FIAP ON

BLOCKCHAIN ADVANCED

ALGORITMOS DE CONSENSO

HENRIQUE POYATOS

4

LISTA DE FIGURAS

SUMÁRIO

4 ALGORITMOS DE CONSENSO

Até o momento, abordamos vários aspectos relacionados ao Bitcoin: o que ele é, como ele funciona, como pode ser adquirido, entre outros. Ao abordar seu funcionamento, descobrimos que o mecanismo principal para tal é o *blockchain*, que revolucionou a forma que atingimos um consenso em uma rede descentralizada de participantes.

Entretanto, o *blockchain* do Bitcoin possui vantagens e desvantagens. Começaremos este capítulo falando sobre algoritmos de consenso, discutindo suas vantagens e desvantagens.

4.1 Algoritmos de consenso: definições e aspectos de segurança

Uma das características mais celebradas da tecnologia *Blockchain* é sua **descentralização**, e é graças a essa característica que é possível criar ambientes em que as partes envolvidas em uma transação ou processo podem fazê-lo diretamente, sem a necessidade do que chamamos de “terceiro de confiança”.

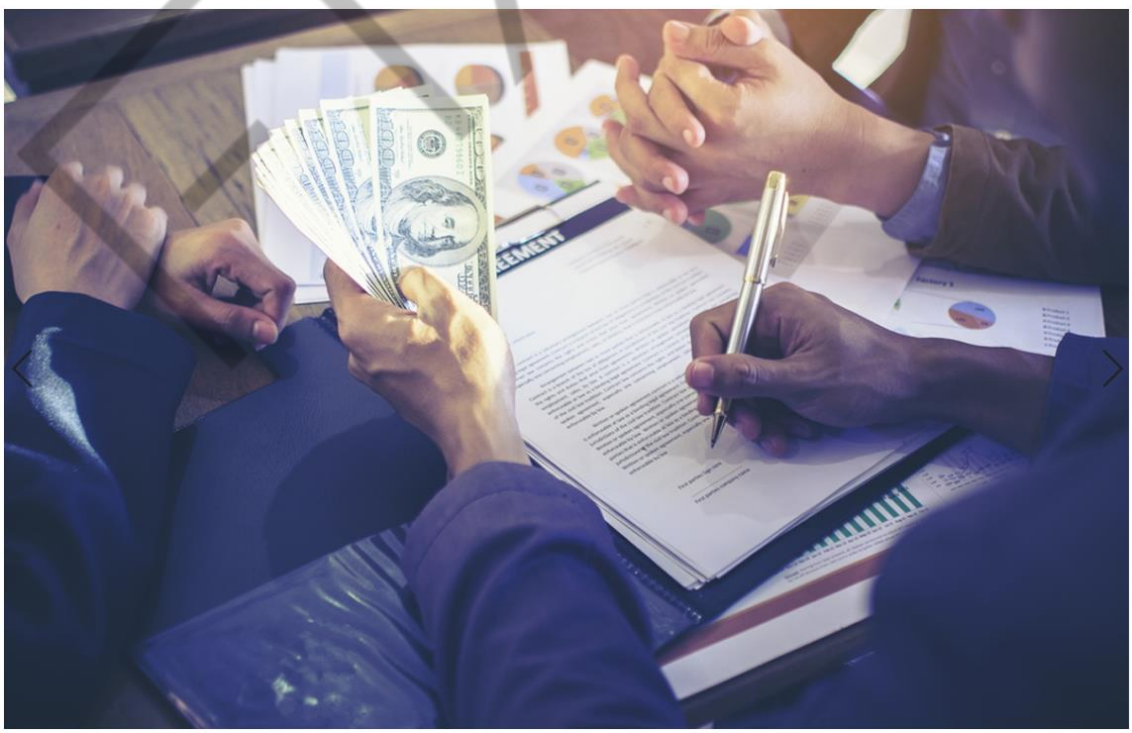

Figura 4.1 – Representação do “terceiro de confiança”
Fonte: Shutterstock (2020)

Considere o caso de uma aposta: você e um amigo resolvem fazer uma aposta, uma das partes afirmando uma coisa e a outra, o contrário. Para evitar problemas no cumprimento da aposta (especialmente no pagamento do perdedor para o ganhador), vocês decidem pagar as “quotas” dessa aposta antecipadamente, e confiam o valor a uma terceira pessoa, nosso “terceiro de confiança”. É ela que fará a custódia do prêmio e resolverá a disputa, entregando o valor total a uma das partes quando a condição da aposta for satisfeita. Como o próprio nome já indica, as partes precisam **CONFIAR** no terceiro, acreditando que ele liquidará a aposta de maneira justa e que **não fugirá com o dinheiro**.

Transações bancárias, contratos, processos de compra e venda, basicamente todas as operações envolvendo duas ou mais partes que não confiam umas nas outras requerem uma entidade central de confiança que garantirá que tudo ocorra conforme foi combinado entre as partes envolvidas.

A grande questão envolvendo entidades centrais de confiança é: até onde elas são realmente confiáveis? Elas não poderiam ser subornadas e favorecer um lado em relação a outro? Elas não poderiam fazer uso do grande poder e controle a elas confiado e impor seus próprios interesses? E a resposta é: **claro que sim**.

E essa é a grande beleza da tecnologia *Blockchain*: em vez de realizar uma atividade por intermédio de um terceiro de confiança, as partes realizam suas atividades diretamente (ponto a ponto) e as outras dezenas, centenas ou milhares de partes (e quanto mais, melhor) servem de “testemunhas” de que aquilo realmente aconteceu. As atividades realizadas (ou valores mudando de mãos) são registradas simultaneamente por todas as partes em um livro-razão (*ledger*) idêntico para todos.

Dessa forma, a confiabilidade das operações é garantida por consenso. Repare que, mesmo que haja partes maliciosas que queiram fraudar as operações registradas, elas são uma minoria que será desconsiderada, pois a maioria vence!

4.2 O problema dos generais bizantinos

O artigo publicado por Lamport, Shostak e Pease (1982) ilustra magnificamente o problema de um consenso descentralizado. Imagine uma situação em que diversas divisões do exército bizantino estão acampadas ao redor de uma cidade inimiga, e

que cada divisão desse exército é comandada pelo seu próprio general. Os generais só podem se comunicar entre si por meio de mensageiros e, depois de observar o inimigo longamente, precisam decidir por um plano comum de ação: atacar ou recuar?

Considere que, alguns desses generais foram subornados e se tornaram traidores, assim sendo, suas decisões não irão ao encontro dos generais leais; um general traidor pode decidir recuar quando o melhor plano de ação seria atacar.

Os generais bizantinos precisam de um algoritmo de consenso que:

a) Todos os generais leais decidam pelo mesmo plano de ação; eles farão o que for decidido, enquanto os traidores farão aquilo que quiserem e;

b) Um pequeno número de traidores não influencie a decisão dos generais leais, fazendo-os tomar a pior decisão.

Se todos os generais trocarem mensagens entre si, eles podem optar pelo plano de ação mais recebido, desconsiderando a opção “votada” em minoria.

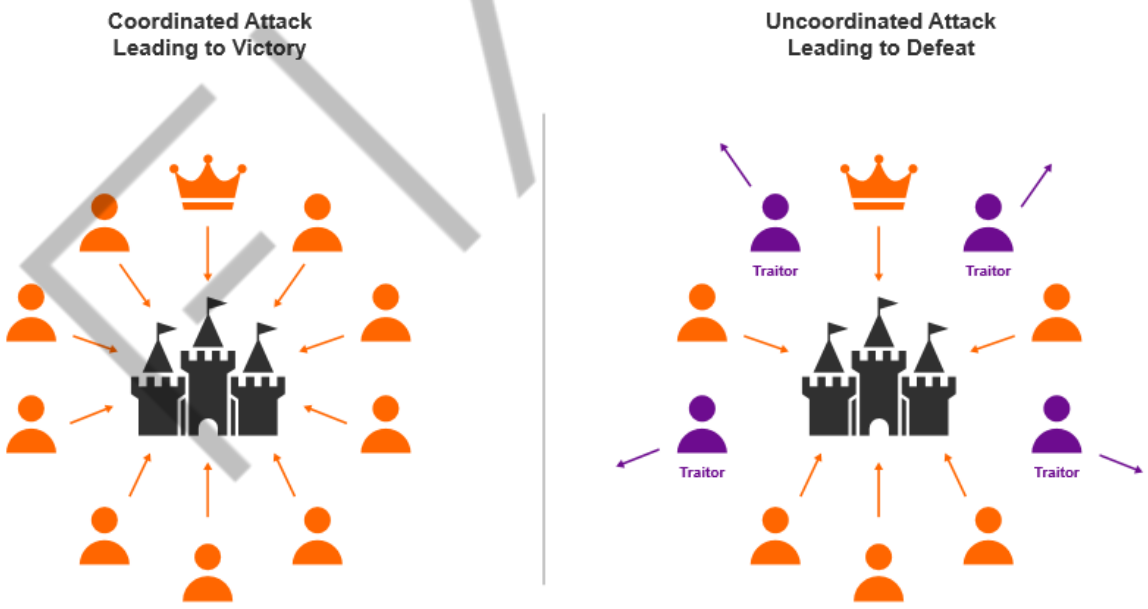

Figura 4.2 – O problema dos generais bizantinos
Fonte: GHOSH (2016)

Em um livro-razão distribuído, quaisquer entradas (as mensagens) para o livro-razão (o tempo de ataque acordado) devem ser confiáveis. As redes digitais geralmente possuem de milhares a milhões de membros ou nós (os generais) que estão dispersos globalmente e não há um comando centralizado (nenhuma

governança central), e é impossível se conhecer e confiar em todos os membros. Então, como você pode confiar nos outros membros da rede e garantir que as entradas para esse registro distribuído sejam precisas e, além disso, garantir que possua as informações corretas? O *Blockchain* resolve esse problema e, no caso do nosso general bizantino, garante que ele possa enviar mensagens confiáveis e liderar um ataque bem-sucedido e coordenado (GHOSH, 2016).

4.3 Descentralização e o ataque de 51%

O problema dos generais bizantinos também ressalta a descentralização de uma rede de *Blockchain* como um dos princípios **inegociáveis** para o pleno funcionamento de tecnologia. **Quanto mais membros independentes uma rede *Blockchain* possuir, mais segura ela se torna**. Voltando ao exemplo dos generais bizantinos, se alguém tomar o controle da maioria dos generais e esse alguém é um traidor, ele pode impor sua vontade aos demais que não tomarão a melhor decisão.

Traduzindo em termos de *Blockchain*, se alguém possuir mais de 51% dos membros de uma rede, pode confirmar operações fraudulentas ou mesmo reescrever o livro-razão como bem desejar. Damos a isso o nome de **ataque dos 51%.**

4.4 Como atingir o consenso em uma rede descentralizada

Conforme abordamos antes, além de garantir que os dados registrados nesse livro-razão são confiáveis, cada membro da rede deve possuir uma **cópia idêntica e completa** desse livro-razão. E, por se tratar de um livro-razão que é escrito a todo instante, ele é dividido em blocos que contêm as transações, operações ou dados que devem ser registrados.

Sempre que novas informações precisam ser registradas, um novo bloco deve ser criado, preenchido, validado e posicionado no final do livro-razão, incrementando esse grande documento. Esses blocos são encadeados de tal maneira que a assinatura usada para validar o bloco anterior é necessária para validar o novo bloco, criando a famosa “cadeia de blocos” que batiza a tecnologia. É esse encadeamento que torna o *blockchain* imutável, já que a alteração ou remoção de um dado já

registrado necessitaria de uma revalidação do bloco em que o dado está e todos os blocos gerados posteriormente.

No entanto, vamos abordar a seguinte questão: se as cópias do *blockchain* são idênticas, como decidir quais transações serão registradas nos novos blocos? Por meio de consenso, é claro! A cada novo bloco é eleito um membro que ganha o direito de registrar os dados no bloco, cabendo aos demais a função de validá-lo.

Vários são os algoritmos de consenso aplicados para esse fim, cada um com suas vantagens e desvantagens. Abordaremos a seguir os principais.

4.4. Proof of Work (PoW) aplicado no consenso de Nakamoto

A prova de trabalho (ou *proof of work, PoW*) é um protocolo criptográfico criado para prevenção de ataques cibernéticos de negação de serviço (*Denial of Service*) e Spam, proposto por Cynthia Dwork e Moni Naor em um artigo em 1993. O termo “prova de trabalho”, entretanto, só foi cunhado seis anos depois, em um artigo de Markus Jakobsson e Ari Juels.

Inspirado por Back (2002) que explorou a prova de trabalho para ataques de negação de serviço em um mecanismo batizado de Hashback, Satoshi Nakamoto adaptou os conceitos de prova de trabalho para que funcionasse como um algoritmo de consenso (NAKAMOTO, 2008), o que passou a ser conhecido posteriormente como consenso de Nakamoto (*Nakamoto consensus*).

4.4.1 Mecanismo

Nesta abordagem, a cada bloco um líder é eleito por meio de uma forma de “loteria”. Falando especificamente da rede Bitcoin, um enigma criptográfico é proposto pelo protocolo, e os membros que participam dessa rede se propõem a decifrá-lo. Basicamente, o enigma é a execução de uma função *hash* SHA-256 utilizando alguns dados específicos do bloco atual e um número aleatório, resultando em um *hash* que comece com um determinado número de zeros. Se o número de zeros em questão não for obtido, a função *hash* deve ser tentada utilizando outro número aleatório.

O enigma criptográfico é este: adivinhar o número aleatório (também conhecido como **nonce**) que, aliado às informações do bloco, deve resultar em um *hash* iniciado por um número de zeros. Para se ter uma ideia como a adivinhação desse número é algo trabalhoso, milhões de tentativas são feitas em um único segundo e esse processo de descoberta leva em torno de dez minutos para acontecer.

Os participantes de rede competem entre si, apostando uma corrida de quem será o primeiro a adivinhar esse número. O nó que conseguir fazer isso primeiro comunica imediatamente a todos os demais participantes qual é o número aleatório; que, por sua vez, param de utilizar números aleatoriamente e usam o número informado para validar a vitória do reclamante. Confirmada a solução do enigma, os participantes da rede, em consenso, elegem esse nó como líder.

O líder eleito tem o direito de determinar quais transações de Bitcoin não confirmadas irão compor o novo bloco; as transações realizadas e não confirmadas do Bitcoin formam um fila que o membro líder deve consultar. Em abril de 2019, o tamanho exato do bloco é de apenas 1MB, espaço capaz de armazenar aproximadamente três mil transações por vez. Todas as demais transações não escolhidas para confirmação no novo bloco permanecem na fila de espera e serão confirmadas nos blocos seguintes. Escolhidas as transações, o vencedor propaga o bloco formado para os demais participantes, e eles armazenam o bloco no final da corrente e se preparam para a próxima corrida.

4.4.2 Incentivo

O conceito de prova de trabalho está na solução do “enigma” (*puzzle*) *criptográfico*... o achado do número é a prova de que alto poder computacional foi empregado. Por se tratar de um *blockchain* público, membros podem entrar e sair da rede de Bitcoin a qualquer momento, sendo assim, podemos ter novos membros fazendo esse processo de validação. No entanto, por que alguém faria um alto investimento em equipamentos, energia elétrica e conectividade de graça?

É aqui que entra o engenhoso incentivo criado por Satoshi: o líder do bloco (e somente o líder) ganha uma recompensa em bitcoins. Para não inundar o sistema econômico gerando todos os bitcoins de uma vez, novas unidades são geradas e

inseridas no sistema a uma taxa constante. São essas novas unidades da moeda que são entregues aos líderes do consenso.

Há um princípio econômico que diz que para algo ser considerado valioso, ele precisa ser finito e escasso. Sendo assim, bitcoins não poderiam ser gerados indefinidamente e, por essa razão, o sistema foi programado para parar de gerar novas unidades quando o total atingir 21 milhões de unidades. Para tal, como pode ser visto no próprio código-fonte do Bitcoin no GitHub, temos a seguinte linha:

```
Consensus.nSubsidyHalvingInterval = 210,000
```

Código-fonte 4.1 Variável que define o intervalo de *halving*
Fonte: GitHub do projeto Bitcoin (2019)

O que significa que a cada 210 mil blocos gerados, acontece um evento conhecido como *halving*, que faz a recompensa cair pela metade. A rede começou com a recompensa de 50BTC por bloco, caindo para 25BTC em quatro anos, 12,5BTC quatro anos seguintes e em 2020 a recompensa passará a ser 6,25BTC.

Nakamoto (2008) considerou a condição desses validadores de rede análoga ao de mineradores de ouro, que empregam recursos para adicionar mais ouro em circulação no mercado, e é por essa razão que os participantes são chamados de mineradores (*miners*). Observe que, embora eles possuam esse nome, o principal papel dos mineradores é a validação das transações no *blockchain*.

Quando o último Bitcoin for gerado em algum momento no ano de 2140, Nakamoto (2008) prevê que a mineração continuará graças às taxas de rede, um valor que os emissores de transação pagam para ter prioridade em suas confirmações.

4.4.3 Vantagens e desvantagens

O consenso da Nakamoto elege seu líder em uma abordagem de loteria, ao promover um enigma criptográfico que obrigue os participantes a adivinhar o nonce cujo ***hash*** satisfaça os parâmetros do sistema. No entanto, essa abordagem seria pseudorrandômica, afinal, os membros podem investir em equipamentos que adivinhem o ***nonce*** cada vez mais depressa, aumentando suas chances de serem escolhidos. Existem hardwares especializados conhecidos como **ASICs** (*Application-specific integrated circuit*, ou circuito integrado de aplicação específica) que, diferentemente de nossos *desktops* ou *laptops* criados para múltiplos propósitos, são

concebidos especificamente para mineração de Bitcoins. Um exemplo é a Bitmain Antminer S9i que com seus 189 chips é capaz de chegar a 14.5 TH/s, ou seja, ela pode “chutar” mais de 14 trilhões de ***nonces*** em um único segundo (BITMAIN, s.d.).

Figura 4.3 – Bitmain Antminer S9i
Fonte: BITMAIN (s.d.)

As ASICs no site da Bitmain custam, em média, dois mil dólares a unidade. É possível formar um *cluster* com esse tipo de equipamento, aumentando as chances de ser tornar líder do bloco. Sendo assim, dificilmente se adquire uma única unidade, e foi assim que surgiram as fazendas de mineração.

Figura 4.4 – Fazenda de mineração clandestina em uma das antigas repúblicas soviéticas
Fonte: KRASNIKOV (2017)

Os altos preços atingidos pelo Bitcoin tornaram a atividade altamente rentável e a corrida criptográfica se tornou uma corrida por hardware. Se em seu início a mineração de Bitcoin era possível utilizando as placas de vídeos de computadores comuns, há vários anos isso se tornou inviável. Sendo assim, mineração de bitcoins é “coisa de gente grande”.

Se por um lado a escala de *hardware* torna o *blockchain* do Bitcoin mais seguro ao obrigar provas de trabalho cada vez mais complexas, por outro, torna-o inseguro ao centralizar cada vez mais a atividade na mão de poucos participantes. A Figura 4.5 mostra a atividade de mineração em um determinado dia de maio de 2019 dividida em *pools* de mineração (que podem ser uma ou mais fazendas de mineração juntando forças pelo “bem comum”).

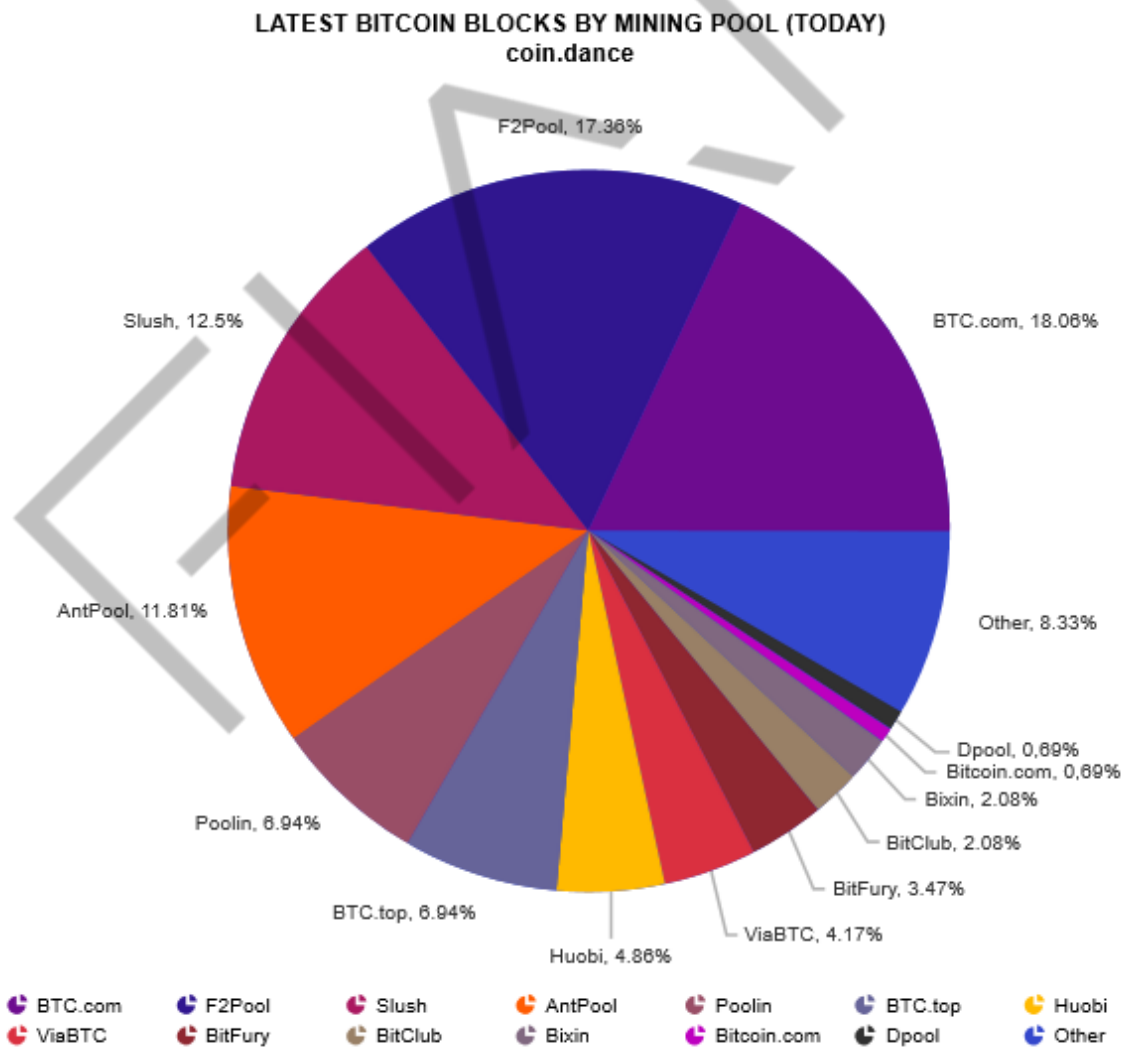

Figura 4.5 – Mineração de bitcoins por *pool* de mineração
Fonte: COINDANCE (2019)

Observe que, se os quatro principais *pools* de mineração resolvessem se tornar um só, esse novo *pool* possuiria sozinho mais da metade do poder computacional da rede, possibilitando um ataque de 51%.

Por outro lado, o altíssimo custo da prova de trabalho desse *Blockchain* também é sua principal força. Quando a Binance, uma das principais *exchanges* de criptoativos, foi hackeada em maio de 2019 foram furtados 7.000 bitcoins de sua *hotwallet*, o que seria equivalente a um prejuízo de quarenta milhões de dólares. Changpeng Zhao, CEO da Binance, discutiu publicamente em sua conta de Twitter uma “reorganização de blocos”, um eufemismo para um ataque de 51% que visaria reverter o furto.

Jimmy Song, um dos desenvolvedores do Bitcoin afirmou que, poucas horas depois do bloco minerado (e, portanto, apenas algumas dezenas de blocos depois) o custo para fazê-lo já seria superior ao prejuízo do *hack*, sem contar o prejuízo em credibilidade que a criptomoeda sofreria e o risco de um *fork* de rede gerando duas moedas diferentes, como ponderou o próprio Changpeng Zhao (CANELLIS, 2019).

Segundo o testemunho apresentado no comitê de energia e recursos naturais do senado americano em agosto de 2018, somente a rede de *blockchain* do Bitcoin consome 1% da energia elétrica gerada no planeta (BRADBURY, 2018). De acordo com Lee (2018), The Economist (2018) e Power Compare (2018), a rede de *blockchain* do Bitcoin consome entre 55,63 e 73,12 TeraWatts/h de eletricidade por ano. Para ilustrar, a Figura 4.6 traz um mapa-múndi com um comparativo do consumo da rede em relação ao consumo de países inteiros. Se o Bitcoin fosse um país, seu consumo energético seria compatível com países como a Colômbia ou o Chile.

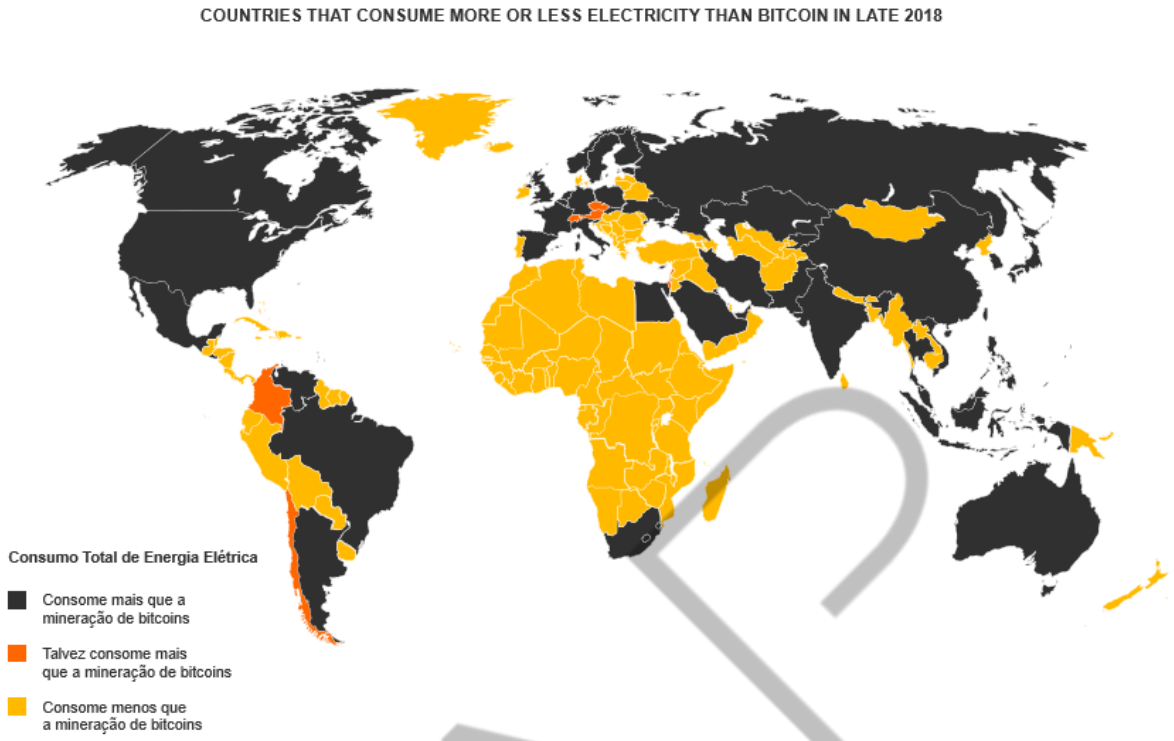

Figura 4.6 – Países que consomem mais ou menos eletricidade que a mineração de bitcoins em 2018
Fonte: POWER COMPARE (2018)

Por fim, no caso específico do Bitcoin, temos um problema de escalabilidade. Cada bloco minerado possui apenas 1 megabyte de espaço disponível para registrar as transações financeiras, o que possibilita três mil transações em média. Como cada bloco é minerado a cada dez minutos (e cada vez que o poder computacional sobe, a dificuldade para adivinhar o **nonce** também sobe proporcionalmente), a rede dessa criptomoeda seria capaz de validar apenas 7 transações por segundo, o que o inviabilizaria para uma série de aplicações.

Embora existam discussões em relação ao aumento do tamanho do bloco e validações de transações em *sidechains* (como o caso da *Lightning Network*), o consenso de Nakamoto é, por concepção e *design*, um consenso mais lento para maior controle da geração sistemática de blocos encadeados e a possibilidade de orfanar blocos que por ventura sejam gerados fora da corrente principal. Assim sendo, faz-se necessária a discussão e aplicação de outros algoritmos de consenso para diferentes aplicações.

4.5 Proof of Stake (PoS)

Em 2011, um usuário do fórum *Bitcoin talk* chamado ***Quantum Mechanic*** propôs um novo algoritmo de consenso chamado *Proof of Stake*. Embora a abordagem também envolva a eleição de um líder de forma aleatória (*lottery approach*), os candidatos a líder deixam de fazer investimentos em *hardware* e passam a fazer investimentos no próprio criptoativo que deve ser validado.

O candidato a líder se compromete a "trancar" na rede uma quantidade de criptoativos que servirá de garantia das transações que ele se propõe a validar. Dessa forma, caso o líder eleito valide transações fraudulentas, ele é punido pois sua garantia (*stake*) será utilizada para sanar eventuais prejuízos.

Trata-se de uma evolução interessante em relação à prova de trabalho aplicada no consenso de Nakamoto: embora a rede possua mecanismos para rejeitar transações fraudulentas, o responsável pela fraude não é punido, ele está "livre" para realizar novas tentativas no futuro.

O *stake* "feito de refém" pela rede e a possibilidade de ter um prejuízo financeiro desencoraja eventuais fraudes no sistema. Além disso, os validadores (e não mineradores) são proprietários de grandes somas no criptoativo que estão validando, assim sendo, permitir fraudes significaria perda de credibilidade e, por consequência, prejuízos financeiros no longo prazo. Os validadores, portanto, tornam-se os maiores interessados em manter a saúde do sistema.

4.5.1 Incentivos

Assim como acontece no consenso de Nakamoto, prevê-se uma recompensa para os membros de rede que queiram fazer esse papel de validadores. Repare que no *Proof of stake*, eles não são chamados de **mineradores** e recebem um nome mais representativo, pois **validar** as transações e promover uma confiança descentralizada é justamente o principal papel desses membros, o recebimento de novos criptoativos é uma consequência desse papel.

Por receberem como recompensa criptoativos da rede que se comprometem a validar e por serem obrigados a fazer um alto investimento nesse criptoativo para se

candidatarem ao papel de validadores (em detrimento do consenso de Nakamoto, cujo alto investimento é feito em *hardware*), eles se tornam os maiores interessados em manter a saúde financeira do sistema.

Caso optem por validar transações fraudulentas na rede, permitem o gasto duplo ou ataques de 51%, a credibilidade do criptoativo será abalada e isso se refletirá rapidamente em seu preço, que provavelmente despencará. Não esqueçamos, além disso, da própria rede detectar as fraudes e confiscar o *stake* desse validador para cobrir os prejuízos. Assim sendo, há vários estímulos para a honestidade e para o bom cumprimento do papel de validador.

4.5.2 Vantagens e desvantagens

Existem, é claro, várias críticas ao algoritmo proof of stake. Do ponto de vista econômico, boa parte do suprimento da criptomoeda seria comprometida, "estacionada" em carteiras dos membros que fazem o papel de validadores. Uma moeda "boa" é uma moeda que circula em um sistema financeiro, serve para pagamentos de produtos ou serviços, serve como unidade de valor e outras propriedades.

Um dos componentes mais importantes de precificação de um criptoativo é a quantidade dele que está sendo negociada nas exchanges, sendo comprado e vendido. Um criptoativo que possua boa parte de seu valor estacionado pode sofrer oscilações maiores em sua cotação, pois um validador em um determinado momento está com seu patrimônio "estacionado" e no momento seguinte resolve "vender tudo", tornando-se o que nesse mercado é chamado de Whale (baleia). Um grande volume de moedas sendo vendidas de uma só vez acaba comprometendo muito seu valor de mercado.

Por outro lado, o ataque de 51% se torna mais improvável em uma abordagem *proof of stake*. Se, em um exercício hipotético, o *blockchain* do Bitcoin se tornasse *Proof of stake*, seriam necessários 75 bilhões de dólares em bitcoins para efetuar um ataque de 51%, já que os mais de 17,7 milhões de unidades em circulação valiam, em maio de 2019, mais de 150 bilhões de dólares.

Por outro lado, uma vez que um membro consiga custodiar mais de 50% dos criptoativos de uma rede de *blockchain*, seria extremamente complicado reverter essa situação, pois esse membro exerceria seu poder econômico, tornando-se validador em grande parte das oportunidades e efetuando ataques de 51%, recebendo continuamente as recompensas de bloco validado e permanecendo cada vez mais "rico" naquela cripto.

Se, no consenso de Nakamoto, um único membro possuir mais de 51% da rede, pode reverter a outros membros fazendo altos investimentos em *hardware*, já a soberania e maioria em uma rede *Proof of Stake* dificilmente se reverte. Assim sendo, recomenda-se atenção, especialmente em criptoativos mais jovens e suscetíveis ao fenômeno.

O algoritmo de eleição de líder precisa respeitar um equilíbrio delicado, pois ele não pode ser totalmente randômico; o tamanho do *stake* deve ser um fator decisivo para eleição pois, quanto maior o *stake*, maior é a garantia de transações que o eleito está comprometendo no sistema, tornando-o mais seguro.

Porém o tamanho do *stake* não pode ser o único fator para a seleção pois, nesse caso, apenas os validadores mais ricos seriam escolhidos e se tornariam mais ricos, aumentando ainda mais a chance de serem escolhidos novamente e desencorajando outros validadores com *stakes* menores a fazer esse papel.

Seja um algoritmo de consenso *proof of work,* seja um *proof of stake*, há sempre a tendência à centralização, sendo assim, manter o sistema descentralizado é um desafio para qualquer ecossistema de *blockchain*.

É por essa razão que existem várias propostas de Proof of Stake. A rede Ethereum procura manter esse equilíbrio complicado com um conjunto de smart Contracts, e o consenso dessa plataforma é chamado de Casper PoS e, no momento desta escrita, está sendo testado nas redes de teste, mas não está em funcionamento na rede principal (mainnet). Lembramos que o Ethereum é a segunda maior rede pública de Blockchain, avaliada em mais de 28 bilhões de dólares e a troca de PoW/Consenso de Nakamoto para Casper PoS é um grande passo.

Outra grande rede de criptoativos que propõe o *Proof of stake* é a Cardano (11º. maior criptoativo em maio de 2019, segundo o índice da Coinmarketcap), que propõe um algoritmo de POS chamado de Ouroboros. De qualquer maneira, esse

algoritmo de consenso foi proposto e precisa ser colocado à prova, o que deve acontecer em breve.

4.6 Outros algoritmos de consenso

Conforme já mencionado em capítulos anteriores, existem outros algoritmos de consenso em estudo ou mesmo em funcionamento. Em redes de *blockchain* permissionadas, cujos nós de validação são conhecidos, outros algoritmos como *Proof of Authority* (POA) são mais indicados. *Blockchains* que utilizam a tecnologia do Hyperledger costumam utilizar algoritmos de consenso baseados no problema dos generais bizantinos, como o *Practical Byzantine Fault Tolerance* (PBFT), embora o Hyperledger permita escolher várias opções de algoritmos de consenso.

Em geral, redes de *blockchain* permissionadas não possuem incentivos para o papel de validação, seja porque o incentivo de manter um nó de validação é intrínseco ao negócio (o membro precisa da rede de *blockchain* funcionando para vender seus produtos ou prestar serviços) ou a rede de *blockchain* não faz parte de um sistema financeiro, como um *blockchain* de rastreamento de alimentos em cadeia logística, ou um sistema de prontuário único de saúde; assim, nesses casos, não há uma “moeda” que mantenha esse sistema funcionando e possa ser usada como recompensa.

REFERÊNCIAS

AUBLIN, Pierre-Louis; MOKHTAR, Sonia Ben; QUÉMA, Vivien. **RBFT: Redundant Byzantine Fault Tolerance.** Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on, pp. 297-306, 2013. Disponível em: <https://pakupaku.me/plaublin/rbft/5000a297.pdf>. Acesso em: 20 jul. 2020.

BACK, Adam. **Hashcash - A Denial of Service Counter-Measure.** 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf>. Acesso em: 20 jul. 2020.

BITMAIN. **Antminer S9i specification.** Disponível em: <https://shop.bitmain.com/promote/antminer_s9i_asic_bitcoin_miner/specification>. Acesso em: 20 jul. 2020.

BITSHARES. **Delegated Proof-of-Stake Consensus.** Disponível em: <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>. Acesso em: 20 jul. 2020.

BUTERIN, Vitalik. **A Proof of Stake Design Philosophy.** 2016. Disponível em: <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>. Acesso em: 20 jul. 2020.

BUTERIN, Vitalik et al. **Proof of Stake FAQ.** 2019. Disponível em: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#so-how-does-this-relate-to-byzantine-fault-tolerance-theory>. Acesso em: 20 jul. 2020.

CANELLIS, David. **Here's why Binance can't erase the $40M hack from Bitcoin's blockchain.** 2019. Disponível em: <https://www.coindesk.com/binance-may-consider-bitcoin-rollback-following-40-million-hack>. Acesso em: 20 jul. 2020.

COINDANCE. **Bitcoin Block Details.** Disponível em: <https://coin.dance/blocks>. Acesso em: 20 jul. 2020.

DWORK, Cynthia; NAOR, Moni. **Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology.** CRYPTO'92: Lecture Notes in Computer Science No. 740. Springer: 139–147, 1993. Disponível em: <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps>. Acesso em: 20 jul. 2020.

EICHMANN, Kerstin. **Machine Economy—a decentralized future that is enabled by autonomous machine-to-Machine transactions!** 2014. Disponível em: <https://medium.com/innogy-innovation-hub/machine-economy-a-decentralized-future-that-is-enabled-by-autonomous-machine-to-machine-e497b90f13c1>. Acesso em: 20 jul. 2020.

GARTNER. **Gartner Says 4.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.** 2017. Disponível em: <https://www.gartner.com/newsroom/id/3598917>. Acesso em 20 jul. 2020.

GHOSH, Debraj. **How the Byzantine General Sacked the Castle: A Look Into Blockchain**. 2016. Disponível em: <https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c>. Acesso em: 20 jul. 2020.

JAKOBSSON, Markus; JUELS, Ari. **Proofs of Work and Bread Pudding Protocols.** Communications and Multimedia Security. Kluwer Academic Publishers: 258–272, 1999.

KRASNIKOV, Denys. **Police find illegal Bitcoin farm at Ukrainian state institute.** 2017. Disponível em: <https://www.kyivpost.com/technology/police-find-illegal-bitcoin-farm-ukrainian-state-institute.html>. Acesso em: 20 jul. 2020.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. **The Byzantine Generals Problem.** ACM Transactions on Programming Languages and Systems, v. 4, n. 3, p. 382–401, 1982.

LEE, Sherman. **Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That.** 2014. Disponível em: <https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#5613fbaa1bc8>. Acesso em: 20 jul. 2020.

LI, Taotao; ABLA, Parhat; WANG, Mingsheng; WEI, Quianwen. **Designing Proof of Transaction Puzzles for Cryptocurrency.** Disponível em: <https://eprint.iacr.org/2017/1242.pdf>. Acesso em: 20 jul. 2020.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2004. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 26 abr. 2019.

NGUYEN, Hugo. **Proof-of-Stake & the Wrong Engineering Mindset.** 2014. Disponível em: <https://medium.com/@hugonguyen/proof-of-stake-the-wrong-engineering-mindset-15e641ab65a2>. Acesso em: 20 jul. 2020.

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

POWER COMPARE. **Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2014.** 2014. Disponível em: <https://powercompare.co.uk/bitcoin-mining-electricity-map/>. Acesso em: 20 jul. 2020.

THE ECONOMIST. **Why bitcoin uses so much energy.** 2014. Disponível em: <https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy>. Acesso em: 20 jul. 2020.

VERMEULEN, Jan. **Bitcoin and Ethereum vs Visa and PayPal – Transactions per second.** 2017. Disponível em: <https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html>. Acesso em: 20 jul. 2020.