contudo, como não há decisão partilhada e descentralizada, a nova versão é disponibilizada sem consenso dos utilizadores.

No caso do protocolo Bitcoin isso não ocorre. Nada é implementado sem que haja um consenso, quase unânime. O Bitcoin adapta-se, atualiza-se e ultrapassa dificuldades, barreiras e problemas, que possam surgir com a evolução do Mundo. Um conceito disruptivo que não cabe, não se encaixa, nem é possível existir no processo de funcionamento da moeda fiduciária.

SegWit e Taproot são os exemplos mais visíveis da adaptação e atualização do protocolo Bitcoin à realidade vivida, em cada momento da sua história.

O protocolo Bitcoin baseia-se na segurança e descentralização, em detrimento da escalabilidade (Trilema das Blockchains). O Bitcoin, em si e na sua origem, não é funcional em transações instantâneas e de valores baixos, como o pagamento de um café ou de um jornal. Porém, ao atualizar-se permitiu o desenvolvimento e utilização de outras aplicações, como, por exemplo, a Lightning Network.

Apesar de não ser escalável de origem, atualiza-se permitindo a adoção de mecanismos/aplicações, que lhe confiram essa característica e o tornem um protocolo com escalabilidade suficiente para a fácil utilização, em transações rápidas e de valores reduzidos.

Satoshi criou algo tão importante e maravilhoso, que, depois de compreendido, tem um valor incomensurável. É impossível não ficar apaixonado por este novo conceito de sistema financeiro. Entidades, empresas e países (El Salvador) começam a compreender as comprovadas capacidades deste protocolo. Lentamente, a sua adoção dá os primeiros passos.

O conteúdo, aqui sintetizado, será um pouco mais aprofundado ao longo do livro. Posso incorrer em repetições propositadas. No final, espero ter conseguido contrariar Satoshi Nakamoto, quando diz que é difícil explicar esta tecnologia ao público, em geral.

Não é fácil expor e apresentar, de uma forma simplificada, conceitos e noções técnicas de criptografia, mecanismos de consenso ou transações via blockchain... Mesmo assim, fiz o exercício de tornar o livro acessível na linguagem e fluído no discurso. A probabilidade de ser, totalmente, compreendido, só daqui a alguns anos, é grande, mas isso não me impediu de te abrir a porta e mostrar o caminho.

Se a tua resposta for SIM, à última frase deste livro, então a minha missão de divulgar, informar e ensinar foi concluída com sucesso. Mas, se porventura, a tua resposta for NÃO, então sugiro uma nova leitura, mas acompanhada de pesquisa para uma melhor compreensão dos conceitos, aqui descritos.

"Escrever uma descrição disto para o público, em geral, é muito difícil.
Não há com o que relacionar."

Satoshi Nakamoto

Parte 1
CONTEXTUALIZAÇÃO

Nota Introdutória

O desafio é grande, mas vou tentar…

Esta obra pretende ir além de um documento de pesquisa e partilha de informação. É uma apresentação simples, concisa e de fácil compreensão daquilo que eu, como pessoa, acredito que será o futuro dos sistemas de pagamento a nível Mundial.

Todo o conteúdo é baseado em pesquisas de fontes disponíveis na internet e livros que li, analisei e estudei. Em momento algum pretendo incentivar ao investimento ou aconselhar a aquisição de qualquer tipo de ativos digitais, nomeadamente: tokens ou criptomoedas (conceitos diferentes - criptomoedas circulam numa blockchain própria e da qual são nativos; tokens circulam numa blockchain, da qual não são nativos, apenas utilizam a rede para circulação).

Reconhecendo e sabendo que uma transmutação está a caminho e que mudará, para sempre, o mundo em que vivemos, tanto do ponto de vista financeiro, económico e social, como do ponto de vista político e de decisões governamentais, decidi, através deste meio, dar a conhecer, de forma muito superficial, o que é a tecnologia Blockchain, o que é o Bitcoin e a Lightning Network. Estas são ferramentas, que estão a alicerçar as bases do novo sistema financeiro Mundial. Não foi por acaso que tudo começou no final de 2008 e início de 2009 – lembras-te da crise do subprime que afetou os mercados Mundiais e, decorrentemente, originou toda a conjuntura económica desfavorável desse período.

O livro foi intitulado de "Um café com o protocolo Bitcoin" (daí, ao longo do texto ser utilizado o masculino, na referência ao Bitcoin), pelo facto de estar escrito com um discurso semelhante a uma conversa de café.

Imagina que ao leres, estás comigo a falar sobre o protocolo Bitcoin, no café, na praia, no comboio, no autocarro...

Foi dividido em duas partes, subdivididas em 3 capítulos: no primeiro faço uma pequena apresentação da tecnologia da Blockchain e do Bitcoin; no segundo explico como é possível conviver com o Bitcoin e no terceiro escrevo, de forma simplista e com linguagem compreensível, o sistema Lightning Network e a próxima atualização do Protocolo – o Taproot.

Existem três livros, os quais aconselho a sua leitura para que todos os conceitos aqui partilhados fiquem muito melhor compreendidos e assimilados. São eles:

"O padrão Bitcoin" de Saifedean Ammous,

"Bitcoin" de António Vilaça Pacheco e

"Bitcoin e Blockchain" de Paulo Alcarva.

O white paper, escrito por Satoshi Nakamoto é, igualmente, leitura recomendada, e está disponível na internet, em versão Portuguesa. Foi este o documento que apresentou ao Mundo o Bitcoin.

Sou médico dentista de profissão, contudo, sempre tive um gosto e aptidão para a área da informática. Como tal, concluí, em 2011, o Mestrado em Informática Médica, na Universidade do Porto e, em 2018, ingressei no Mestrado de Segurança Informática, na Universidade de Coimbra. Admito que seria muito complexo terminá-lo em tempo útil, com os conhecimentos que possuo na área e, sobretudo, a reduzida disponibilidade de tempo possível para esse projeto. No entanto, alcancei algo muito valioso dessa experiência - as aulas de Criptografia, do Professor Fernando Boavida, tendo concluído a disciplina com 15 valores, na época normal, apesar de ser trabalhador estudante deslocado. Foi uma alegria imensa, colocada ao nível da conclusão do Mestrado.

A disciplina de Direito e Segurança Informática foi, igualmente, concluída na época normal, tendo ampliado e sistematizado, ainda mais, os meus conhecimentos.

As noções adquiridas de criptografia permitiram-me compreender, muito melhor, a tecnologia Blockchain e todo o mecanismo de funcionamento do protocolo Bitcoin. Acredito que este é uma referência no mundo das criptomoedas e que facultará a todos, sem exceção, o acesso a um sistema financeiro sem fronteiras ou limitações e, eventualmente, vir a tornar-se a moeda de reserva mundial.

Foi em 2010 / 2011, na fase embrionária deste sistema, que tive o meu primeiro contacto, aquando de uma pesquisa, na internet.

Sustentada numa ideia ténue, recordo ser uma noite chuvosa quando li algo que dizia (ideia principal, não palavras reais): o PC deverá estar ligado 24h por dia, para dar suporte à rede e ter capacidade de validação, o que permitirá receber as recompensas. Como não conhecia nem compreendia o seu potencial, pensei, no imediato, que os custos de energia não justificariam o risco. Pouco tempo depois (2012 / 2013), na Praça da República, em Coimbra, após um jantar de antigos colegas de Faculdade e grandes amigos (António, José e Luís), cito as palavras do José – "o futuro é blockchain, é o que está a dar". Nenhum de nós, nem mesmo ele, tínhamos noção da certeza, força e inevitabilidade das suas palavras.

Não tive a oportunidade de conhecer o Bitcoin Faucet, mas, também, ninguém imaginava o fruto, que daí adviria, isto porque, nos primeiros anos do Bitcoin (2008 a 2012), a informação era reduzida e os meios para obter fontes fidedignas muito limitados.

Estes últimos parágrafos têm o propósito de contextualizar-te, esclarecer-te e responder-te à questão, que, possivelmente, estarás a fazer a ti mesmo: - Como é que o Jorge, sendo médico dentista, escreve este livro e fala de Blockchain, Bitcoin, computação etc..

Lembro que toda a informação, aqui partilhada, é superficial e este conteúdo pouco aprofundado. Ao leres este livro, ajudo-te a abrir a porta e a indicar o caminho. Percorre-lo já será uma decisão e uma opção da tua pessoa. Contudo, como ninguém começa uma viagem sem preparação e, também, ninguém começa uma caminhada sem o primeiro passo, vê este conjunto de páginas como isso mesmo, um "guia turístico".

O livro é gratuito e passível de ser partilhado, fotocopiado e distribuído. A informação nele contida está disponível na internet, apenas, transmitida de forma mais compacta e compreensível. Partilhar conhecimento sobre um assunto tão importante e disruptivo, como o Bitcoin não poderia, de modo algum, ser remunerado. Porém, se achares que deves contribuir com algo, sugiro que dês um donativo a uma Instituição de Solidariedade Social, à tua escolha.

Desfruta da leitura e boa viagem ao mundo do Bitcoin.

"O Bitcoin está para o sistema financeiro como a Internet está para o sistema de comunicação."

"O Bitcoin não é de ninguém, mas será utilizado em todos os países, logo, nunca será moeda estrangeira."

"É uma base de dados distribuída globalmente,
com acréscimos à base de dados por consentimento da maioria."

Satoshi Nakamoto

Capítulo 1. **Blockchain e Bitcoin**
Enquadramento Tecnológico e Económico

Blockchain a Cadeia de Blocos

A tecnologia de Blockchain surgiu em 1991, quando Stuart Haber e Scott Stornetta, pertencentes à Xerox, idealizaram um sistema de armazenamento de dados e informação com robustez suficiente para se tornar imutável e inviolável, tendo por base as propriedades matemáticas da criptografia.

É uma tecnologia, que permite o registo de novas informações numa base de dados, sendo do tipo append-only, dado que, apenas, permite a adição; edição ou remoção são, virtualmente, impossíveis.

Chama-se blockchain, pois junta as duas palavras block e chain (cadeia de blocos), visto ser uma base de dados, que funciona com blocos encadeados, numa estrutura em que o bloco seguinte terá, no seu conteúdo, juntamente com as suas informações, uma "impressão digital do bloco anterior", que, por sua vez, terá um novo bloco ligado a este, e assim sucessivamente.

A título de exemplo, a blockchain é semelhante a um "tecido digital", no qual uma pequena alteração numa "costura", irá comprometer todo o encadeamento seguinte.

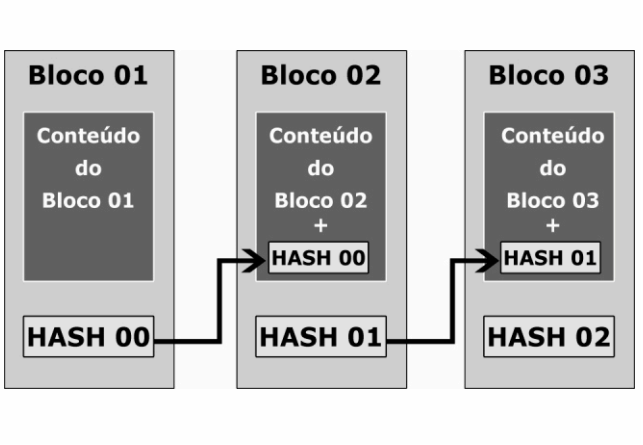

Imagem 1 - Blockchain

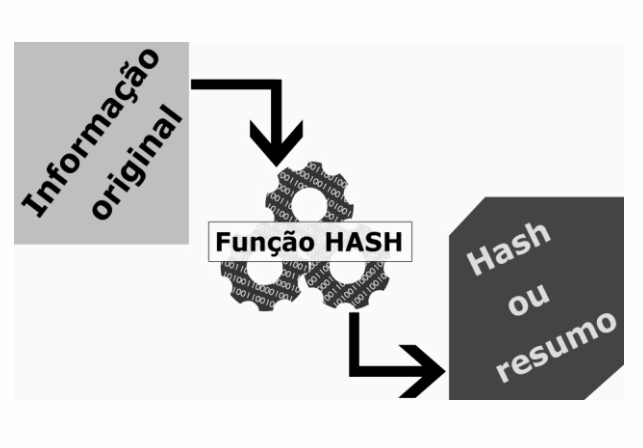

Imagem 2 - Função Hash

A Função Hash ou Impressão digital do Bloco

Para uma melhor compreensão da construção da cadeia de blocos, característica da Blockchain, é fundamental perceber o que é a função hash (resumo). Por diante não será utilizado termo resumo, mas o estrangeirismo hash.

O algoritmo matemático da função hash deve utilizar os dados de entrada (mensagem) e transformá-los de maneira a que os dados de saída hash (resumo) sejam padronizados no seu tamanho de memória e no número de caracteres alfanuméricos.

Na criptografia moderna, estas funções hash unidirecionais são considerados os operários, dada a importante utilidade, que possuem pelo facto de serem, praticamente, impossíveis de reverter.

Devem possuir quatro propriedades principais: ser fácil de computar o hash para qualquer mensagem; gerar a mensagem, a partir

do hash, deve ser difícil; a modificação da mensagem sem alterar o hash deve ser difícil e deve, igualmente, ser difícil encontrar duas mensagens diferentes com o mesmo hash.

Esta função hash fará com que todos os blocos de informação, numa blockchain, estejam de tal maneira unidos que a sua alteração é, praticamente, impossível.

O hash é a impressão digital de cada bloco, a qual será incluída no bloco seguinte, criando, deste modo, a cadeia de blocos – blockchain.

O Padrão Ouro, Bretton Woods e Bitcoin

Todos nos recordamos da crise Mundial de 2008 – subprime, o que implicou em algumas economias mais fragilizadas, o resultado nas instituições bancárias e nas poupanças dos seus clientes.

No entanto, há uma conjuntura económica e política anterior, que é importante mencionar e salientar.

Durante vários anos, o mundo viveu no sistema monetário conhecido por padrão-ouro. Este metal precioso era tido como referência, a nível mundial, na regulação da emissão de moeda. Na prática, a impressão de dinheiro estaria dependente das reservas de ouro detidas pelo país emissor de moeda.

No ano de 1944 foi assinado o Acordo de Bretton Woods, no qual o Dólar Americano passou a estar sustentado pelas reservas de ouro americanas. Decorrentemente, todas as outras moedas nacionais ficaram ligadas ao dólar, passando-se para o sistema dólar-ouro. O dólar tornou-se a Moeda de Reserva Mundial. O Florim Fiorentino ou o Ducato Veneziano foram, igualmente, moedas de reserva Mundial, tal como aconteceu com o Real Português entre, aproximadamente, 1480 e 1550.

Contudo, em 1971, o presidente americano Nixon decidiu cancelar os acordos de Bretton Woods.

Em resultado da guerra do Vietname, a impressão de dólares deixou de respeitar a quantidade de ouro em reserva. A 15 de Agosto, após o célebre discurso de Richard Nixon, foi criado o conceito de moeda fiduciária, do latim fidúcia (confiança), na palavra do governo. Nesse momento, todas as moedas nacionais passaram a não estar ligadas ao ouro, pois o seu elo de ligação (indireto), o dólar americano, rompeu esse vínculo.

Uma moeda deve respeitar 3 funções: instrumento de troca, unidade de conta e reserva de valor.

Desde 1971, o dólar americano perdeu 80% do seu poder de compra.

Acredita-se que o Euro perdeu um terço da sua capacidade de compra, desde a sua introdução na economia e há quem defenda que o fim do padrão-ouro conduziu a todos os problemas financeiros e económicos atuais – crises e questões relacionadas com as dívidas soberanas.

A reserva de valor é tida como uma proteção contra as inconstâncias do mercado, isto é, a manutenção do poder de compra com o decorrer do tempo. Esta função da moeda dá, à pessoa, a possibilidade de proteger o seu património contra a volatilidade económica.

O ouro é, pela narrativa da humanidade, escasso e foi, sempre, reconhecido como reserva de valor.

Ao romper a ligação com o ouro, nos anos 70, presume-se que o respeito pela função de reserva de valor, atribuída à moeda, foi perdida. A emissão de moeda, equilibrada por algo com quantidade limitada, como o ouro, deixou de ser obrigatória.

É neste contexto económico, criptográfico e tecnológico, que surge em 2008, pela primeira vez, uma aplicação efetiva da utilidade

da tecnologia de blockchain – num sistema financeiro e de pagamento.

A 18 de agosto de 2008, é registado o domínio bitcoin.org e em 31 de Outubro, de 2008, é publicado o white paper, que apresenta, oficialmente, o Bitcoin, cujo identificador internacional é BTC. Nesse documento, nas primeiras frases é efetivada uma crítica subliminar à confiança no sistema financeiro. O mesmo artigo científico define o limite máximo de fornecimento de 21 milhões de Bitcoins. O Bitcoin, tendo uma quantidade máxima de unidades, é um ativo escasso.

No dia 3 de janeiro de 2009 é minerado, por Satoshi Nakamoto, o bloco 0 ou Genesis da blockchain.

O Bitcoin foi, oficialmente, aceite por El Salvador, como moeda de circulação, a 7 de Setembro, de 2021, uma data marcante na vida desta criptomoeda.

Bitcoin e Satoshi Nakamoto

Escolheu-se o sistema económico por exigir muita confiança e onde a tecnologia fosse utilizada para melhorar algo, que vinha sendo perdido, a confiança nas instituições financeiras. Surgiu então o primeiro dinheiro em formato digital descentralizado.

Satoshi Nakamoto, criador do Bitcoin, é alguém, totalmente, desconhecido. Não se sabe se é uma pessoa, se é um grupo de pessoas ou um consórcio empresarial. Sabe-se, apenas, que foi quem assinou o primeiro white paper, onde descreve um sistema de pagamentos, ponto-a-ponto (peer-to-peer), totalmente descentralizado e livre, independente de governos ou entidades e com capacidade de ser o futuro dinheiro digital universal, impossibilitando a dupla utilização de fundos.

Esse documento é, na minha perspetiva, um dos maiores marcos da história da Humanidade. Coloco a criação e o desenvolvimento do sistema de pagamento Bitcoin ao nível da invenção da roda e da descoberta do Caminho Marítimo para Índia. Quando estudares e aprofundares os teus conhecimentos neste sistema, entenderás as minhas comparações.

Satoshi deu-nos, através da sua criação, algo capaz de mudar para sempre a história da humanidade, à semelhança da roda e do Caminho Marítimo para a Índia.

Satoshi é o exemplo de alguém, cuja criação foi de valor incalculável, capaz de mudar a vida de milhões de pessoas, sem ter uma empresa, escritórios físicos e não sendo CEO. Continua anónimo, fora dos palcos da fama e longe dos holofotes, ainda que possuindo uma riqueza intocável, até hoje, de milhões de Bitcoins, nas suas carteiras.

Por essa razão, vemos, muitas vezes, a frase "We are all Satoshi" (somos todos Satoshi), não é por acaso.

A primeira homenagem oficial a Satoshi Nakamoto encontra-se na cidade de Budapeste, na Hungria. A estátua, na qual o espelho reflete a imagem de quem a vê, numa alusão à ideia "somos todos Satoshi", foi apresentada ao público a 16 de Setembro de 2021.

"É uma base de dados distribuída globalmente,
com acréscimos à base de dados por consentimento da maioria."

Satoshi Nakamoto

Trilema das Blockchains

O Bitcoin não foi, efetivamente, o primeiro dinheiro digital. B-Money, HashCash ou Bit Gold surgiram nos anos 90. Contudo, o Bitcoin é a primeira criptomoeda descentralizada, que utiliza a tecnologia blockchain, pilar de criação de confiança no sistema, impedindo o "gasto duplo" (utilização simultânea das mesmas unidades, em transações diferentes).

A blockchain, onde circula o Bitcoin, desenvolvida por Satoshi Nakamoto, é descentralizada e segura, mas não tem escalabilidade suficiente, isto é, não tem capacidade de processamento de um grande número de transações por segundo (TPS). É composta por uma rede de computadores, que validam e confirmam as transações num livro de razão (base de dados), público e distribuído por todos os nodes (mineradores), onde estão registadas todas as transações realizadas dentro da rede. Percebe-se que existe muita transparência.

O registo nesse livro de razão implica o respeito pela verdade do Algoritmo de Consenso, ou seja, o mecanismo capaz de garantir que todos os membros (máquinas) da rede concordam com uma única fonte de verdade.

No entanto, esta tecnologia, apesar de disruptiva e das vantagens que apresenta, envolve algumas limitações.

Segundo Vitalik Buterin (criador de outra blockchain, a rede Ethereum), os códigos de programação, desenvolvidos até hoje, não permitem que as blockchains possuam três propriedades em simultâneo, nomeadamente: segurança, descentralização e escalabilidade.

Uma blockchain descentralizada e com escalabilidade suficiente para processar milhões de transações por segundo (TPS) irá comprometer a sua segurança. Para ser segura e ter escalabilidade suficiente terá de ser centralizada. A rede VISA é um exemplo de uma rede capaz de processar milhares de transações por segundo, com segurança, mas não é descentralizada. Uma rede descentralizada e segura não poderá apresentar uma escalabilidade suficiente para a sua utilização em larga escala.

As caraterísticas de segurança e descentralização da rede Blockchain, onde circula o Bitcoin, dão-lhe o estatuto de quase inviolável e a mais segura, até hoje criada, porém, a sua escalabilidade é limitada.

Imagem 3 - Trilema das Blockchains

Prova de trabalho. O mining ou mineração de Bitcoins.

O mecanismo ou algoritmo de consenso é o método, através do qual os membros de uma rede blockchain chegam a um acordo sobre a verdade única. Este estabelece a confiabilidade na rede e a confiança entre os nós, ainda que sejam desconhecidos. O procedimento garante que cada novo bloco, adicionado à blockchain, é a única versão da verdade acordada entre os participantes no processo de validação.

Existem vários algoritmos de consenso, nomeadamente: Proof-of-work (Prova de Trabalho); Proof-of-Stake (Prova de Participação); Delegated Proof-of-Stake (Prova de Participação Delegada); Practical Byzantine Fault Tolerance (Tolerância a Falha Bizantina), delegada ou simples; Federated Byzantine Agreement (Consenso Federado Bizantino), entre outros.

Uma transação de Bitcoin, para ser dada como confirmada, necessita de ser verificada, registada no livro razão e distribuída por todos os nodes (nós) da rede. Este processo implica um poder de cálculo computacional muito grande. Para custear o investimento nos processadores, na energia e o apoio no funcionamento da rede, os proprietários desses equipamentos são recompensados, ganhando Bitcoins ao desempenhar essas funções. Este é o chamado mining ou mineração.

No protocolo Bitcoin, o processo de validação e confirmação das transações – mecanismo de consenso - é do tipo proof-of-work (prova de trabalho). Cada node (minerador) vai competir com os outros para encontrar a solução de um problema matemático complexo, por tentativa e erro, a qual permitirá adicionar um novo bloco à blockchain. As transações confirmadas são incluídas nestes blocos.

Este problema matemático é calibrado para que, em média, a criação de um bloco demore 10 minutos. A calibração é feita pelo ajuste de dificuldade do problema matemático a resolver. Existindo muitos mineradores, a dificuldade aumenta, diminuindo a probabilidade de criar o bloco, um ajuste, que ocorre a cada 2016 blocos criados (sensivelmente 2 semanas).

O primeiro node a encontrar a solução e anexar o bloco recebe Bitcoins como recompensa. Atualmente, o valor pago por cada bloco adicionado é de 6,25 Bitcoin.

No entanto, estas recompensas já foram superiores e com o decorrer dos anos será mais difícil obter novos Bitcoins.

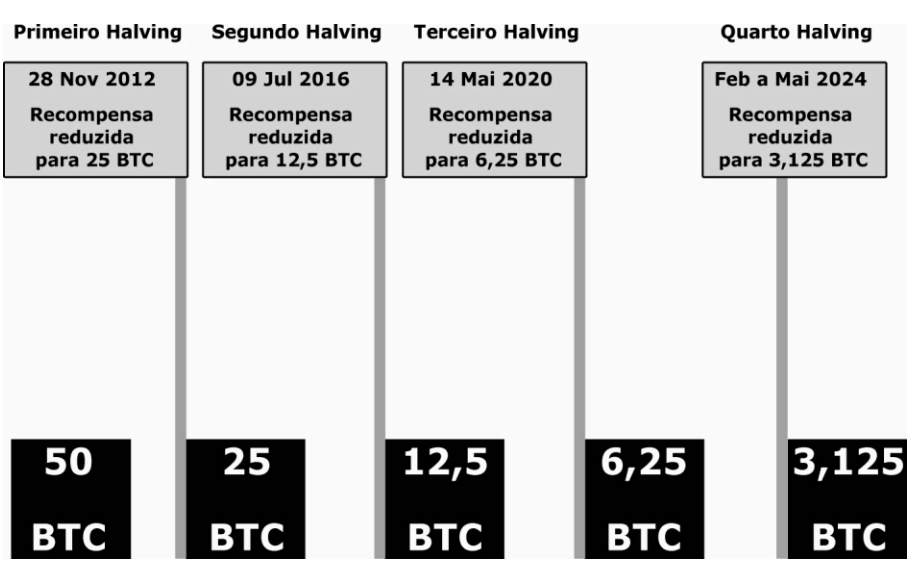

Imagem 4 - Halvings Bitcoin

Halvings e o modelo deflacionário

Existem momentos em que o valor da recompensa é reduzido para metade – os halvings.

A cada 210.000 blocos adicionados à blockchain ocorre uma redução, no valor da recompensa de bitcoins, paga aos mineradores. No início, cada bloco adicionado dava direito a 50 Bitcoins. Entretanto, esse valor tem vindo a ser diminuído e, em 11 de Maio, de 2020, ocorreu o último halving, o qual cortou para 6,25 Bitcoins o valor da recompensa, por bloco adicionado. Prevê-se um novo halving na primavera de 2024. Nesse momento, o valor da recompensa será de 3,125 Bitcoins.

Economia do Bitcoin

Os Bitcoins criados e distribuídos pelos mineradores são a fonte de moedas, que alimenta a economia do Bitcoin.

O modelo económico, criado por Satoshi Nakamoto, determina um limite máximo de 21 milhões de Bitcoins a serem minerados, ou seja, o fornecimento máximo de moeda é esse, não sendo possível minerar mais, contudo prevê-se que o último Bitcoin seja minerado em 2140.

Verifica-se, assim, que é uma moeda escassa. Sabendo que a cada 210.000 blocos a criação de Bitcoins é reduzida para metade, percebe-se que, pela lei da oferta e da procura, e pelo facto do modelo financeiro desta criptomoeda ser deflacionário, o preço do Bitcoin tenderá a subir ao longo do tempo. Mais procura, mais dificuldade em obter, menos disponibilidade, subida do preço até se atingir uma volatilidade, virtualmente, inexistente.

Esta é a razão, pela qual, muitas vezes, é apelidado de Ouro Digital ou Ouro 2.0, por ser difícil de obter, ter uma quantidade finita e ser tido como reserva de valor. Pessoalmente discordo, pois, a meu ver, o ouro pode ser reserva de valor, mas sendo o seu transporte e armazenamento complexo, do ponto de vista de segurança e logística e apresentar uma aplicabilidade reduzida no nosso quotidiano (joalharia e uma ou outra aplicação como metal condutor inoxidável), está muito longe daquilo que o Bitcoin pode fazer pelas nossas vidas.

Experimenta pagar um café com ouro ou levar as tuas poupanças, convertidas em barras de ouro, de um país para o outro… Um simples QR-Code com um endereço de Bictoins é capaz de armazenar milhões de Euros em Bitcoins. Pensa nisto!

A mineração cria mais Bitcoins. Os mineradores vendem-nos às empresas de troca de criptomoedas – os Exchanges. Estas, por sua vez, vão disponibilizá-los para que os seus clientes os possam adquirir, através da compra com cartão de crédito, troca por moedas fiduciárias (EUR, USD, GBP) ou troca por outras criptomoedas.

Neste contexto, se a procura aumenta e a disponibilidade é menor, o preço sobe. Se a obtenção de Bitcoins, por recompensa, é reduzida a cada 210.000 blocos, o fornecimento é cortado ao longo do tempo. Pela história, cada vez são mais pessoas, empresas e entidades a adquirir, utilizar e adotar esta moeda, logo a procura aumentará.

Não se sabe até onde poderá chegar o preço de um Bitcoin, mas percebe-se que irá subir, ao longo do tempo, independentemente, da volatilidade do preço ao longo da sua história.

Acredito que poderá ultrapassar a capitalização de mercado do Ouro, maior do mercado financeiro, $11T USD = 9.784.452.938.600,00 Euros (mais de 9 biliões de Euros à data de 4 de Setembro de 2021). Uma nota: a Apple (AAPL) é o segundo ativo em capitalização de mercado com $2,5T USD.

1 BTC	=	**100.000.000 Satoshis**
0,1 BTC	=	**10.000.000 Satoshis**
0,01 BTC	=	**1.000.000 Satoshis**
0,001 BTC	=	**100.000 Satoshis**
0,0001 BTC	=	**10.000 Satoshis**
0,00001 BTC	=	**1.000 Satoshis**
0,000001 BTC	=	**100 Satoshis**
0,0000001 BTC	=	**10 Satoshis**
0,00000001 BTC	=	**1 Satoshis**

Imagem 5 - Bitcoin a unidade. Satoshi a fração.

Bitcoin a unidade. Satoshi a fração

Em 2009 possuir um Bitcoin era como ter cêntimos. Com a valorização desta moeda, começou a tornar-se muito caro obter uma unidade. Então, sabendo que o Bitcoin é fracionado em 100 milhões de sub-unidades, determinou-se que a fração mais pequena do Bitcoin é o Satoshi (SATS), em homenagem ao seu criador.

Com esta identidade monetária, passou a optar-se por falar em Satoshis ou SATS, em vez de Bitcoins, quando os valores em questão não ultrapassam uma unidade. Por exemplo, uma compra de 1Eur daria 0,000024 BTC (à data da escrita deste parágrafo), é mais prático dizer que a compra de 1 Euro são 2400 SATS.

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Criptografia e Carteiras de Criptomoedas

Uma carteira digital é uma das ferramentas essenciais para o acesso ao mundo das criptomoedas. Estas são, igualmente, fundamentais para o seu armazenamento e interação com diferentes blockchains.

Estes instrumentos informáticos utilizam um tipo de criptografia denominada de criptografia assimétrica, a qual, resumidamente, é um sistema criptográfico composto por chaves públicas, que, tal como o nome indica, podem ser distribuídas e chaves privadas, as quais, por sua vez, permitem reverter a encriptação da mensagem e, como é evidente, nunca devem ser partilhadas ou cedidas. Esta técnica, ao utilizar, duas chaves diferentes para realizar funções opostas (pública vai encriptar e privada reverter) assume o nome de criptografia assimétrica.

Nas carteiras de criptomoedas, com este mecanismo de encriptação, a chave pública é utilizada para gerar endereços públicos, a fim de serem distribuídos e partilhados. Com estes é possível receber, nessas carteiras, ativos digitais. A chave privada é aquela que permite assinar as transações (envio de valor) e aceder aos fundos da carteira, razão, pela qual, deve ser guardada com a maior segurança possível.

Estas chaves podem ser armazenadas em hardware, podem ser utilizadas por software ou, em alternativa, impressas em papel ou noutro material como, por exemplo, metal.

Atualmente, para facilitar a memorização das chaves privadas, existe o sistema de seed-phrase (frase semente), que permite a codificação das chaves privadas, através de 12 ou 24 palavras. Não vou explicar o mecanismo criptográfico, subjacente a este sistema, mas aconselho a pesquisa sobre o mesmo. As palavras da seed, inseridas na ordem correta, permitem fazer a recuperação da carteira e dos fundos nela contidos.

Um exemplo: possuo uma carteira com várias criptomoedas, entre as quais, bitcoins, no meu telemóvel. Por um incidente, este fica danificado, irremediavelmente. Adquiro um novo equipamento, instalo a carteira mobile e aplico as palavras da minha seed, pela ordem correta, et voilá, os fundos da carteira são carregados no novo dispositivo. Contudo, se essa seed for obtida por alguém, de um modo malicioso, executa os mesmos passos e, automaticamente, tem acesso aos meus fundos, de forma não autorizada.

Carteiras de Criptomoedas

De acordo com as suas caraterísticas de armazenamento ou "responsabilidade" da custódia das chaves, as carteiras podem ser classificadas da seguinte maneira:

· Manutenção e "responsabilidade" na custódia das chaves

Custodial (com custódia). São os tipos de carteiras, que os Exchanges, empresas de compra e venda de criptomoedas, utilizam e facultam aos seus clientes. A chave privada não está na posse do cliente. Para enviar fundos, quem assina a transação são os sistemas dos Exchanges, responsáveis pelas transações. Dá-se a ordem de transferência, mas a mesma só é executada, após a indicação e validação por parte do sistema.

Non custodial (sem custódia). São os tipos de carteira, onde a responsabilidade é toda da parte do utilizador, o qual tem na sua posse o conjunto de chaves: pública e privada, e é este quem assina as transações.

Num exemplo, comparando a conta bancária e o porta-moedas. A conta bancária é uma carteira Custodial, pois os fundos do cliente estão (pensamos) armazenados no banco. Quando é dada uma ordem de transferência, a mesma só é processada no momento em que o sistema do banco valida essa ordem. Caso se perca o acesso à conta bancária, pode recorrer-se ao Apoio a Cliente, para proteger os fundos e dar novo acesso. No caso do porta-moedas, já é do tipo não-custodial: o proprietário é responsável a 100% pela manutenção dos fundos. Se mantiver no porta-moedas 100Euros, em notas e moedas, e o perder, quem o encontrar, muito provavelmente, não os irá devolver.

Exodus, Trustwallet ou Atomic são exemplos de carteiras non custodial.

· Consoante o método de armazenamento das chaves existem

Carteiras online. Software em versão mobile ou desktop, que permite guardar, receber e enviar criptomoedas, sempre, com a responsabilidade da manutenção das chaves imputada ao proprietário.

Carteiras físicas ou offline. Carteiras que não se encontram, permanentemente, ligadas à internet, daí o termo offline. Existem as Hardwallets, dispositivos de armazenamento físico e as Paper wallets, mais vulgarizadas e, virtualmente, sem custos de aquisição, nas quais as chaves são impressas. Chama-se paper por utilizarem o papel, no entanto, hoje em dia já podem ser impressas noutros materiais, como metal.

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Exchanges, Plataformas de aquisição.

Para perceberes, como atualmente, se tornou fácil adquirir Bitcoins é importante saberes o que se passou no início.

Os primeiros Bitcoins tiveram de ser minerados. A partir daí era praticável a sua comercialização. Contudo, até 2010, só era possível a compra peer-to-peer no fórum Bitcointalk, isto é, um minerador que tivesse, em carteira Bitcoins minerados, fazia uma proposta de venda e quem a aceitasse receberia os Bitcoins, mediante o respetivo pagamento.

Em 2010, Gavin Andersen cria o Bitcoin Faucet, um sítio web, onde, somente, era necessário indicar o endereço Bitcoin recetor e escrever as duas palavras "Captcha", para se obter 5 Bitcoins, gratuitamente.

Este foi, de facto, o primeiro sítio web de distribuição de Bitcoins, o qual desempenhou um papel fundamental na construção da comunidade. Em 2012, encerrou, tendo na sua folha de distribuição um total de 19.700 Bitcoins enviados, gratuitamente.

Mais tarde, foram surgindo outras empresas, umas mais sólidas do que outras, umas mais capazes de lidar com as ameaças de segurança do que outras. Lembro o caso do roubo dos 460 milhões de dólares, do Mt. Gox, posterior liquidação e consequente falência. Hoje em dia existem várias empresas especializadas na compra, venda e trading de criptomoedas, à semelhança das corretoras da bolsa.

Vou enumerar algumas, por ordem alfabética. Reforço a ideia de que jamais estou a aconselhar ou a incentivar à sua escolha. São elas: Binance, Coinbase, Crypto.com, Gemini, Huobi, Kraken, entre outras. Em Portugal, atualmente, a Criptoloja e a Mind the Coin são as empresas, que obtiveram licença de funcionamento.

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Como obter Bitcoins

A mineração e a aquisição são duas opções de obtenção de Bitcoins. Contudo, o método mais fácil e acessível de os obter consiste na sua compra, através de um Exchange (corretora), explicado de seguida.

Os programas de remuneração permitem, igualmente, a obtenção de criptomoedas de forma gratuita. Embora os valores obtidos sendo reduzidos, possibilitam, ainda assim, alguma rentabilidade, quase a custo zero.

Conta no Exchange

O processo é muito simples, fácil e rápido, e o protocolo é semelhante para todos os Exchanges.

O primeiro passo é a escolha da plataforma. Posteriormente, é realizada a inscrição e a abertura de conta com email/username e password e, por fim, é necessária a verificação da identidade do cliente.

Atualmente, os exchanges têm políticas de AML - anti money laundring (anti lavagem de dinheiro), pelo que, é quase obrigatório, em todos eles, passar pelo filtro KYC – Know your customer, processo de validação da identidade, com documento de identificação e um conjunto de selfies, obtidas e analisadas por sistemas de inteligência artificial. O processo é semelhante à abertura de uma conta bancária digital, como Revolut ou N26.

Existem exchanges que não exigem este processo, no entanto, implementam limites de transação, depósito ou levantamento.

Após a conta aberta e a identificação verificada, é possível adquirir Bitcoins ou outras criptomoedas, das duas formas mais usuais, troca ou compra.

- Trocar

  Troca ou trading de Bitcoins por moeda fiduciária (EUR, USD, GBP) ou outras criptomoedas.

  Para se efetuar a troca, é necessário depositar fundos na conta pessoal do exchange, em moeda fiduciária ou criptomoedas, e escolher o par de troca para realizar a operação. Trata-se de um processo semelhante ao FOREX - Foreign Exchange (troca de divisas nacionais).

  Os fundos em moeda fiduciária podem ser enviados, via transferência bancária.

- Compra Online

  A outra possibilidade, facultada em alguns exchanges, é a aquisição via cartão de crédito. Tudo semelhante a uma compra online. No entanto, neste caso, os exchanges cobram taxas altas de utilização do cartão, podendo atingir valores acima dos 9%, em alguns casos.

Após a validação da troca ou compra com cartão de crédito, os Bitcoins são adicionados à carteira da conta do cliente. Uma carteira com custódia, como explicado, anteriormente.

Programas de remuneração

Esta é, indubitavelmente, a opção mais barata, pois permite a obtenção de Bitcoins (neste caso Satoshis) ou outras criptomoedas, sem investimento direto.

Existem programas de fidelidade, nos quais, realizando determinadas tarefas, diariamente, são recebidos ativos digitais, como recompensa.

Noutra vertente, cartões crypto (explicado mais adiante) oferecem reembolsos, em percentagem, das compras realizadas (programas de cashback).

No meu entendimento, o programa mais vantajoso que existe, atualmente, é o do browser BRAVE.

Ao utilizares este browser para navegar na Internet, em detrimento do Chrome, Opera, Firefox ou outro, recebes BATs (Basic Attention Token – ativo digital que circula na rede Ethereum), por cada vez que te é mostrada uma notificação. Esses BATs são enviados para a tua carteira digital e, posteriormente, farás deles o que entenderes. Se, por exemplo, os trocares por BTC, vais receber Bitcoins grátis. O programa está bem concebido e ao dia 8, de cada mês, ser-te-ão creditados os BATs relativos às recompensas do mês anterior.

[na página http://i2eonline.medium.com tem uma publicação que explica, em detalhe, este programa]

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Já tenho Bitcoins e agora?

Após a aquisição dos Bitcoins, ou outras criptomoedas, há várias opções: manter, aplicar, gastar, trocar ou transferir.

Numa breve abordagem, deixo, aqui, uma pequena noção do que pode ser feito com Bitcoins ou outras criptomoedas.

Manter. Adquiri os Bitcoin num Exchange e mantenho-os na carteira da minha conta, como se fosse uma "conta à ordem". Estão livres para aplicar, gastar, trocar ou movimentar.

Aplicar. Em determinados Exchanges é possível aplicar fundos em produtos financeiros, onde, mediante o tempo de bloqueio até à maturidade, são pagas taxas de juro. Atenção: nenhum produto deste tipo tem garantia do capital investido. Neste mundo financeiro, apenas, tens a garantia do teu capital estar investido em ativos voláteis e aplicado em produtos de alto risco.

Gastar. No momento atual, vários Exchanges disponibilizam programas de cartões Visa ou Mastercard Crypto, isto é, cartões de pagamento, de ambas as redes, mas que permitem gastar, em compras, o teu saldo da carteira de criptomoedas. Aqui incluem-se os programas de reembolso, mencionados anteriormente.

Um exemplo: compraste 100 Euros de Bitcoins e obtiveste uma valorização do teu investimento de 8%, ou seja, o teu cartão de pagamento permitir-te-á gastar até 108 Euros. Porém, pode acontecer que esse investimento desvalorize. Imaginemos, 5%, nesse caso o cartão só permitirá gastar até 95 Euros.

Trocar. É o chamado trading. Trocaste Euros por Bitcoins e verificas que, agora, há um par, que te permite rentabilizar, ainda mais, o investimento. Trocas os Bitcoins pela criptomoeda desse par. Recordo, contudo, que neste processo existem as fees (taxas de trading do Exchange) e o trading implica muito estudo e análise técnica. Para ser rentável, terá de ser muito bem definido o momento de entrada e o de saída, a estratégia a aplicar e uma correta utilização da funcionalidade stop-loss. É necessária muita experiência.

Transferir. Transferir Bitcoins implica realizar uma transação de fundos, através da blockchain, como será explicado mais à frente. Deverá ser indicado o endereço de destino, o valor a enviar e, posteriormente, é assinada a transação com a chave privada, no caso de carteiras non-custodial. Quando se trata de transferências, provenientes de carteiras de Exchanges, é fundamental perceber o protocolo de transação externa, definido por cada entidade.

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Problema da escalabilidade

A capacidade de processamento de transações da rede blockchain, onde circula o Bitcoin, é, como já foi referido, limitada, dadas as características técnicas do seu código de programação. Recorde-se que Satoshi Nakamoto limitou o tamanho do bloco, a 1 Megabyte, em 2010.

A resolução de problemas matemáticos complexos, por computadores potentes, permitirá a confirmação das transações. Estas, para serem registadas na blockchain, têm de ser incluídas num bloco, tal como mencionado, anteriormente.

O dilema da escalabilidade do Bitcoin encontra-se aqui.

Com um bloco de tamanho máximo de 1 Megabyte, apenas podem ser registadas 2000 transações, em cada novo bloco. Este é formado a cada 10 minutos. Assim, uma sobrecarga da rede vai implicar que haja uma competição pelo espaço no bloco, para que a confirmação da transação se afigure mais rápida. Taxas de transação mais elevadas garantem prioridade de inclusão no bloco. Houve períodos em que utilizadores esperaram várias semanas pela confirmação das suas transações.

Percebe-se que este funcionamento não é compatível com transações do quotidiano à escala mundial.

Exemplo: o pagamento de um café implicaria um tempo longo de confirmação de transação. Em alternativa, para reduzir esse tempo, o custo da taxa de transação teria de ser maior, eventualmente, custar mais do que o próprio café.

No entanto, sendo uma blockchain descentralizada e segura, neutra e sem fronteiras, aberta e resistente à censura, transparente e de acesso público, e capaz de sobreviver desde que exista, apenas, uma cópia do livro de registos (imagina um cataclismo à escala mundial, desde que um node mantenha a cópia da blockchain ela sobreviverá), não poderia ser escalável a um nível de adoção massiva, por milhões de utilizadores. Encaixa-se, aqui, o Trilema das Blockchains.

Esta conjuntura levou à criação de soluções, que vão permitir ao Bitcoin ser a moeda de utilização universal, em grandes ou pequenos valores de pagamentos.

A Lightning Network é uma dessas soluções, da qual falarei na segunda parte deste livro.

"Tenho a certeza de que dentro de vinte anos ou haverá grande volume de transações ou nenhum volume"

Satoshi Nakamoto

Transações, mempool, taxas e gargalo no contexto da escalabilidade

Como já foi mencionado atrás, as transações na rede Bitcoin têm de ser confirmadas e, para tal, é paga uma taxa de rede, semelhante às taxas cobradas pelos bancos, contudo, há uma diferença, o tempo de chegada dos fundos é mais rápido, em condições normais.

Para se compreender a dinâmica da confirmação das transações, é necessário perceber alguns conceitos, nomeadamente: transação e mempool.

Transações

Uma transação de Bitcoin é constituída por três componentes: entrada, valor e saída.

Quando um utilizador solicita o envio de Bitcoins da sua carteira (software onde os bitcoins são mantidos e guardados, aplicação mobile, desktop ou noutro formato) denomina-se entrada da transação (endereço remetente). O endereço da carteira de destino é a saída da transação e o número de Bitcoins a enviar, o valor da transação. A certificação de que os fundos não são usados, mais do que uma vez, é a confirmação da transação, tarefa que é executada pelo minerador. A transação é, sempre, assinada pelo remetente, a testemunha.

Ao solicitar a transação, o utilizador determina uma taxa de rede, poderá ser zero.

Mediante os valores a pagar, os mineradores determinam quais as transações, que mais lhe interessam, do ponto de vista de recompensa. As mais altas têm, naturalmente, prioridade. No exemplo da taxa proposta de valor zero, provavelmente, nunca ocorrerá a sua confirmação ou até poderá ser confirmada, caso surja um altruísta que a valide.

Harold Thomas Finney, conhecido por Hal Finney, foi a primeira pessoa a receber Bitcoins. A transação efetuou-se a 12 de Janeiro, de 2009. Satoshi Nakamoto enviou 10 BTC para Hal Finney nessa operação.

Anos mais tarde, Laszlo Hanyecz realizou a primeira compra com Bitcoins. A 22 de Maio, de 2010 foram compradas, por este programador, 2 pizas por 10.000BTC. Esse dia é conhecido pelo Pizza Day.

O mesmo Laszlo Hanyecz foi pioneiro nos pagamentos, através da Lightning Network. A 25 de Fevereiro de 2018, ao pagar por 2 pizas o valor de 0.00649 BTC, efetivou o primeiro pagamento através deste sistema.

Confirma-se o modelo deflacionário do Bitcoin. A mesma quantidade do mesmo produto foi adquirida, em 2010, com o valor situado na ordem das dezenas de milhar e em 2018, na ordem das centésimas milésimas.

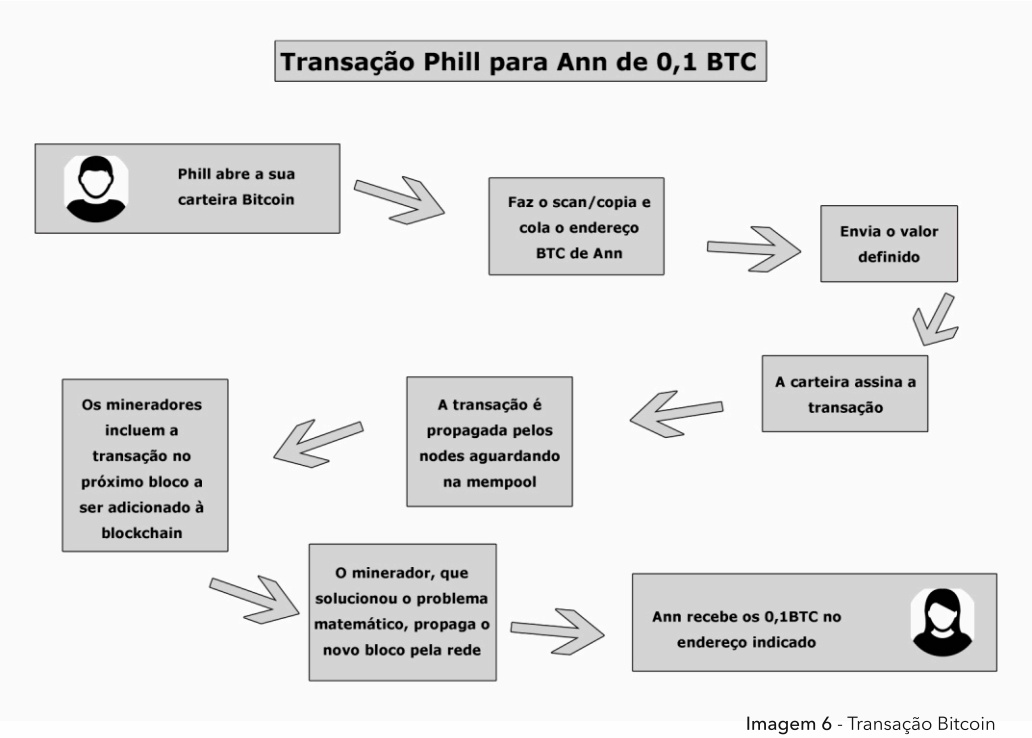

Imagem 6 - Transação Bitcoin

Mempool, taxas e gargalo

Esta capacidade de decidir quais as transações mais rentáveis vai criar uma espécie de "área de espera" – a mempool ou pool de memória. Aqui, os pedidos de confirmação de transação aguardam até que um minerador selecione e confirme a transação. Pela lógica, em períodos de grande afluência (congestionamento da rede), as taxas serão mais altas e nos períodos de menor congestionamento os mineradores confirmarão toda e qualquer transação.

Este fenómeno denomina-se por efeito de funil ou gargalo.

Num exemplo prático: um utilizador de autoestrada, que investiu no aluguer de um identificador de pagamento rápido, consegue ter a sua confirmação de entrada e saída da via muito mais, rapidamente, do que aqueles que não quiseram pagar pelo equipamento. Nas horas de ponta têm de esperar na fila até que possam confirmar a sua entrada ou saída da rodovia. O utilizador, que pagou pelo identificador, tem uma validação mais rápida.

Neste contexto, uma das formas para se poupar nas taxas de transação é utilizar a rede em períodos de menor congestionamento. Por outro lado, dever-se-á evitar várias transações de saída de uma carteira para o mesmo endereço. Juntar todos os fundos e transferi-los de uma só vez é, igualmente, um modo de reduzir as taxas de rede.

"Poderá fazer sentido ter algumas (bitcoins) caso (a tendência) pegue. Se pessoas suficientes pensarem da mesma forma, testemunharemos uma profecia auto-realizável. Quando isso acontecer será possível desenvolver variadas aplicações para o mundo real."

Satoshi Nakamoto

Parte 2
CONSTRUIR O FUTURO, ATUALIZANDO-SE

"Poderá fazer sentïdo ter algumas (bïtcoïns) caso (a tendêncïa) pegue. Se pessoas sufïcïentes pensarem da mesma forma, testemunharemos uma profecïa auto-realïzável. Quando ïsso acontecer será possível desenvolver varïadas aplïcações para o mundo real."

Satoshï Nakamoto

Anteriormente, foi descrito o problema da escalabilidade do Bitcoin. O seu código, ao limitar a 1 Mb o tamanho do bloco a adicionar à blockchain, a cada 10 minutos, faz com que somente cerca de 2000 transações sejam confirmadas por cada bloco, isto é, o reduzido número de 7 transações por segundo (TPS).

Bitcoin Cash - o Hard Fork

Este problema da escalabilidade levou, em 2017, à criação de uma nova criptomoeda com base no código original – o Bitcoin Cash. Surgiu em resposta a uma necessidade de aumentar a escalabilidade da Blockchain, permitindo a possibilidade de mais transações validadas por segundo. A base foi a alteração do tamanho do bloco para 8 Megabytes. Desta forma, mais transações são incluídas no mesmo bloco. Com esta alteração foi possível aumentar a capacidade de confirmação de 7 para 116 TPS.

O hard fork ocorreu, uma vez que a blockchain nessa data (1 de Agosto de 2017) se dividiu, dando origem a caminhos diferentes, mas paralelos, e onde circulam duas criptomoedas diferentes. Não alongo esta temática. Fiz uma alusão sumária, somente, com o intuito de contextualizar o SegWit (descrito em seguida). A criação da nova moeda foi uma resposta à adoção, pelo Bitcoin, desse protocolo revolucionário, mas polémico na altura.

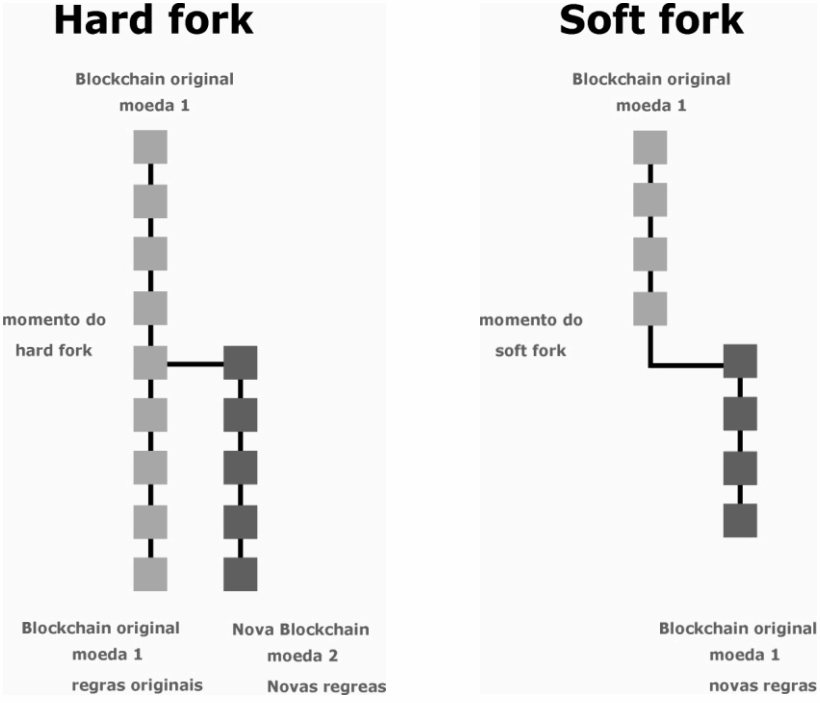

Imagem 7 - Forks

"Poderá fazer sentïdo ter algumas (bïtcoïns) caso (a tendêncïa) pegue. Se pessoas sufïcïentes pensarem da mesma forma, testemunharemos uma profecïa auto-realïzável. Quando ïsso acontecer será possível desenvolver varïadas aplïcações para o mundo real."

Satoshï Nakamoto

Capítulo 3. **BGV - Bitcoin à Grande Vitesse**
SegWit - Segregated Witness

Problema da maleabilidade

Um dos problemas detetados na rede onde circula o Bitcoin foi a maleabilidade das transações. Uma pequena alteração, não autorizada, na ID da transação, faria com que um utilizador desonesto recebesse o dobro do valor, em duas transações diferentes.

Exemplo: Ann envia 2 Bitcoins para o endereço de Phill. Phill recebe os Bictoins, mas altera, maliciosamente, o ID da transação. Esta deixa de ser visível no livro de registos, com a ID original, apesar de ter sido realizada. Phill, então, umas horas depois, solicita um novo pagamento a Ann, informando que não recebeu os fundos, atuando, assim, de forma ilícita. Ann, que os enviou, não encontra o ID (original) da sua transação no registo e assume que ficou pendente. Volta a realizar uma nova transação, agora, com uma taxa de rede mais alta (o que foi explicado sobre o mempool e a "auto-estrada"). Phill recebe, desta forma, o dobro da quantia.

Contudo, o importante, não é descrever o problema em si, mas contextualizar-te no aparecimento do update SegWit, um soft-fork, considerando que as alterações preservaram o protocolo original, isto é, não deram lugar a um novo caminho e a uma nova moeda.

Como referido, anteriormente, uma transação tem de ser assinada pelo remetente. Esta assinatura vai provar que os fundos são, efetivamente, de quem os envia. Essa transação será incluída num novo bloco, que é adicionado à blockchain, o qual incluí um número limitado de transações, uma vez que o seu tamanho máximo é de 1 Mb, pelo que só as transações com maior taxa de rede serão incluídas e, deste modo, confirmadas - problema da escalabilidade.

Repito, algumas vezes, o que foi referido, pelo facto de ser um método mais fácil de revisão e sistematização dos conteúdos.

Permitir um maior número de transações implica aumentar a capacidade do bloco ou reduzir a memória, que cada transação ocupa. Satoshi limitou no código o tamanho máximo do bloco (1Mb), como visto atrás. Deste modo, reduzir o tamanho da informação da transação, a incluir no bloco, será a alternativa.

Assinatura

A informação de uma transação na rede Bitcoin inclui a assinatura (testemunha), a prova que os fundos são, efetivamente, do emissor. Porém, esse conteúdo tem um peso de 65% do total da memória da transação, quase 2/3 do que esta ocupa no bloco.

O que o SegWit faz é remover esse conteúdo da transação (segregação da testemunha) e armazená-lo numa side chain (cadeia paralela) e fora da blockchain principal. O tamanho de memória, que a transação ocupa no bloco é, substancialmente, reduzido, permitindo que mais transações sejam adicionadas ao mesmo bloco para a sua confirmação.

Um maior número de transações incluídas por bloco conduz a mais transações confirmadas simultaneamente, aumentando o TPS e reduzindo as taxas de rede.

Por outro lado, ao remover a testemunha dos dados da transação, não é mais possível alterar essa informação. Pieter Wuille, ao criar esta atualização, abriu a caixa de pandora da blockchain, facilitando o aparecimento de outras funcionalidades, como protocolos de segunda camada e contratos inteligentes.

Ao criar, ainda que acidentalmente, este update, Pieter Wuille facilitou algo inimaginável, a possibilidade de micropagamentos (Lightning Network).

"Poderá fazer sentïdo ter algumas (bïtcoïns) caso (a tendêncïa) pegue. Se pessoas sufïcïentes pensarem da mesma forma, testemunharemos uma profecïa auto-realïzável. Quando ïsso acontecer será possível desenvolver varïadas aplïcações para o mundo real."

Satoshï Nakamoto

Lightning (Relâmpago)

A menor distância entre dois pontos é uma reta. Contudo, no Universo, nem sempre é possível levar a efeito essa regra. O caso dos relâmpagos (lightning, em inglês) é o melhor exemplo de como um raio se desloca no espaço, de acordo com a resistência com que se depara, encontrando, assim, a melhor rota e o trajeto mais eficiente.

A Lightning Network funciona seguindo esse princípio: um pagamento entre dois utilizadores encontrará, sempre, a rota mais rápida e eficiente entre eles.

Contextualização

Um micropagamento é, como o próprio nome indica, uma transação de valor muito reduzido. A realidade da primeira camada da rede blockchain não permite que este tipo de transações seja exequível. No exemplo apresentado, do pagamento do café, a taxa de rede para confirmação rápida seria, várias vezes, maior que o valor do próprio café, podendo dar-se a eventualidade de só o ter em mão, 10min depois de o pagar, caso o proprietário do estabelecimento só servisse, após a receção dos fundos.

Por outro lado, sem a existência do SegWit, ao efetuar esse micropagamento, independentemente dos custos da taxa de rede, o proprietário do café, agindo de forma maliciosa, editava o ID da transação, antes da confirmação, recebendo por 1 café o valor de 2.

Como a Lightning Network foi concebida e vocacionada para micropagamentos não confirmados, o seu funcionamento não seria exequível, sem o desenvolvimento do SegWit.

Neste enquadramento, desenvolveu-se algo que, na minha perceção, será utilizado, mundialmente e num futuro próximo, no sistema de micropagamentos do nosso quotidiano.

Canais de pagamento, smart contracts (contratos inteligentes), Multisig (assinatura múltipla)

Para se compreender o funcionamento da Lightning Network é necessário perceber alguns conceitos, nomeadamente: canais de pagamento, smart contracts e carteiras multisig.

O sistema Lightning Network foi proposto, pela primeira vez, por Joseph Poon e Thaddeus Dryja, em 2015. O objetivo era apresentar uma alternativa capaz de dar ao Bitcoin a possibilidade de ser utilizado como forma de pagamento no dia-a-dia. Os criadores pretendiam facultar à blockchain uma ferramenta, que aumentasse a sua escalabilidade, mas que, simultaneamente, respeitasse os requisitos necessários à sua compatibilidade com os princípios de segurança e programação do código original.

A base de funcionamento da Lightning Network são as carteiras MultiSig e os seus smart contracts (contratos inteligentes). Trata-se de códigos de programação de execução autónoma. No caso da Lightning Network, os smart contracts são do tipo MultiSig, assinatura múltipla, onde dois ou mais utilizadores validam e confirmam as transações com as suas assinaturas. Estes contratos inteligentes criam os canais de pagamento dentro da Lightning Network.

Exemplo: Ann é dona de uma tabacaria e Phill compra o Jornal todos os dias. Para facilitar os pagamentos, a Ann e o Phill abrem um

canal de pagamento entre eles, criado a partir de uma carteira multisig, na qual é executado um smart contract, onde todas as transações são confirmadas por ambas as assinaturas.

Diariamente, Phill envia o valor do jornal a Ann, dentro desse canal, e, sempre que existe uma transferência, ambos assinam a atualização dos saldos dos extratos de cada um, daí MultiSig (assinatura múltipla).

Todas estas transações não ficam registadas na blockchain principal, pois ocorrem numa camada diferente, a segunda camada. Os mecanismos de registo e validação na blockchain principal, são ultrapassados, reduzindo o tempo de confirmação e taxas de rede da transação.

Para que Phill possa enviar, diariamente, o valor do jornal a Ann necessita de ter fundos na sua carteira MultiSig (cofre). Para tal, deposita fundos provenientes da sua carteira Bitcoin. Esta transação é a que fica registada na blockchain principal (transação inicial). Depois da disponibilização dos fundos na carteira MultiSig, Phill pode transferi-los, rapidamente, entre os vários canais de pagamento abertos, incluindo o que criou com Ann.

Quando a Ann ou o Phill pretenderem finalizar o contrato, fecham o canal de pagamento e retiram os fundos, essa é a outra transação registada na blockchain principal (transação de finalização).

Pode dizer-se que os endereços MultiSig são uma espécie de carteiras pré-pagas. Até ao valor máximo depositado, é possível transferir fundos entre os utilizadores, que assinam o contrato inteligente.

O facto de apenas duas transações, inicial e de finalização, ficarem registadas na blockchain principal, torna este sistema capaz de ser utilizado em pagamentos de pequenas quantias no nosso quotidiano (micropagamentos). O número de transações dentro do canal de pagamento é ilimitado e quase instantâneo. Apenas, o valor de fundos, nele depositado, e bloqueado determina o máximo de fundos, possível transferir entre os utilizadores.

Invoice - Fatura

Uma característica interessante na rede Lightning é o facto de nenhum utilizador poder enviar um pagamento sem existir uma "fatura", previamente, criada pelo recetor, ou seja, o recetor dos fundos emite a fatura antes do pagamento ser efetuado e, após, a emissão dessa "fatura", é gerado o código, através do qual o emissor poderá enviar o montante definido.

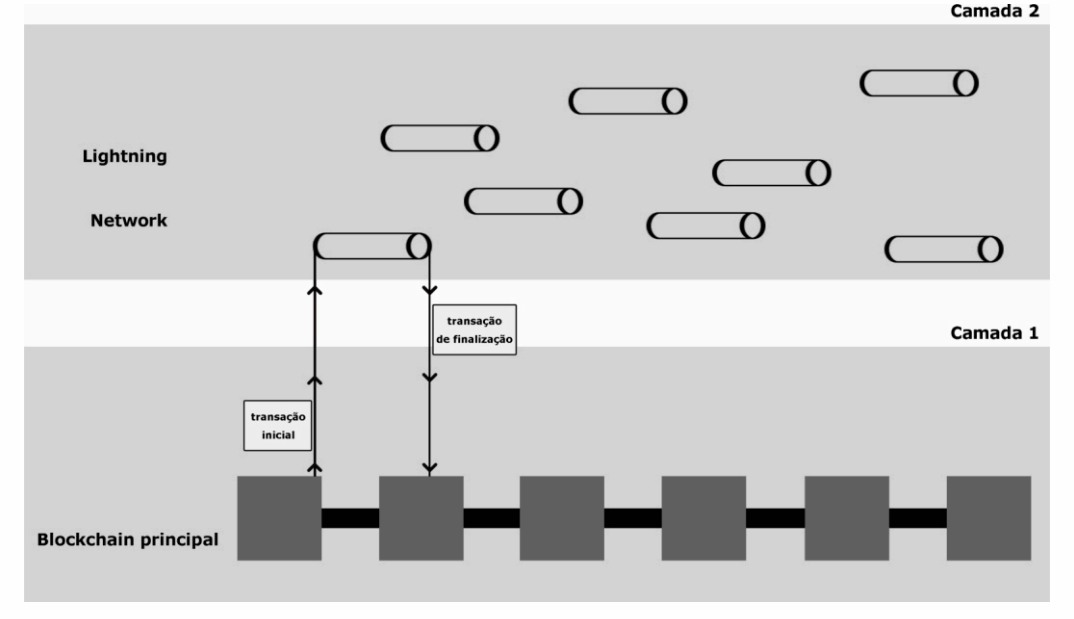

Imagem 8 - Camadas Blockchain

"Poderá fazer sentïdo ter algumas (bïtcoïns) caso (a tendêncïa) pegue. Se pessoas sufïcïentes pensarem da mesma forma, testemunharemos uma profecïa auto-realïzável. Quando ïsso acontecer será possível desenvolver varïadas aplïcações para o mundo real."

Satoshï Nakamoto

Ligações entre os nós

Para uma maior eficiência, a rede permite a abertura de um canal de pagamento, entre dois utilizadores, servindo-se das ligações pré-existentes. Caso contrário seria complexo o seu funcionamento com incontáveis canais de pagamento.

Exemplo: a Ann e o Phil têm um canal de pagamento aberto. A Ann tem um canal de pagamento aberto com a Jane. O Phil tem um canal de pagamento aberto com o Sam. Caso o Sam pretenda enviar fundos para a Jane, a rede assume a ligação, existente entre todos, como sendo o canal Sam – (Phill - Ann) - Jane.

Havendo necessidade de privacidade, a integridade da mensagem tem de ser garantida. Apesar de serem nodes (nós) intermediários de rede, Phill e Ann não devem ter acesso ao conteúdo e à informação da mensagem (pagamento), enviada de Sam para Jane. É neste contexto que surge a técnica Onion Routing (Roteamento Cebola).

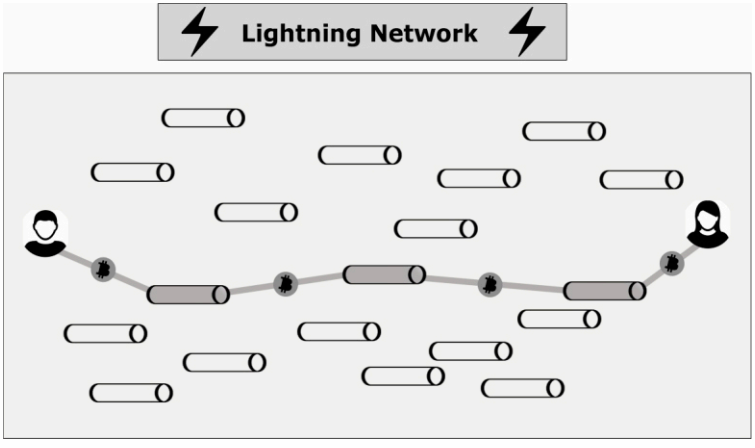

Imagem 9 - Lightning Network

Onion Routing

A técnica de roteamento Onion (cebola em inglês) é utilizada nas transações de pagamentos da Lightning Network.

Esta técnica implica que a mensagem seja encapsulada em várias camadas de criptografia, à semelhança de uma cebola (que é constituída por várias camadas).

Os dados da mensagem (pagamento) são transmitidos pelos vários nós da rede (computadores/utilizadores, que se ligam entre si). Porém, ao estarem encriptados em várias camadas, cada nó só irá conseguir desencriptar a parte, que lhe está associada. Ao desencriptar saberá, também, o nó seguinte, para o qual deverá enviar a mensagem. A última camada a ser desencriptada é a que leva ao destino final. Desta forma, cada nó só tem acesso à informação do nó que o antecede, imediatamente, e ao nó seguinte para onde deve encaminhar a mensagem.

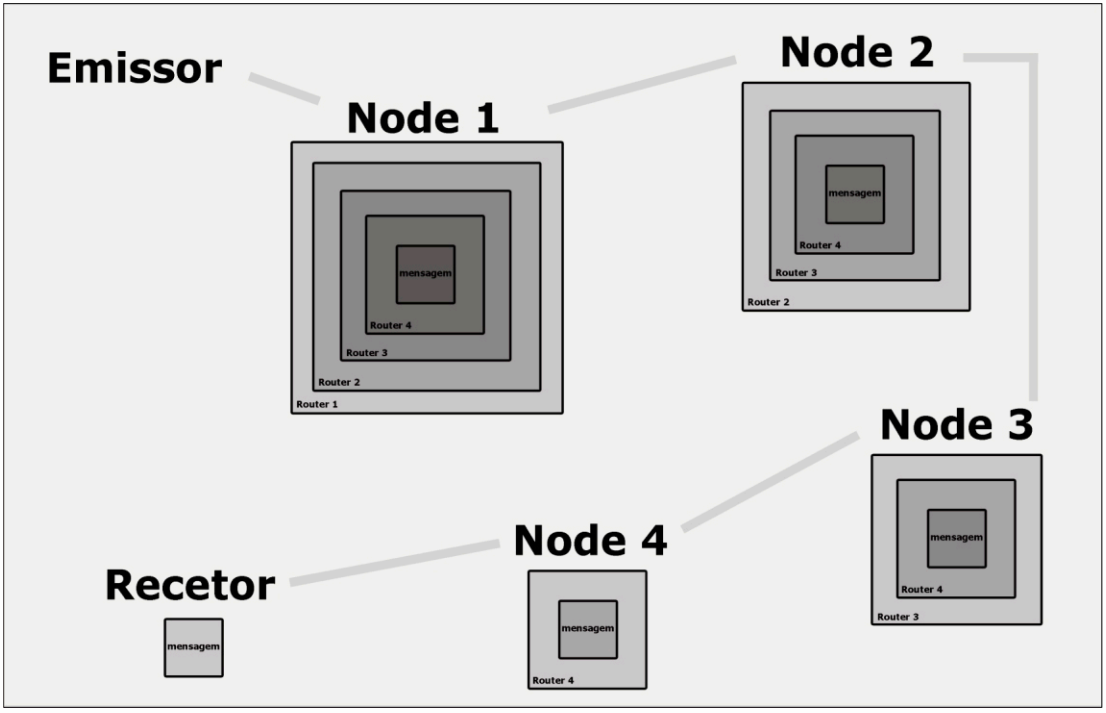

Imagem 10 - Onion Routing

Source Routing (Cálculo da rota)

Quando é enviado um pagamento, através da rede Lightning, o trajeto ou caminho é calculado, previamente, pelo emissor. Este cálculo e determinação dos nós a utilizar, até chegar ao destino final, chama-se de Source Routing e permite uma maior privacidade no envio das mensagens.

Os nós intermediários só têm acesso aos dados a que estão autorizados a aceder. Este método difere de outros em que os nós intermediários determinam o nó seguinte, não existindo um trajeto, previamente, definido.

O mecanismo de cálculo da rota está limitado a 20 nós. Assim, o emissor do pagamento efetua as instruções de encriptação em camadas. Cada nó, através do qual o pagamento irá circular, pode desencriptar a sua parte, conhecendo, como dito anteriormente, o nó que o antecede e o nó seguinte de destino (analogia às camadas da cebola).

Com esta combinação de técnicas de roteamento (Onion e Source), o emissor e o destinatário têm as identidades protegidas, o que confere à rede um grau elevado de privacidade e sigilo, bem como uma maior resistência à censura.

"Poderá fazer sentïdo ter algumas (bïtcoïns) caso (a tendêncïa) pegue. Se pessoas sufïcïentes pensarem da mesma forma, testemunharemos uma profecïa auto-realïzável. Quando ïsso acontecer será possível desenvolver varïadas aplïcações para o mundo real."

Satoshï Nakamoto

Capítulo 3. **BGV - Bitcoin à Grande Vitesse**
Taproot - Atualização e evolução.

Taproot - Atualização e evolução

Uma das maiores vantagens do Bitcoin é o facto de, ao contrário do dinheiro fiduciário, não ser estático. Ele tem a capacidade de evoluir, através de várias atualizações, tornando-se mais adaptado à realidade intemporal, mais robusto e capaz de ultrapassar as barreiras e problemas, que surgem ao longo do tempo. Esta possibilidade de se adaptar, atualizar e evoluir confere ao Bitcoin um incremento inato do seu valor.

Taproot é a raiz axial de uma planta, que cresce em direção ao interior do solo, ramificando-se em todas as direções, tornando-a mais fixa e sustentada ao seu local de plantação.

Este soft-fork (Taproot) dará ao Bitcoin mais sustentabilidade de rede; expansão, pela adoção de novos recursos e melhorias na segurança e escalabilidade.

A analogia com a raiz das plantas conduziu à utilização do termo.

Sistema de Votação

As melhorias implementadas são, sempre, propostas e votadas num sistema descentralizado e aprovadas por maioria dos participantes na rede – mineradores. O consenso é imperativo!

As sugestões de alteração ou mudança denominam-se de BIPs (Bitcoin Improvement Proposal). Neste sistema de governação é necessária uma grande uniformidade nas decisões, visando tornar o protocolo aceite e compatível com as diferentes realidades dos vários mineradores. Ásia, Europa ou América… possuem contextos distintos, conferindo-lhes realidades de mineração diversificadas, nas vertentes: económica, legal, política ou de acesso aos recursos, entre outras.

Em 2017, o BIP-141 foi votado, resultando na aprovação do SegWit (segregação da testemunha). Esse evento, pelas divergências que a proposta gerou, conduziu, como já descrito, ao surgimento da nova moeda Bitcoin Cash. Esta possibilidade evidencia que o Bitcoin promove a liberdade de decisão e efetiva a prática da democracia.

Aprovação do Taproot

O sistema de votação, no caso do Taproot, foi definido com o seguinte esquema:

- a cada conjunto de 2016 blocos minerados, sensivelmente 2 semanas, há um ajuste da dificuldade da rede;
- durante este período, os mineradores sinalizavam, em cada bloco minerado, o seu apoio à atualização;
- sabendo que, para a sua aprovação era necessária uma supermaioria de 90%, o valor de 1816 blocos sinalizados, com apoio, seria o suficiente para a aprovação do soft-fork.

No entanto, o limite estabelecido para a obtenção de consenso foi de 6 períodos (12 semanas). Então, se em cerca de 3 meses não houvesse um período de mineração, com 90% de votos favoráveis (blocos minerados sinalizados com apoio), o Taproot não seria implementado.

O período eleitoral de 6 epochs (períodos de mineração de 2 semanas) teve início a 1 de maio de 2021 e a 12 de junho de 2021, o bloco 687285 confirmou o lock-in (aprovação) do Taproot. Este será ativado no bloco 709632, cuja mineração prevê-se a 14 de Novembro de 2021.

O dia 12 de junho de 2021 marca um momento histórico na vida do Bitcoin, um sentimento, apenas, vivido em 2017, aquando da aprovação do SegWit.

Taproot - o que muda

O desenvolvimento do Taproot teve um foco no aumento da privacidade, da segurança, da fungibilidade e da facilidade de utilização dos smart contracts. A maior alteração será ao nível das assinaturas. A facilidade de criação e utilização de contratos inteligentes é, indubitavelmente, outra vantagem desta atualização, a qual permitirá ao ecossistema e ao protocolo Bitcoin evoluírem, no sentido de se tornarem mais adaptados à realidade atual do criptoespaço.

Assinaturas Schnorr

Satoshi Nakamoto optou pelo Algoritmo de Assinatura Digital de Curvas Elípticas (ECDSA) quando escreveu o código do Bitcoin. Em 2008, este era o standard de utilização. A escolha deveu-se ao facto das assinaturas Schnorr, desenvolvidas e patenteadas por Claus-Peter Schnorr, nos anos 80, não serem, amplamente, utilizadas no ano de apresentação do Bitcoin, ao mundo.

A patente, ao manter-se em vigor até 2008, impediu a sua utilização massiva, durante esse período. Acredita-se que o génio, por trás da criação do Bitcoin, teria optado por este tipo de assinaturas, se as mesmas fossem de utilização, em massa, e identificadas como padrão.

Linearidade como Vantagem

O protocolo de assinatura de Schnorr é passível de ser utilizado em esquemas multiassinatura, dado que a assinatura conjunta resultante apresenta o mesmo tamanho de uma assinatura simples.

Em virtude do tamanho da assinatura não se alterar, independentemente do número de signatários, que participam no processo de assinatura da transação, confirma-se o comportamento linear, deste protocolo, em relação ao tamanho da assinatura resultante.

MultiSig com assinaturas Schnorr

A alteração do sistema de assinaturas beneficiará todos: utilizadores individuais e exchanges. A fungibilidade do Bitcoin aumentará, na medida em que este novo tipo de assinaturas confere uma maior privacidade nas transações MultiSig.

Não será possível reconhecer transações MultiSig. O protocolo Schnorr condensa todas as assinaturas, envolvidas numa transação MultiSig, numa única chave - agregação de chaves - a qual assina a transação. O método e tipo de assinatura envolvidos nas transferências de fundos tornarão, virtualmente impossíveis de distinguir, transações de contratos inteligentes, endereços individuais ou endereços MultiSig.

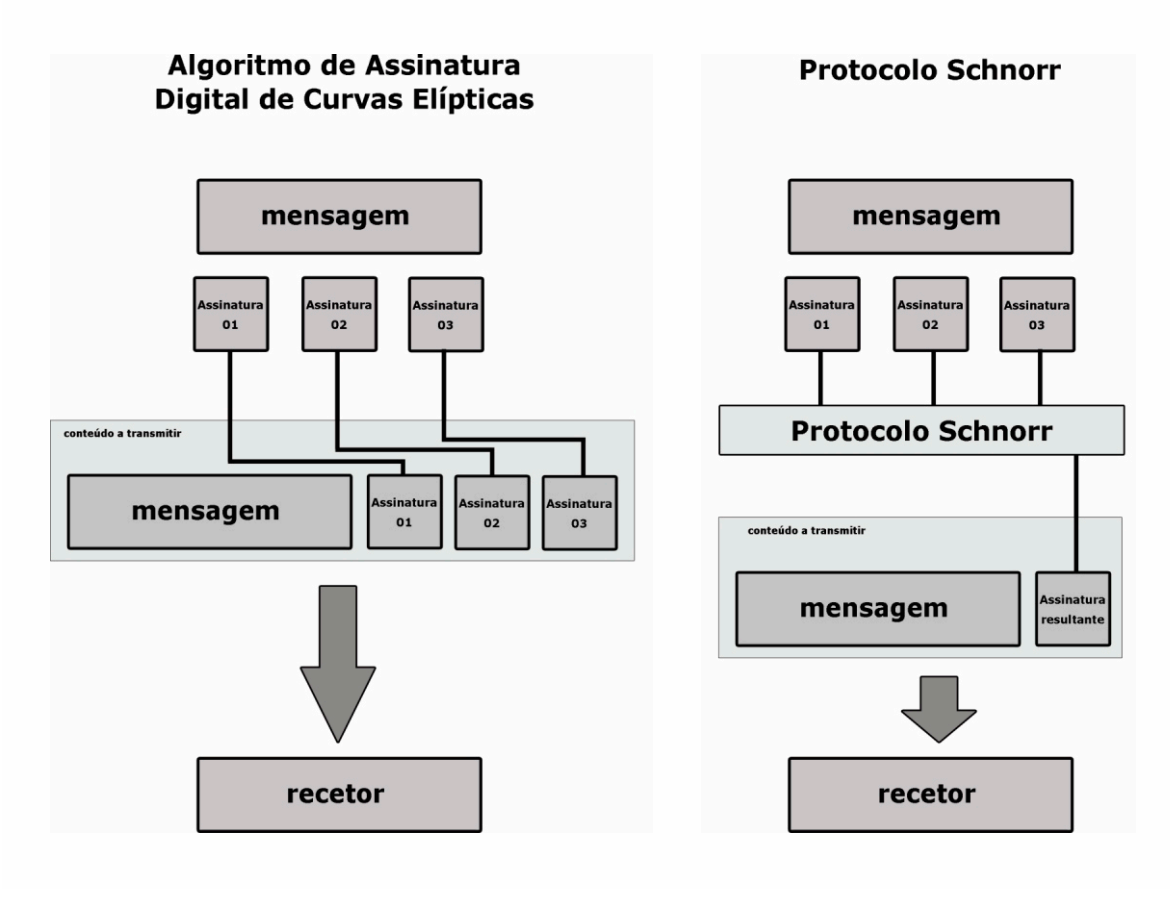

Imagem 11 - Assinaturas ECDSA vs Schnorr

Fungibilidade

Este novo esquema tornará o Bitcoin muito mais fungível. As origens e a história dos gastos de Bitcoins serão indistinguíveis. A rede tornar-se-á mais opaca, menos identificável, mais fungível e, como tal, menos resistente à censura. O tracking (seguimento) será, praticamente, impossível. As "impressões digitais", registadas no trajeto percorrido pelos fundos, tornar-se-ão mais complexas de detetar.

Tal como acontece no dinheiro físico, uma nota de 50 Euros pode ter sido utilizada em operações ilícitas, contudo, não é possível detetar tal situação em ambiente normal de circulação. Independentemente das transações em que esteve envolvida, o seu valor, de 50 Euros, mantém-se inalterado.

Caso o protocolo Bitcoin não reúna um determinado nível de fungibilidade, corre-se o risco de, no futuro, uma determinada moeda minerada, ao ser identificada como envolvida em transações menos corretas ou noutro tipo de movimentações, implicar uma perda do seu valor, por rejeição dos utilizadores.

Redução do peso de memória

Ao agregar várias assinaturas numa só, a memória utilizada na transação será menor.

Atualmente, o peso das assinaturas é de 72bytes e com assinaturas Schnorr esse peso diminuirá para 64bytes (redução de 11 a 12%). Menos memória utilizada na transação conduzirá a um maior número de transações incluídas no bloco, o que implicará um decréscimo das taxas. Estas, pagas pelos Exchanges nas suas transações MultiSig, poderão reduzir em cerca de 30%, esperando-se que a situação se reflita no cliente.

Smart contracts - Lightning Network e DeFi

No sistema Lightning Network, as assinaturas Schnorr permitirão que os contratos do tipo Hash Time Locked Contracts (HTLCs) passem a ser do tipo Point Time Locked Contracts (PTLCs). Esta alteração aumentará a privacidade e diminuirá a possibilidade de tracking, uma vez que a cada node é adicionado um conjunto de informações aleatórias.

Estes contratos PTLC permitirão, da mesma forma, uma lógica de contrato inteligente mais complexa, criando condições de garantia à blockchain sem precedentes. Simultaneamente, vão melhorar os oráculos (sistemas de ligação e transmissão de dados com o exterior da blockchain).

Por outro lado, a criação de smart contracts tornar-se-á mais facilitada e menos dispendiosa.

Os novos contratos de log discreto (DLCs) serão mais fáceis de utilizar na blockchain do Bitcoin. Estes estão projetados para conectar a blockchain com o mundo real, estabelecendo pontes de comunicação, que trazem informações do mundo físico para o interior da blockchain.

A facilidade de criação e utilização de smart contracts dará à blockchain a possibilidade, à semelhança da rede Ethereum, de desenvolvimento e funcionamento de dApps, abreviatura de Decentralized Applications (aplicações descentralizadas). Com isto, o mundo das Finanças Descentralizadas, DeFi (Decentralized Finance), as suas vantagens (e também desvantagens), possibilidades, funcionalidades e potencialidade ficarão ao alcance do Bitcoin.

"Se você não acredita ou não entende, não tenho tempo para tentar convencer, desculpe.."

Satoshi Nakamoto

O mundo moderno tem evoluído de forma acelerada. Ainda há pouco telefonávamos para casa uns dos outros e num intervalo reduzido de tempo passámos a efetuar chamadas em dispositivos móveis.

Os telemóveis, para além do exercício de comunicação, eram utilizados, ludicamente, para o passatempo do "jogo da serpente". Converteram-se em potentes e eficientes equipamentos capazes de processar jogos online, em tempo real; de transmitir emissões de televisão em direto; de permitir a visualização em streaming de filmes e séries; como alternativa ao GPS dos veículos e, em certas situações, como substitutos do computador pessoal, entre outras funções.

À semelhança da evolução tecnológica dos telemóveis, também, não estará muito distante a evolução dos métodos de pagamento. Estes basear-se-ão num sistema financeiro universal, livre, transparente e descentralizado.

Como disse no início, este pequeno livro é, somente, a porta de entrada para um amanhã, que vislumbro como realidade futura. Viveremos num ambiente em que receber o salário, ao minuto, poderá ser uma opção do trabalhador ou entidade patronal. O pagamento pelo tempo de visualização de um filme ou evento desportivo, por via de uma carteira digital, instalada no televisor, computador ou dispositivo móvel passará a ser habitual. Alugar uma viatura e efetuar o pagamento durante a sua circulação tornar-se-á comum no serviço de rent-a-car.

Pagamentos em cafés, tabacarias, supermercados ou frutarias, entre outros, consumar-se-ão recorrendo à tecnologia Lightning Network.

A Internet das Coisas, conceito que demonstra como dispositivos vão poder comunicar entre si sem intervenção humana, como já ocorre hoje em dia, vão dar lugar aos "pagamentos entre coisas".

Receber Satoshis por assistir a um anúncio publicitário ou enviar Satoshis para ler um artigo será tão usual como utilizar hoje um motor de busca.

A Lightning Network é, na minha perceção, situada na realidade à data da escrita deste livro, a resposta à necessidade de escalabilidade da rede, onde circula o Bitcoin.

A blockchain, até ao momento, é a base de dados mais robusta, segura, transparente e em funcionamento, criada pelo Homem. No entanto, carece de maior escalabilidade para uma utilização massiva.

Acredito que o Bitcoin não substitua, na totalidade, o dinheiro fiduciário. O correio eletrónico não terminou com o serviço de correio físico. Cartões bancários, contas bancárias ou intermediários de pagamento converter-se-ão em opção pessoal de utilização.

As características de segurança, transparência e descentralização da blockchain, associadas às possibilidades, que o protocolo SegWit lhe conferiu e à velocidade proporcionada pela Lightning Network, tornam possível vivermos numa realidade, onde a confirmação descentralizada de pagamentos será tão ou mais rápida, tendo como comparação a rede centralizada Visa.

O resultado de vasta pesquisa/investigação, análise e estudo, durante largo período de tempo, levou à escrita deste pequeno, prático e importante livro entre os meses de maio e setembro, de 2021.

Naturalmente, no futuro, ficará desatualizado, dadas as constantes atualizações ao protocolo Bitcoin. A fantástica atualização Taproot, que será feita à rede blockchain do Bitcoin, com implementação prevista para novembro, de 2021, como referido, atesta isso mesmo. O Bitcoin evolui, não é estático.

Propositadamente, não aprofundei toda a informação aqui descrita. Realizei, somente, uma abordagem superficial de todo o protocolo e da sua abertura à possível evolução. Percorrer o caminho, investigando e ampliando o conhecimento, nesta temática, já será uma opção tua.

Porém, saber que o leste, até aqui, constitui, para mim, motivo de grande alegria. É sinal que consegui captar a tua atenção e despertar a tua curiosidade para algo que me fascina e apaixona. Somos privilegiados por viver num Mundo em que a tecnologia, criada por Satoshi Nakamoto, dirige-se para uma utilização fácil, simples e tão usual, como o simples ato de ligar uma luz em nossa casa. As crenças e ideias descontextualizadas da eletricidade, nos seus primórdios, assemelham-se às incertezas do Bitcoin. O futuro encarregar-se-á de extinguir as imagens distorcidas e clarificar as dúvidas existentes.

Provavelmente, ainda nos posicionamos no ano 2 ou 3 da adoção do Bitcoin. Todas as tecnologias disruptivas demoram cerca de uma década para terem a adoção, em massa (eletricidade, motor a vapor, elevador, automóvel, telemóvel), e, sempre, passam pelo processo inicial de negação, crítica destrutiva e rejeição, até serem compreendidas e acolhidas.

A circunstância pandémica de 2020, de forma muito mais assertiva que a crise de 2008, demonstrou a premente necessidade de existir um ativo capaz de ser reserva de valor e, que simultaneamente, se apresente de fácil utilização, no nosso quotidiano, como meio de pagamento, não desvalorizando, mesmo em condições adversas.

O Bitcoin não é o Ouro 2.0. O Bitcoin é ele próprio. Escasso, deflacionário, de base matemática, impossível de falsificar, de ser, duplamente, gasto ou de ter um aumento de fornecimento, pelo que valorizar-se-á ao longo do tempo.

Quando a sua adoção for uma realidade, perceber-se-á que no início (momento atual), foi um jogo de acumulação. É possível ganhar dinheiro com Bitcoin? Sim, mas essa não é a intenção subjacente à criação deste ativo digital. O seu propósito de descentralização da confiança, criação de critérios de transparência e confirmação da robustez na segurança, não têm preço. O Bitcoin, depois de compreendido, assume valor inquantificável.

A sua volatilidade ainda é elevada, fazendo parte do processo de crescimento e definição da solidez. Para já, os maiores utilizadores são traders, especuladores e pessoas, cujo objetivo (não criticável) é o do enriquecimento. Esta circunstância gera uma instabilidade de preços diários, semanais, mensais e anuais. Quando grandes empresas, dos mais variados setores, como já testemunhamos hoje em dia, iniciarem o processo de adoção, em grande escala, e utilizarem o Bitcoin como moeda de pagamento, essa volatilidade tenderá a diminuir.

O Bitcoin é uma alternativa a um sistema incapaz de se atualizar, de se moldar e adaptar a novas circunstâncias e conjunturas.

Até 1971 a emissão de papel monetário estava ligado a um ativo, escasso, difícil de obter e capaz de valorizar com o passar do

tempo – o ouro. O Bitcoin é escasso, difícil de obter e capaz de valorizar com o passar do tempo. Tornar-se-á Reserva de Moeda Mundial? Veremos…

Ao terminar este livro, deixo um agradecimento a todos quantos tornaram possível o projeto, em particular aos meus amigos Macabis: Daniel, David, Domingos e Eduardo e a toda a equipa da LegendExotica.

E de um modo muito especial aos meus pais pelo apoio incondicional.

"Escrever uma descrição disto para o público, em geral, é muito difícil.
Não há com o que relacionar."

Satoshi Nakamoto

Será que neste ponto contrariei Satoshi Nakamoto?

Setembro de 2021
Jorge Filipe Ribeiro

Jorge Filipe Oliveira Costa Ribeiro
16 de Janeiro de 1983
Natural de Santa Maria da Feira

2008
Licenciatura em Medicina Dentária
Faculdade de Ciências da Saúde
da Universidade Fernando Pessoa

2011
Mestrado em Informática Médica
Falculdade de Medicina
da Universidade do Porto

2018/19
Frequência no Mestrado
em Segurança Informática
Depart. de Engenharia Informática
da Universidade de Coimbra

https://i2e.online