Fundamentos em Blockchain

Daniel Duarte Figueiredo

2021

Fundamentos em Blockchain

Daniel Duarte Figueiredo

Sumário

Capítulo 1. Introdução a Blockchain

A tecnologia que chamamos de Blockchain (ou cadeia de blocos, em português) corresponde ao sistema de registro descentralizado que foi introduzido juntamente com o Bitcoin em 2008. Apesar de hoje a tecnologia ir muito além das criptomoedas, para se compreender a Blockchain é interessante inicialmente entender o surgimento e o funcionamento da primeira e principal moeda virtual descentralizada do mundo. Este capítulo tem o objetivo de apresentar o surgimento e a história do Bitcoin, explorando-se o contexto no qual ele surgiu, sua utilização inicial e conceitos básicos.

Contexto de surgimento do Bitcoin

A partir dos anos 1980, em especial no fim da década, iniciaram-se os esforços por parte de pesquisadores na construção de moedas digitais. Isto foi viabilizado porque nesta época a criptografia passou a ser mais acessível e compreendida.

Em 1982, o cientista da computação e criptógrafo David Chaum, considerado o pai das pesquisas na área de privacidade online, criou o conceito de assinaturas cegas, um novo tipo de criptografia que possibilitaria a criação de sistemas de pagamentos não rastreáveis com mais auditabilidade e controle do que os sistemas existentes na época, ao mesmo tempo que aumentava a privacidade.

Figura 1 - David Chaum.

Fonte: https://www.chaum.com.

A partir da tecnologia de assinaturas cegas, Chaum concebeu o eCash, um sistema criptográfico de dinheiro digital que tinha como uma de suas características o anonimato. A equipe de Chaum trabalhou desenvolvendo o eCash durante os anos que se seguiram, e em 1990, David Chaum fundou a empresa DigiCash, que tinha como principal produto o sistema eCash. Os usuários armazenavam dinheiro digital criptograficamente assinados por bancos (utilizando as assinaturas cegas criadas por Chaum) no software do eCash, e podiam trocar por produtos nas lojas que aceitavam a moeda sem ter que informar dados pessoais. A DigiCash conseguiu alguns grandes bancos como cliente, mas o eCash acabou não tendo muita aceitação pelo público geral, levando a empresa a declarar falência em 1998 e David Chaum vender suas patentes. Em 1999 Chaum concedeu uma entrevista à Forbes, em que disse "*Era difícil conseguir comerciantes suficientes para aceitar o eCash, de forma a atrair usuários o bastante para usá-lo, e vice-versa*"1.

Além do eCash, existiram diversas outras moedas digitais e sistemas de dinheiro virtual baseados em criptografia (o que chamamos hoje de criptomoedas) que antecederam o Bitcoin. Muitas delas, assim como o eCash, eram soluções centralizadas gerenciadas por corporações.

Alguns exemplos notáveis:

▪ E-Gold foi criado em 1996 pelo oncologista Douglas Jackson e o advogado Barry Downey, para transferência de posse de ouro digitalmente. Teve rápido crescimento e foi alvo de diversas tentativas de fraudes e de vários golpes, levando o governo dos Estados Unidos a intervir e encerrar as atividades em 2007.

▪ Beenz.com, fundada em 1990 por Charles Cohen. Usuários recebiam a moeda digital beenz em troca de diversas atividades online, como visitar ou realizar compras em determinados websites. Se propunha como uma moeda global que poderia ser trocada por produtos. Encerrou as atividades em 2001.

1 https://www.forbes.com/forbes/1999/1101/6411390a.html#4d65ca86715f

▪ Flooz.com, que surgiu em 1999 como concorrente do beenz e um marketing bem mais agressivo. Levantou cerca de 35 milhões de dólares de investidores.

Foi envolvida em esquemas criminosos e também declarou falência em 2001.

O comércio digital estava em ascensão, mas os consumidores estavam preferindo usar cartões de crédito e o dinheiro digital não emplacou nessa época. Por serem centralizadas, muitas destas soluções acabaram por falência ou sofreram com fraudes, intervenções governamentais e investigações.

Outro importante antecessor do Bitcoin, um dos primeiros a caminhar para o lado da descentralização, foi o B-money, com características parecidas com o Bitcoin, como a utilização de uma função de prova de trabalho (Proof-of-Work), que é um componente essencial do protocolo Bitcoin que será explicado posteriormente. O B-money é referenciado pelo autor do artigo que descreve o funcionamento do Bitcoin.

Em 1998, o famoso criptógrafo Nick Szabo (inventor do termo “smart contracts”) criou o Bit Gold, plataforma monetária descentralizada, apontada como o precursor direto da arquitetura do Bitcoin. O Bit Gold nunca foi implementado de fato, mas sua publicação certamente foi uma das principais inspirações para a criação do Bitcoin.

Figura 2 - Nick Szabo.

Fonte: **https://blockchainlive.com/speakers/nick-szabo/.**

Crise financeira de 2008

Um outro elemento importante no contexto em que surgiu o Bitcoin foi a crise econômica de 2008. A eclosão da crise mundial com a falência do banco Lehman Brothers ocorreu em 15 de setembro de 2008, e o artigo descrevendo o funcionamento do bitcoin foi publicado exatamente 45 dias depois, em 31 de outubro do mesmo ano.

Bitcoin surgiu como alternativa disruptiva ao modelo econômico atual, que é propenso a crises, e isto estava muito claro com a crise que eclodiu. Uma curiosidade interessante é que o autor, Satoshi Nakamoto, inseriu nos dados do primeiro bloco do Bitcoin (chamado de bloco gênese) o seguinte texto codificado: “The Times 03/Jan/2009 Chancel or on brink of second bailout for bank”, que serve como uma prova de que a rede entrou em funcionamento depois desta data e corresponde a uma manchete sobre a crise econômica.

Criação e história do Bitcoin

A história do Bitcoin começa em 2008, quando foi publicado um *whitepaper* (artigo descrevendo o seu funcionamento) por um autor desconhecido, que assinou o artigo usando o pseudônimo de Satoshi Nakamoto. Conforme descrito anteriormente, antes do surgimento do Bitcoin houveram várias tentativas de se criar moedas digitais, além de trabalhos teóricos que

inspirariam a criação da moeda, portanto o Bitcoin foi inovador através da combinação de tecnologias que já existiam.

O Bitcoin consiste em:

▪ Uma rede *peer-to-peer* (par-a-par) totalmente descentralizada.

▪ Um registro público de todo o histórico de transações (a *Blockchain* ou cadeia de blocos).

▪ Emissão de moeda de forma matemática e determinística.

▪ Um sistema descentralizado de verificação de transações.

O título do documento publicado por Satoshi foi “Bitcoin: A Peer-to-Peer Electronic Cash System” (que pode ser traduzido para algo como “Bitcoin: Um sistema Fundamentos em Blockchain – Página 8 de 60

par-a-par de dinheiro eletrônico”). É interessante ressaltar que o termo *cash* em inglês é usado para dinheiro em espécie, que é o conceito que o Bitcoin estava tentando recriar no mundo digital: quem possui bitcoins, a moeda do sistema, pode gastá-los trocando por produtos ou serviços sem precisar se identificar e informar dados pessoais, como é o caso das compras virtuais utilizando-se cartões de crédito.

Em 2009 a rede Bitcoin foi criada usando-se uma implementação baseada no artigo de Satoshi Nakamoto. O software do Bitcoin é de código aberto e é mantido por um grande grupo de voluntários. O funcionamento é baseado em fundamentos matemáticos e criptográficos transparentes e não existem entidades centralizadoras responsáveis por mantê-lo no ar, e sim uma vasta rede distribuída e descentralizada.

Alguns fatos importantes na história do Bitcoin que ocorreram nos primeiros anos após sua criação:

▪ Primeira transação de bitcoins foi de 10 BTC para o programador Hal Finney, autor do RPOW (reusable proof-of-work).

▪ Primeiro registro de compra com bitcoin: 2 pizzas por 10.000 BTC, em 17 de maio de 2010, por Laszlo Hanyecz.

▪ Em 15 de agosto de 2010, uma falha de segurança foi explorada para gerar mais de 184 bilhões de bitcoins indevidamente, porém foi corrigida e o protocolo foi atualizado.

▪ Satoshi Nakamoto se afastou do público em abril de 2011.

Nas seções seguintes, alguns dos conceitos fundamentais para se compreender o funcionamento do Bitcoin e a tecnologia Blockchain são discutidos.

Criptografia

A criptografia é uma tecnologia que existe há milhares de anos, usada para mascarar mensagens ou entradas de diversos tipos. Era usada na antiguidade em formas rudimentares, manuais, e atualmente existem algoritmos muito avançados de criptografia digital.

Uma das possíveis formas de se classificar os tipos de criptografia existentes é diferenciando entre criptografia assimétrica (pública) x e criptografia simétrica (privada)

▪ Assimétricas: pares de chaves – chave pública e chave privada.

▪ Simétricas: as duas pontas devem conhecer a mesma chave.

Desde a invenção da criptografia assimétrica (ou criptografia de chave pública) nos anos 1970s, várias funções matemáticas adequadas foram descobertas, como exponenciação de números primos e multiplicação de curva elíptica (base da criptografia usada no Bitcoin).

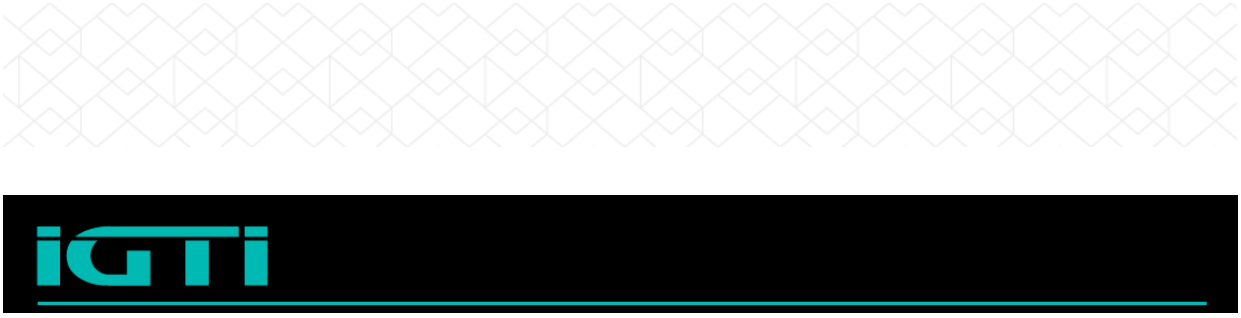
No protocolo do bitcoin, o acesso às moedas é controlado por pares de chaves da criptografia assimétrica, em que a chave pública é usada para receber bitcoins e a chave privada para assinar transações para gastá-los. Uma assinatura gerada com a chave privada pode ser validada sem que a chave seja revelada.

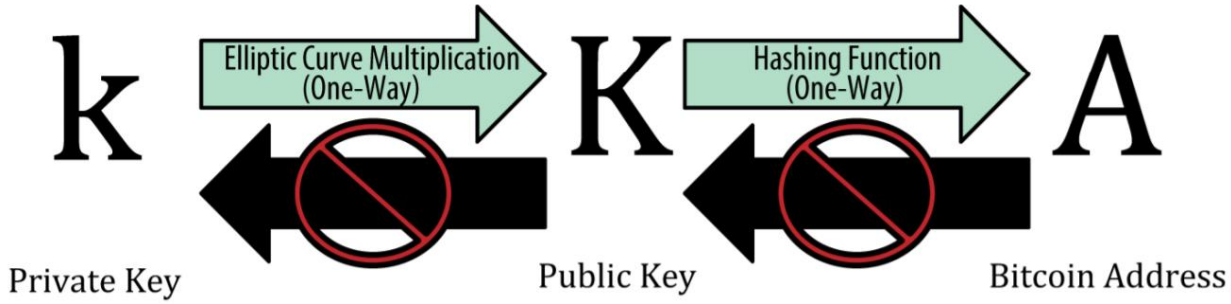
Funções de dispersão criptográfica, ou funções hash, são funções injetivas (de uma via) que são praticamente impossíveis de inverter. Estas funções geram

“impressões digitais” chamadas de hashs, que possuem tamanho fixo a partir de entradas de tamanhos aleatórios. Estas funções são usadas amplamente no protocolo do Bitcoin, como, por exemplo, nos endereços, nos endereços de scripts e no algoritmo de prova de trabalho da mineração.

Propriedades da função hash:

▪ Fácil de encontrar o valor de dispersão (resumo ou hash) a partir da entrada, mas difícil de gerar uma mensagem a partir do hash.





▪ Livres de colisões (entradas distintas não geram a mesma saída).

▪ Entradas de qualquer tamanho geram saídas do mesmo tamanho.

▪ Pequenas modificações na mensagem modificam completamente o hash.

No Bitcoin gera-se uma chave privada k, que consiste em um grande número aleatório, e então computa-se a chave pública correspondente K, usando-se multiplicação de curvas elípticas. Produz-se um endereço bitcoin computando-se o hash SHA256 a partir de K e então o hash RIPEMD160 a partir do resultado.

Figura 3 - Mastering Bitcoin, 2007.

Fonte: Antonopoulos, Andreas M.

Assinaturas Digitais

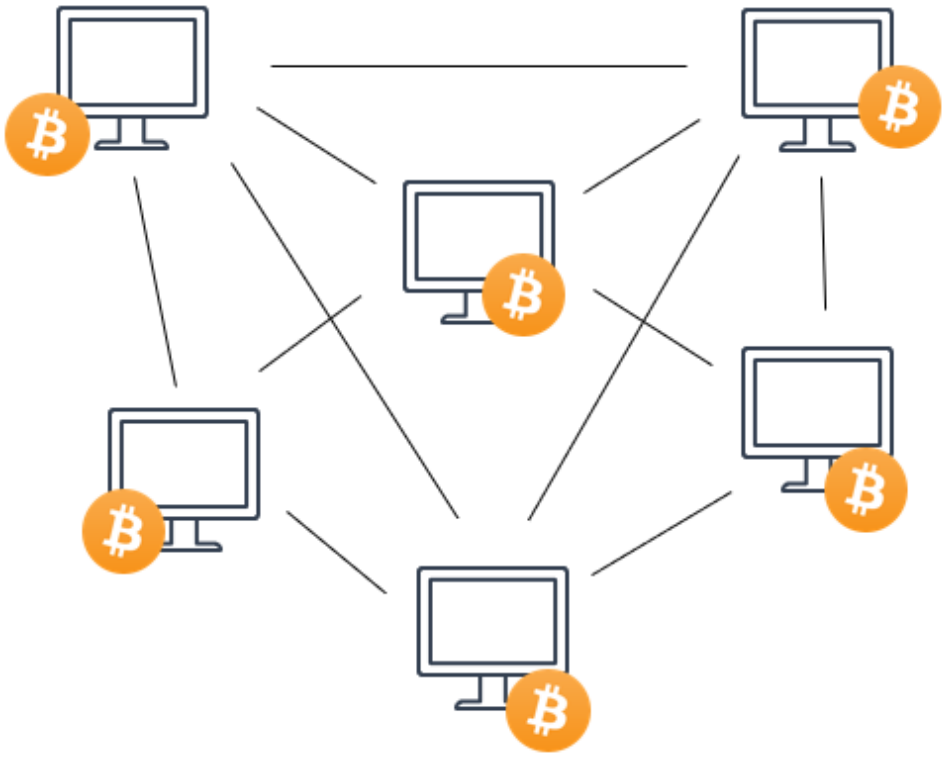
Assinatura digital é um método de autenticação de informação digital baseado em criptografia que substitui a assinatura física.

Propriedades:

▪ **Autenticidade:** qualquer receptor deve conseguir verificar que a assinatura é legítima.

▪ **Integridade:** não é possível “copiar e colar” em outro documento, qualquer alteração no documento invalida a assinatura.

▪ **Irretratabilidade:** o emissor não pode negar a autenticidade.



O funcionamento das assinaturas digitais é baseado na criptografia de chave pública e função hash criptográfica. Assinaturas digitais consistem em:

▪ Um algoritmo de assinatura: dada uma mensagem (documento) e uma chave privada, produz-se uma assinatura.

▪ Um algoritmo de verificação: dada uma mensagem, chave pública e assinatura, é possível validar a autenticidade (sem necessidade de revelar a chave privada que gerou a assinatura).

Rede P2P e Nós

O Bitcoin está estruturado como uma rede *peer-to-peer* sobre a Internet. O

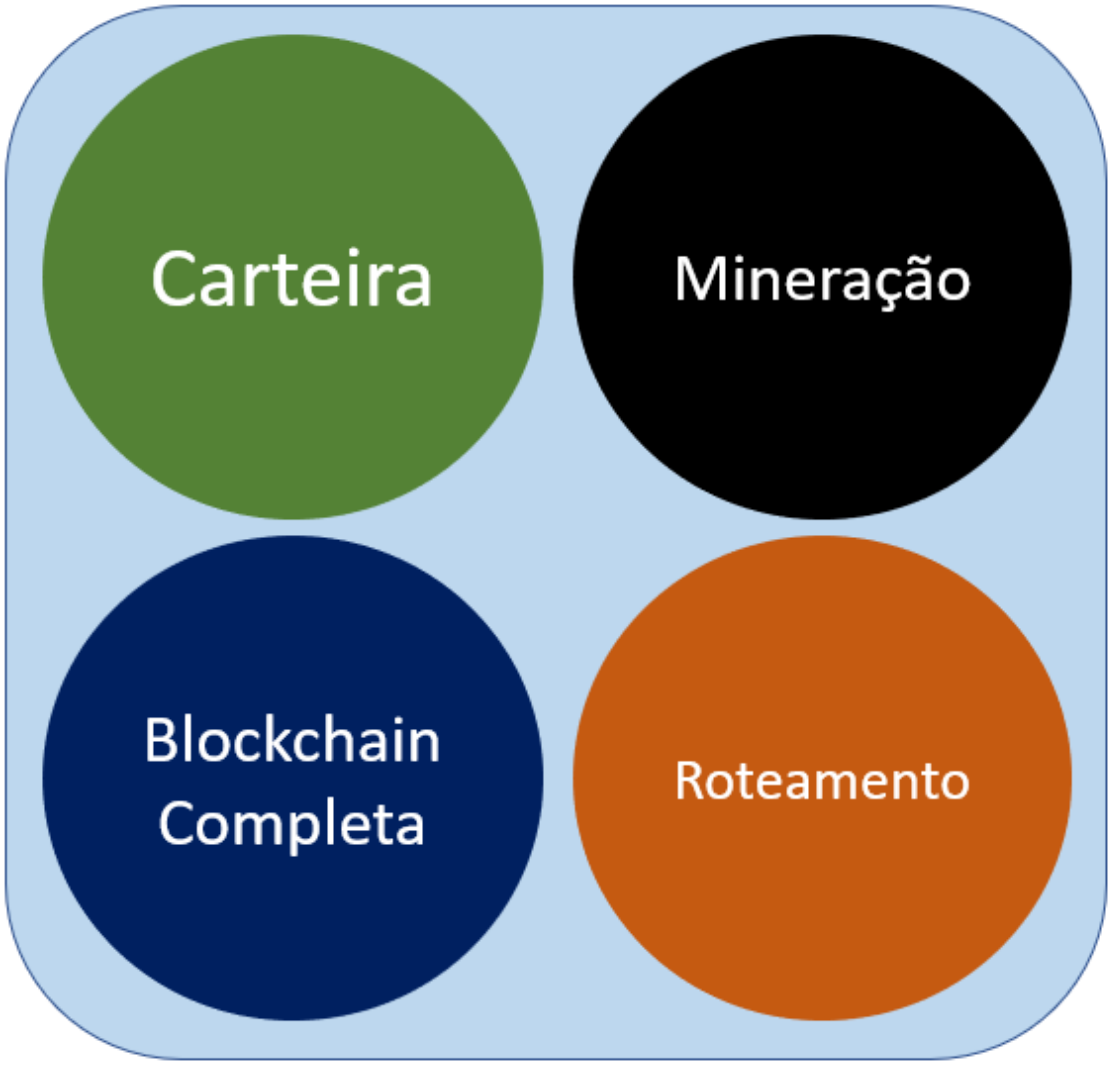
termo *peer-to-peer,* ou P2P, significa que os usuários que participam da rede são pares entre si, não sendo possível haver algum nó “especial”. A tecnologia *peer-to-peer* não foi inventada junto com o Bitcoin e já existia em tecnologias como o Torrent.

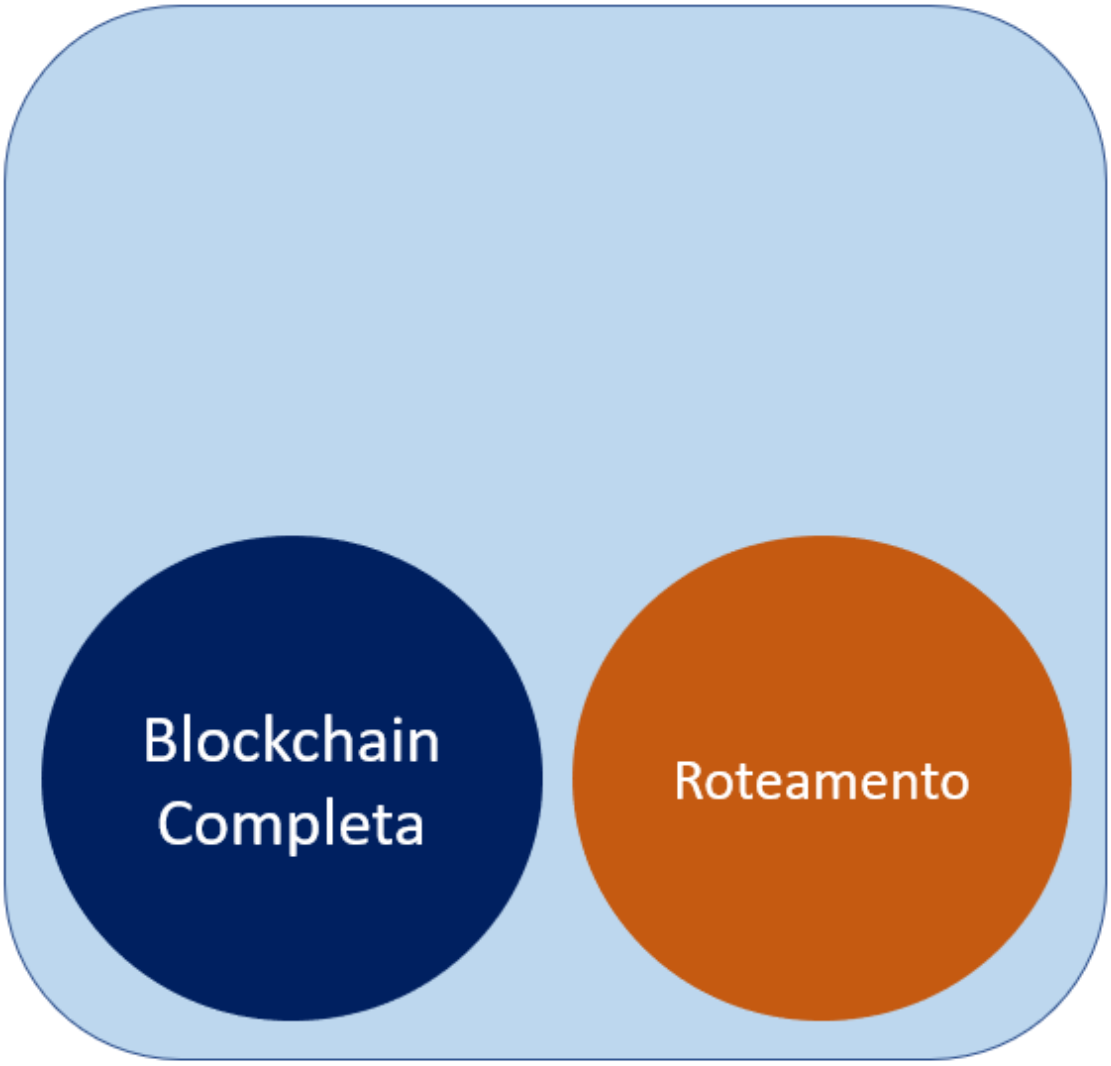
Computadores conectados à rede P2P do Bitcoin são chamados de **nós.** Os nós são essencialmente iguais, não havendo distinção de importância ou priorização, mas podem desempenhar diferentes funções.

Figura 4 - Rede P2P do Bitcoin.

O termo “rede Bitcoin” se refere a todos os nós executando o protocolo P2P.

Além do protocolo P2P, um nó pode executar outras funções, como carteira e


Carteira
Mineração
Blockchain Completa
Roteamento



mineração. Um nó usando o cliente de referência (Bitcoin Core) com todas as funções possíveis está ilustrado na figura 5.

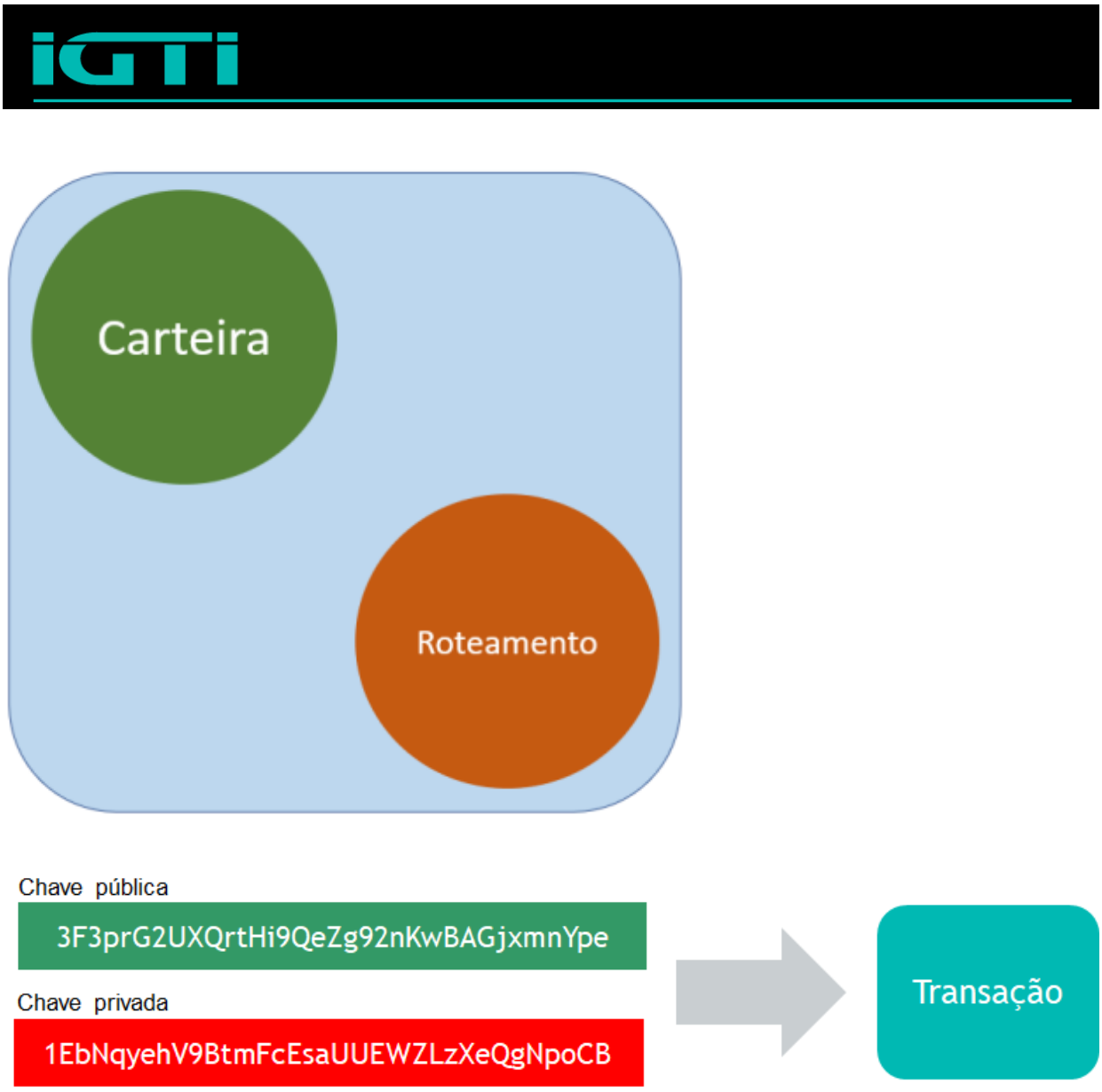
Figura 5 - Nó de referência do Bitcoin Core.

A função de roteamento é necessária para todos os nós participarem da rede.

Um nó é classificado como um nó completo (*full-node*) quando possui localmente uma cópia completa da blockchain (aproximadamente 185 GB em setembro de 2018). Nós completos conseguem validar todas as regras independente dos demais nós. São essenciais para a manutenção da rede descentralizada.

Figura 6 - Nó completo ou Full-node.

Em contrapartida, existem também os chamados nós leve (*lightweight node* s ou SPV – *Simplified Payment Verification*), que são nós que possuem apenas cópia Fundamentos em Blockchain – Página 13 de 60



parcial da Blockchain. Não conseguem validar todas as regras de consenso, somente transações. São muito mais leves que um nó completo e são comumente usados como carteira em diversos dispositivos, inclusive dispositivos móveis, computadores pessoais, entre outros. Para se comunicarem com a rede, precisam se conectar a um nó completo (*full node*).

Figura 7 - Nó leve ou Lightweight-node.

Carteiras

Carteira é um software usado para gerenciar seus endereços bitcoin e suas chaves secretas, usada para enviar, receber e armazenar bitcoins.

Carteira é representada por um endereço ou chave pública correspondente a um conjunto único de caracteres alfanuméricos, que deve ser informado nas transações. As transações devem ser assinadas com a chave privada correspondente, para se provar a posse da carteira ou endereço.

Figura 8 - Esquema de transação de Bitcoins.

Manipular carteiras próprias é muito diferente de deixar bitcoins ou outras criptomoedas em corretoras. A segurança de carteiras envolve um correto armazenamento da chave privada, que deve ser protegida para que outras pessoas não tenham acesso indevido aos seus fundos, mas não pode ser perdida ou esquecida, pois pode significar em perda de todos seus bitcoins, uma vez que não existe um servidor central com o poder de recuperar ou alterar a chave esquecida.

Além disso, é sempre mais seguro executar a carteira em um nó completo da rede. Caso não seja possível, deve-se buscar um *full-node* confiável para se conectar.

Transações

Transações correspondem a transferência de bitcoins de um endereço para outro, feitas através de mensagens assinadas digitalmente enviadas para a rede do Bitcoin. O conteúdo da mensagem expressa uma transferência de valor e a assinatura digital é feita com a chave privada do emissor.

Após gerar uma mensagem correspondente a uma transação válida, em geral com auxílio de uma carteira, o emissor transmite a transação à rede utilizando seu nó completo ou um nó leve conectado a um nó completo.

Transações transmitidas na rede são coletadas por mineradores, incluídas em blocos e gravadas permanentemente na Blockchain.

Condição mínima para que haja uma transação:

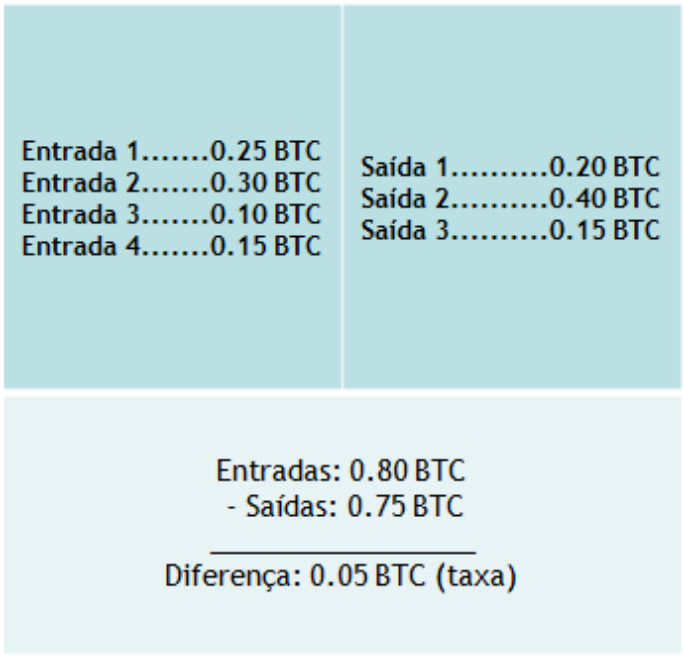
▪ Chave pública do emissor.

▪ Chave privada do emissor para assinar transação.

▪ Chave pública (endereço) de destino.

Em softwares que desempenham função de carteira, o usuário só precisa informar o endereço de destino.

A transação pode ter várias entradas (inputs) e saídas (outputs).



▪ Entradas: débitos em endereços Bitcoin.

▪ Saídas: créditos em endereços Bitcoin.

A soma das saídas é ligeiramente menor que a soma das entradas, sendo que a diferença corresponde às taxas que são pagas aos mineradores. Quanto maior a taxa definida, maior a chance de a transação ser coletada rapidamente (priorizada pelos mineradores), levando a confirmações mais rápidas.

Para cada entrada em uma transação, deve ser comprovada a posse através de assinaturas digitais.

Figura 9 - Entradas, saídas e taxas de uma transação.

Campos em uma transação:

▪ Versão (4 bytes).

- Contador de entradas (1 a 9 bytes).
- Lista de entradas.
- Contador de saídas (1 a 9 bytes).
- Lista de saídas.
- Locktime (4 bytes).

Transações Visualizar informações sobre uma transação bitcoin

67ff1a575d5dc9c214651bcaa1411c2b6f089a3837ef80bbdf46115688bd0090

1FHmv2TdLKLAZV9sWAVKJtELFpvZLxx5gP 1BUbC75HTJrq8KoDnsMejDGUMU6cUkNN7S 1cMRzGuLZtJZXpGxhhXdhDb18bo2UJXYy 17ecvBTLr1DXnnniqLcXwU8iyhiQzHxRrH 1BMrz8kfPsUoEyg48Kw6uVWowF3kzDRDp8	→	1JeYaDbXQbkois7LQcwR6UfVgj6A3tYL1P 1HdQBmZeAzhXrWuChV68SfQPdeCSRAAgJp	1.3756 BTC 3.01626014 BTC

3 Confirmações | 4.39186014 BTC

Resumo	
Tamanho	964 (bytes)
Peso	3856
Hora de Recepção	2018-11-14 10:35:19
Incluída Nos Blocos	550049 (2018-11-14 10:35:32 + 0 minutos)
Confirmações	3
Visualizar	Ver Árvore

Entradas e Saídas	
Total de Entrada	4.391962 BTC
Total de Saída	4.39186014 BTC
Taxas	0.00010186 BTC
Taxa por byte	10.566 sat/B
Taxa por unidade de peso	2.642 sat/WU
Estimativa de BTCs transacionados	3.01626014 BTC
Scripts	Mostrar scripts & coinbase

Figura 10 - Transação real.

Fonte:

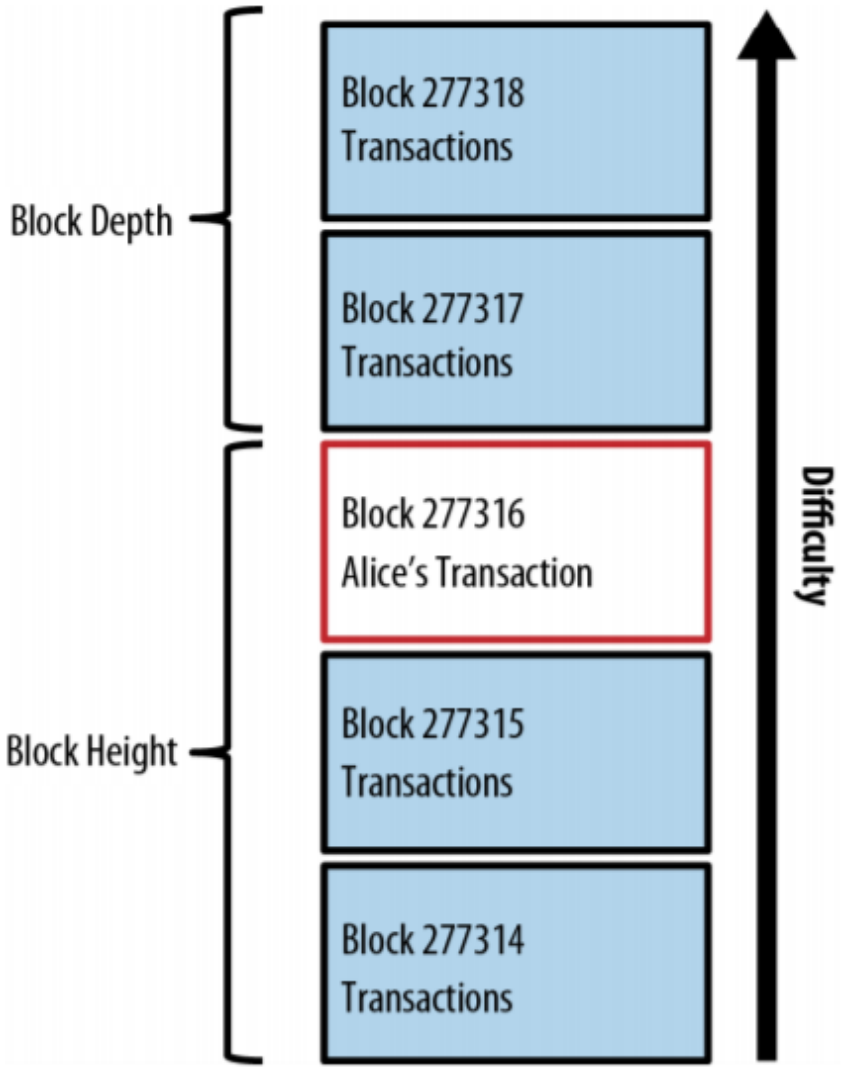
https://blockchain.com/btc/tx/67ff1a575d5dc9c214651bcaa1411c2b6f089a3837ef80bbd

f46115688bd0090

Estrutura de blocos

Os dados das transações de Bitcoins são permanentemente gravados em estruturas chamadas de blocos, que são organizados em uma sequência linear ao longo do tempo, chamada de Blockchain (cadeia de blocos). Novos blocos vão sendo adicionados sempre no fim da cadeia.

Figura 11 - Mastering Bitcoin, 2007.



Fonte: Antonopoulos, Andreas M.

Em geral, a cadeia é visualizada como uma pilha vertical.

▪ O termo *block height,* ou altura do bloco, é usado para a distância de um determinado bloco até o primeiro.

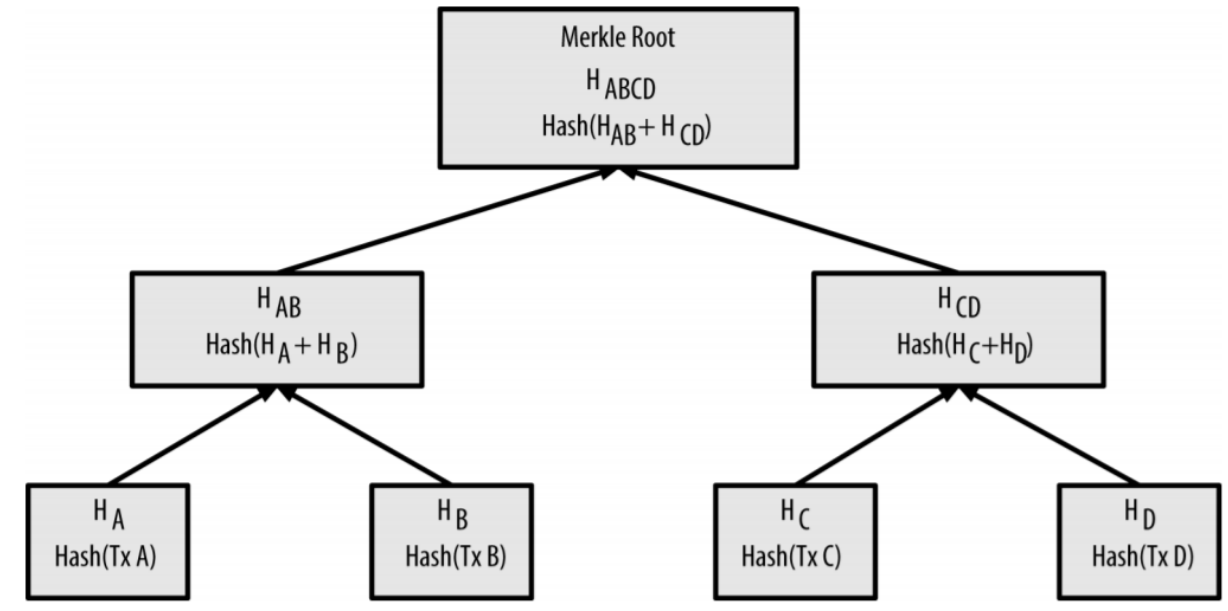
▪ O termo *block depth,* ou profundidade, é usado para se referir a quantos blocos foram adicionados depois de um determinado bloco.

A dificuldade da rede aumenta com o tempo, pois o protocolo se ajusta automaticamente, conforme será explicado na apresentação dos conceitos de consenso e prova de trabalho.

Figura 12 - Estrutura de um bloco.

Fundamentos em Blockchain – Página 18 de 60

Campo	Tamanho	Descrição
Tamanho do bloco	4 bytes	Tamanho do bloco em bytes a partir deste campo
Cabeçalho do bloco	80 bytes	Metadados detalhados a seguir
Contador de transações	1-9 bytes	Nº transações
Transações	variável	As transações do bloco



As transações propagadas na rede são coletadas por mineradores e incluídas em blocos. Os hashs das transações são organizados em estruturas chamadas de árvores de dispersão, ou árvores de Merkle, que funcionam da seguinte

forma: no primeiro nível da árvore são dispostos hashs individuais de cada transação. Do segundo nível em diante, os hashs do nível anterior são concatenados dois a dois, e então computa-se o hash de cada par, conforme ilustrado na figura 13. Esse processo é seguido até o último nível, a raiz de Merkle.

Figura 13 - Árvore de Merkle.

Fonte: Antonopoulos, A. - Mastering Bitcoin, 2007.

Conforme ilustrado na figura 14, o cabeçalho de um bloco possui dois hashs muito importantes:

▪ Hash da raiz de Merkle do próprio bloco.

▪ Hash do cabeçalho do bloco anterior (que por sua vez possui o hash do bloco precedente e sua própria raiz).

Campo	Tamanho	Descrição
Versão	4 bytes	Versão do protocolo (regras que o bloco segue)
Hash do cabeçalho do bloco anterior	32 bytes	Hash criptográfico representando bloco anterior na cadeia
Raiz de Merkle	32 bytes	Hash da raiz da árvore de Merkle das transações do bloco
Timestamp	4 bytes	Data e hora UNIX aproximadas de criação do bloco
Dificuldade Alvo	4 bytes	Dificuldade do algoritmo *Proof-of-Work* para este bloco
Nonce	4 bytes	Contador utilizado como *nonce* no *Proof-of-Work*

Se um dado de alguma transação for alterado, a configuração da árvore é alterada e gera um hash da raiz de Merkle completamente diferente. Se um dado de qualquer bloco na cadeia for alterado, todos os seguintes são impactados, visto que cada um referencia o anterior.

Figura 14 - Cabeçalho do bloco.

Quando uma transação é incluída em um bloco válido da cadeia, é dito que ela possui uma confirmação. Cada bloco adicionado posteriormente é uma confirmação adicional. Por convenção, após seis confirmações a transação é considerada irrevogável, pois o esforço computacional para invalidar e recalcular seis blocos seria absurdo.

A estrutura de blocos descrita é responsável pela imutabilidade dos dados gravados na Blockchain.

Algoritmo de Consenso

Transações de bitcoins são organizadas em blocos, que possuem:

▪ Hash do bloco imediatamente anterior.

▪ Árvore de Merkle, composta pelos hashs de suas transações.

Como cada bloco referência o anterior, eles formam uma cadeia sequencial chamada de Blockchain. Uma vez que a rede é descentralizada, como os nós entram Fundamentos em Blockchain – Página 20 de 60

em consenso em relação à inclusão de um novo bloco? O que impede alguém de alterar um dado no meio da cadeia e recriar todos os blocos seguintes?

A principal inovação do Bitcoin é o mecanismo descentralizado para o consenso emergente. No Bitcoin, não existe uma votação ou momento exato onde o consenso ocorre, por isso é dito que ele **emerge** das interações dos milhares de nós, seguindo regras simples. Todo o modelo de segurança do Bitcoin deriva desta invenção.

O consenso descentralizado emerge de quatro processos independentes, que ocorrem nos nós:

▪ Verificação independente de cada transação pelos nós completos.

▪ Agregação das transações em novos blocos, de forma independente, pelos nós mineradores, junto com a prova-de-trabalho.

▪ Verificação independente dos novos blocos por cada nó e montagem da cadeia.

▪ Escolha independente por cada nó da cadeia, com maior esforço computacional demonstrado através da prova-de-trabalho.

Um breve histórico do algoritmo chamado de **Proof-of-Work** (PoW), ou prova de trabalho, é apresentado a seguir:

▪ 1993: surge em um artigo o conceito de forçar o usuário a provar que realizou alguma tarefa para ter acesso a um serviço, para inibir acessos inúteis. O nome

“proof-of-work” ainda não havia sido usado nesta ocasião.

▪ 1997: publicado o algoritmo chamado Hashcash de Adam Beck, muito semelhante ao *proof-of-work* do bitcoin. Inclusive, este trabalho é posteriormente referenciado no whitepaper do Bitcoin.

▪ 1999: primeira vez que foi usado o termo proof-of-work.

▪ 2004: o programador Hal Finney publica um trabalho chamado de *reusable proof of work* (RPOW), que também serviu de base para o bitcoin.

▪ 2008: proof-of-work é usado para alcançar o consenso descentralizado no Bitcoin.

Uso do proof-of-work no Bitcoin: os blocos possuem cabeçalhos com dados referentes ao bloco anterior, às transações do próprio bloco, e um número

“nonce”. Como uma das propriedades das funções hash (como a SHA256 usada no Bitcoin) garante que é difícil forçar uma saída manipulando-se a entrada, cada vez que o “nonce” do cabeçalho é alterado, o hash computado para o bloco é completamente diferente. Isso ocorre mesmo se os demais dados do bloco permanecerem iguais e o “nonce” for alterado em apenas uma unidade. Para um bloco ser considerado válido, é necessário encontrar um número “nonce” que, combinado aos demais dados do cabeçalho, gera um hash de valor menor que um determinado número (o que na prática implica que o hash deve começar com um determinado número de zeros à esquerda).

O protocolo do Bitcoin foi construído de forma que existe um valor de

“dificuldade” que varia com o tempo para que o tempo necessário para se encontrar um bloco válido seja, na média, 10 minutos.

Na medida que os recursos computacionais foram evoluindo, a dificuldade foi aumentando (ou seja, o número de zeros na frente do hash, que deve ser encontrado para validar um bloco, foi aumentando).

Por causa da forma que a Blockchain é construída, cada vez que um bloco válido é adicionado na cadeia, todos os usuários precisam recomeçar a busca pelo hash válido.

O algoritmo de proof-of-work no Bitcoin é como um desafio matemático gigantesco e competitivo, que reinicia cada vez que um participante encontra uma solução e cuja dificuldade se ajusta automaticamente.

Atualmente, a dificuldade é tão alta que o gasto com energia elétrica é muito alto e só é possível participar do “jogo” com hardware especializado (circuitos integrados específicos para a aplicação - ASIC).

Incentivos e Mineração

Como foi visto, participar da manutenção da rede significa ceder recurso computacional e gastar energia elétrica para solucionar um complexo desafio criptográfico, que é reiniciado cada vez que um participante encontra uma solução.

Considerando-se que atualmente o processo é bastante custoso, qual é o benefício ou incentivo para se participar da rede?

Os nós que encontram um bloco válido realizando a prova de trabalho, recebem dois tipos de recompensa:

- Taxas de transação de todas as transações do bloco.

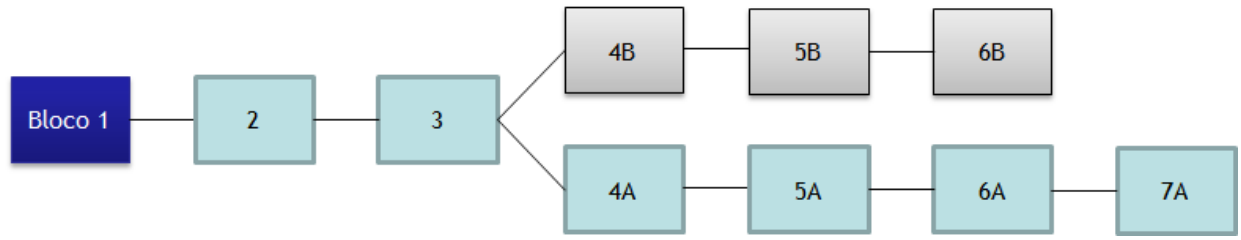
- Novas moedas criadas.

Como a rede é distribuída, dois ou mais nós podem, quase simultaneamente, encontrar blocos válidos diferentes, gerando temporariamente duas versões da cadeia.

Como o próximo bloco possuirá o hash do bloco anterior, os nós tem que escolher qual das versões eles irão estender.

A cadeia que tiver suporte de mais poder computacional vai sempre crescer mais rapidamente.

Figura 15 - Bifurcação na cadeia.



O comportamento honesto é incentivado pelo protocolo do Bitcoin. Os mecanismos de incentivo levam os participantes a entrar em consenso, gerando blocos válidos a cada dez minutos.

A confiança em uma entidade centralizada é substituída pela confiança na força computacional. O custo é sempre superior ao benefício em ações mal-intencionadas. É mais rentável seguir as regras do sistema do que tentar burlá-las.

Nenhuma autoridade central tem o poder de emitir Bitcoins.

O processo de verificar transações, organizá-las em blocos e realizar esforço computacional através da prova de trabalho proporciona uma forma justa de distribuição inicial de moedas.

Satoshi Nakamoto comparou a emissão de novos bitcoins pelo gasto de tempo de CPU e energia elétrica com a atividade de mineradores de ouro gastando seus recursos e tempo para adicionar mais ouro em circulação.

O processo que vimos como um todo, amarrado pelos mecanismos de incentivo, é a chamada mineração de Bitcoin.

Quando um bloco válido é inserido na cadeia, a corrida para encontrar um bloco válido é reiniciada. Cada nó minerador prepara um candidato para um novo bloco e começa a executar as funções hash referentes à prova de trabalho, para encontrar um bloco válido. Os candidatos a bloco possuem transações e propagadas na rede coletadas e verificadas pelo nó, e uma outra transação especial:

▪ A primeira transação em um bloco é de novos Bitcoins recém-criados, com destino ao nó minerador.

▪ Se o nó encontra o bloco antes dos demais, ele é creditado com Bitcoins que não são debitados de ninguém (são novos).

O bitcoin é uma moeda deflacionária: o protocolo se ajusta reduzindo pela metade, a cada aproximadamente 4 anos (ou 210000 blocos), o número de novos bitcoins criados a cada bloco. O limite máximo de moedas é de 21 milhões.

O número de bitcoins em circulação segue uma curva previsível que alcançará 21 milhões no ano de 2140. Não é possível inflacionar o bitcoin

“imprimindo” moedas além da taxa definida pelo protocolo.

Em 2009, quando a rede do Bitcoin entrou em funcionamento, cada novo bloco incluído na rede creditava ao nó que o encontrou 50 novas unidades de Bitcoin (50 BTC).

Este número foi reduzido para 25 BTC após os primeiros 210000 blocos (no final de 2012) e posteriormente para 12.5 BTC, quando chegou no bloco de altura 420000, em 2016, que corresponde à recompensa atual.

Este número será reduzido novamente por volta de 2020 para 6.25 BTC, e assim por diante. O termo mineração é usado pois a recompensa é projetada para simular retornos cada vez menores, assim como na mineração de metais preciosos.

Capítulo 2. Expansão da tecnologia Blockchain além do Bitcoin Após o início do seu funcionamento em 2009, o Bitcoin foi conquistando públicos cada vez maiores e atraindo a atenção de pessoas de áreas distintas. Muitas pessoas começaram a perceber que a tecnologia por trás da moeda digital, a chamada Blockchain, poderia ser empregada de outras formas. Neste capítulo iremos tratar da expansão da tecnologia para além do Bitcoin, abordando o surgimento de outras criptomoedas, plataformas e projetos que utilizam a Blockchain de formas diferentes do Bitcoin.

As primeiras Altcoins

Após o surgimento do Bitcoin e introdução da tecnologia Blockchain, a popularização destes levou a novas aplicações. Os primeiros usos de Blockchain fora do Bitcoin que vamos analisar são as altcoins.

O termo “Altcoins” é em geral usado para qualquer criptomoeda que não seja o Bitcoin. A maioria possui código derivado do código do Bitcoin (forks). Geram uma blockchain separada e diferente da original. Alterações no código original podem focar em escalabilidade, velocidade da transação, tamanho de um bloco, etc.

Figura 16 – As primeiras Altcoins tinham código baseado no Bitcoin
Primeiras Altcoins:

Figura 17 – Namecoin.

▪

Namecoin (abril de 2011):

– Primeiro fork de código do Bitcoin conhecido.

– O termo mais usado para a Namecoin é Alt Chain, pois seu foco não é ser uma moeda como o bitcoin.

– Proposta de substituir o Domain Name Service (DNS) de forma descentralizada.

Figura 18 – IXCoin.

▪

IXCoin (agosto de 2011):

– Também baseada no código do Bitcoin.

– O IXCoin mantém o limite total de 21 milhões de unidades, mas aumenta a recompensa por bloco para se chegar ao limite mais rapidamente.

▪

Tenebrix (setembro de 2011):

– Alterações no algoritmo de Proof-of-Work do Bitcoin.

– Algoritmo de consenso chamado de **scrypt proof of work.**

– Serviu de base para o Litecoin.

Figura 19 – Litecoin.

▪

Litecoin (outubro de 2011):

– Além de implementar o scrypt, reduziu o tempo de geração do bloco drasticamente em relação ao Bitcoin.

– Alcançou boa popularidade devido às transações significativamente mais rápidas.

– Muitas altcoins hoje em dia são derivadas do Litecoin.

Figura 20 – Peercoin.

▪

Peercoin (agosto de 2012):

– Primeira criptomoeda a usar um algoritmo de consenso híbrido entre Proof-of-Work e Proof-of-Stake (prova de participação) para emitir novas moedas.

– Usa mecanismo de mineração baseada em prova de trabalho semelhante ao do Bitcoin, mas também permite que que proprietários de Peercoin gerem mais unidades a partir de um processo mais eficiente em termos de energia gasta, que é baseado na prova de participação.

– Taxa de inflação alvo de 1% ao ano.

Figura 21 – Dogecoin.

▪

Dogecoin (dezembro de 2013):

– Emissão rápida.

– Incentivo ao gasto e circulação.

– Surgiu como uma “piada” e ganhou popularidade em fóruns, usada para

“agradecer” criadores de conteúdo.

– Seu valor de mercado (total obtido multiplicando-se o número de moedas em circulação pelo preço unitário) passou de US$ 1 bilhão em janeiro de 2018.

Figura 22 – Ethereum.

▪

Ethereum (julho de 2015):

– Código **não** é baseado no Bitcoin.

– Máquina de Turing completa: funciona como computador descentralizado.

– Execução de contratos inteligentes na Blockchain.

– Introduz o **ether**, moeda própria usada para pagar execuções de contratos.

– Revolução no uso de tecnologia Blockchain.

A próxima seção é dedicada a uma visão mais detalhada da plataforma do Ethereum, tendo em vista sua importância e diferença significativa para o Bitcoin e para as Altcoins que existiam até então.

Ethereum e Tokens

É uma plataforma em blockchain aberta que permite que qualquer um desenvolva e utilize aplicações decentralizadas com tecnologia Blockchain.

Possui sua própria moeda interna, o Ether (ETH), que é usado para pagar execuções dos seus contratos inteligentes.

É possível se criar operações de qualquer nível de complexidade, diferente do funcionamento do Bitcoin.

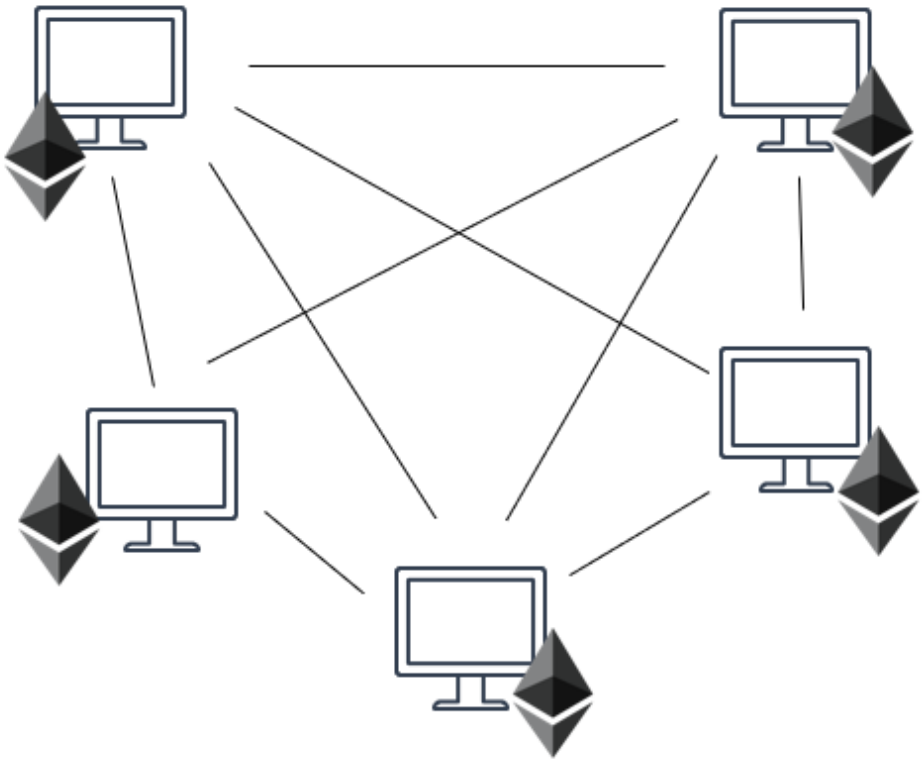
Consegue executar códigos das mais variadas complexidades.

É uma Máquina Turing completa.

Possui linguagens de desenvolvimento simples, baseadas em Javascript (Solidit) e Python (Vyper).

Sendo também uma tecnologia peer-to-peer, cada nó participando da rede roda uma versão da EVM, que executa todas as regras do consenso da rede.

Figura 23 – Rede P2P do Ethereum.



O Bitcoin é uma lista de transações, onde para saber o saldo de um determinado endereço, é calculado o saldo com base nas transações. O Ethereum guarda o estado de cada conta.

Figura 24 – Comparação entre Bitcoin e Ethereum

Existem dois tipos de contas no Ethereum: carteiras e contratos. As carteiras são análogas às carteiras do protocolo Bitcoin estudadas anteriormente: são controladas por chaves privadas e, assim como no Bitcoin, podem realizar operações de transferência (são usadas para enviar, receber e armazenar ether e tokens no Fundamentos em Blockchain – Página 31 de 60

Ethereum). Além destas funcionalidades, no Ethereum as carteiras são responsáveis também para realizar chamadas e contratos.

Os contratos são criados e controlados por carteiras e não possuem chave privada associada. São programáveis para executar lógicas imutáveis a cada transação enviada por carteiras. Não são capazes de operar de forma independente, sendo necessário que uma carteira inicie uma transação para que determinadas funções do contrato sejam executadas.

A possibilidade de programar contratos imutáveis no Ethereum abriu a possibilidade de criar moedas internas com as mais diversas regras, os chamados tokens. Os contratos de tokens armazenam dados como:

▪ O saldo de cada carteira.

▪ Regras de transação do token.

▪ Oferta total de tokens.

▪ Regras de emissão.

A comunidade busca padronizar os códigos de tokens a fim de criar interfaces que sejam facilmente integráveis a:

▪ Corretoras onde os tokens podem ser negociados.

▪ Aplicações descentralizadas (dApps).

▪ Etc.

Esses padrões são formalizados por meio de propostas chamadas de *Ethereum Request for Comments* (ERC).

Exemplos dos principais padrões de tokens no Ethereum:

▪ ERC-20:

– Tokens fungíveis (moedas).

– Transferíveis.

– Possível definir regras de autorização de transferência entre carteiras.

▪ ERC-721:

– Tokens não-fungíveis.

– Podem ser utilizados como colecionáveis, comprovantes de autenticidade (ativos reais) e de várias outras formas.

– Contém métodos de verificação de posse.

– Também são transferíveis.

Forks das cadeias de transações

Quando falamos em Altcoins, falamos de forks do código do Bitcoin dando origem a novas moedas em cadeias separadas.

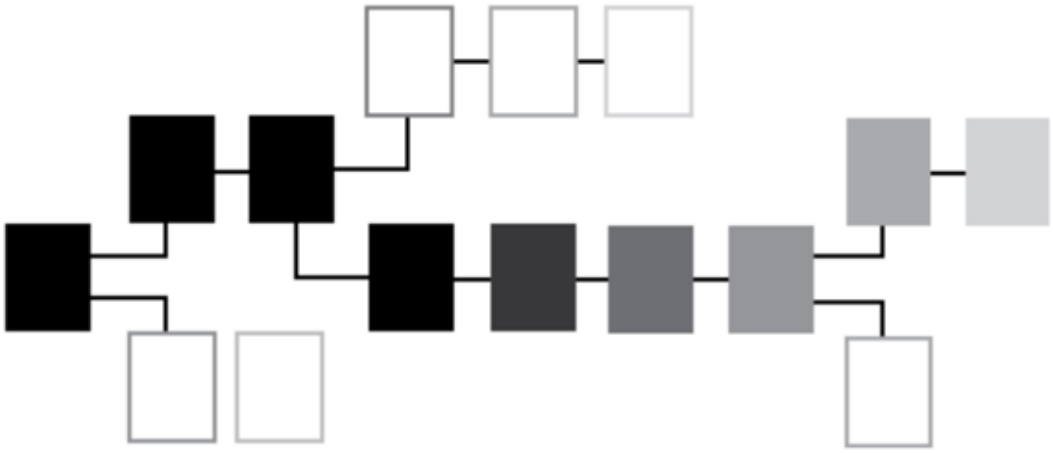
Forks também podem se referir a atualizações no protocolo de uma Blockchain que não necessariamente têm objetivo de gerar uma nova moeda:

▪ O fork surge de uma alteração no código do software da Blockchain em questão.

▪ Os nós completos (full nodes) escolhem entre atualizar sua versão do software ou não.

Se houver unanimidade (ou algo muito próximo), o protocolo é atualizado e segue existindo uma versão principal da cadeia de transações. Se os mineradores se dividirem, pode haver uma divisão da Blockchain, ou chain split.

Figura 25 – Chain splits.



Fonte: **https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-**

fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9

Diferença entre Soft Fork e Hard Fork:

▪ Soft Fork:

– Alteração no protocolo em que blocos que antes seriam válidos passam a ser inválidos. Ex.: redução de tamanho de bloco.

– Nós rodando versão desatualizada aceitam novos blocos.

– Chances reduzidas de causar uma divisão da Blockchain.

▪ Hard Fork:

– Alteração no protocolo em que blocos que antes não eram válidos passam a ser aceitos. Ex.: aumento no tamanho do bloco.

– As novas regras não são compatíveis com as antigas, portanto todos os nós devem atualizar.

– Chances altas de causar uma divisão da Blockchain.

O que define se um hard fork resultará em divisão da rede é a adoção dos nós completos e dos mineradores. Dois cenários (de vários) possíveis são:

▪ Todos os nós e mineradores atualizam para o novo código: a rede se mantém uma só, com o novo código.

▪ Maioria dos nós e mineradores (mas não todos) atualizam para o novo código: A rede é dividida em duas (chain split), causando o surgimento de uma nova moeda no caso de redes como a do Bitcoin e Ethereum.

A plataforma chamada Ethereum Classic surgiu do mais famoso caso de *chain split* por hard fork do Ethereum. Em junho de 2016 foi criado o The DAO, um fundo para financiar aplicações distribuídas na Blockchain que arrecadou cerca de 150 milhões de dólares em ETH. 28 dias depois do seu lançamento, devido a falhas técnicas, o equivalente a cerca de 50 milhões de dólares em ethers foi roubado do fundo por um hacker.

Figura 26 – The DAO.

Para corrigir isso foi feita uma alteração no código do Ethereum que invalidava todos os blocos a partir de um ponto anterior ao roubo (hard fork) invalidando, consequentemente, as transações do ataque.

Como nem toda a comunidade concordava com essa alteração, continuaram existindo nós e mineradores com o código antigo, que foi chamado de Ethereum Classic.

Figura 27 – Ethereum Classic.

No início de novembro de 2018, o Ethereum Classic possui valor de mercado de mais de 780 milhões de dólares, contra 18 bilhões do Ethereum. Um dos principais responsáveis pela sua sobrevivência é o empresário e investidor Barry Silbert, que detém grande poder de influência e é apoiador e investidor declarado do ETC.

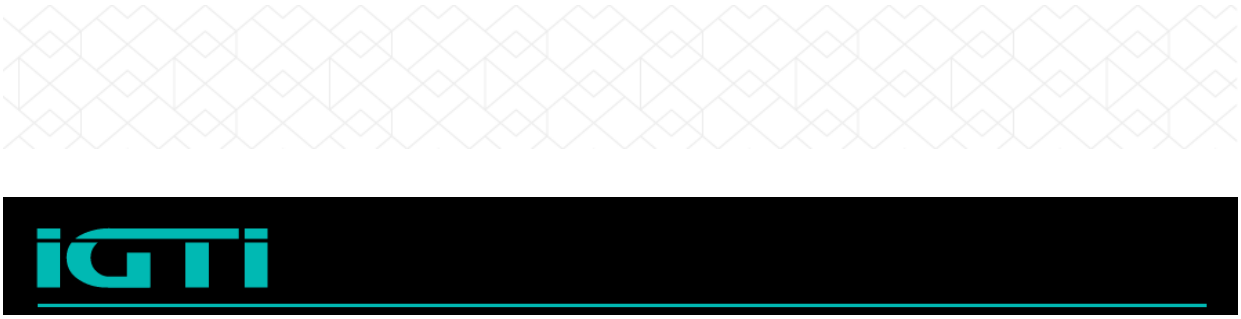
O Bitcoin já passou por alguns hard forks famosos que acarretaram em separação da cadeia de transações e no surgimento de novas criptomoedas.

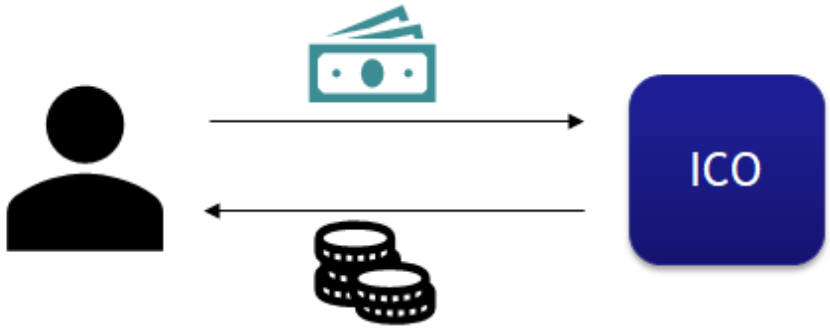
Quando os forks citados abaixo ocorreram, foram geradas novas blockchains e os usuários passaram a ter uma unidade de uma nova moeda para cada 1 BTC que ele possuía na cadeia original.

Figura 28 – Bitcoin Cash.

Bitcoin Cash: primeiro fork que conseguiu poder de mineração suficiente para criar uma segunda rede. Feito em agosto de 2017, o novo código aumentou o limite do tamanho do bloco.

Figura 29 – Bitcoin Gold.





Bitcoin Gold: realizado em 24 de outubro de 2017, o novo código alterou o código de mineração para funcionar com GPU, ao invés de ASIC especializada.

Sofreu um ataque em maio de 2018 devido ao baixo número de mineradores.

Figura 30 – Bitcoin Private.

Bitcoin Private: realizado em 28 de fevereiro de 2018, implementou o zk-SNARKs, uma forma de realizar transações de forma totalmente privada. Também sofreu um ataque devido ao baixo número de mineradores, em outubro de 2018.

ICOs (*Initial Coin Offerings*)

O termo ICO (*initial coin offering*) ou oferta inicial de moeda é análogo a um IPO de bolsa onde investidores adquirem ações de empresas. Apesar da analogia, existem diferenças muito significativas, como questões regulatórias e técnicas.

ICOs são utilizados para se arrecadar fundos através de *crowdsales* ou *crowdfundings*, onde o público interessado investe em um projeto e, em troca, recebe uma quantidade de novas criptomoedas.

Figura 31 – Initial Coin Offerings.

Os processos de *crowdfunding* ou financiamento coletivo não são invenção das criptomoedas e existem desde antes do surgimento da Blockchain. Além disso, vimos que mesmo algumas das moedas digitais que antecederam o

Bitcoin, como o Flooz, passaram por processos de distribuição de moedas em troca de investimentos.

Figura 32 – Mastercoin, o primeiro ICO.

Muitas fontes consideram que o primeiro ICO como conhecemos hoje foi da criptomoeda Mastercoin, em julho de 2013. A proposta do Mastercoin era diferente das altcoins da época: ao invés de criar uma Blockchain nova, ela usava a Blockchain do Bitcoin.

O ICO arrecadou em torno de 5000 BTC, que na época totalizava cerca de $500000 dólares. O Mastercoin mudou de nome e passou por um rebranding total, sendo atualmente conhecido como Omni.

Figura 33 – Omni, novo nome do Mastercoin.

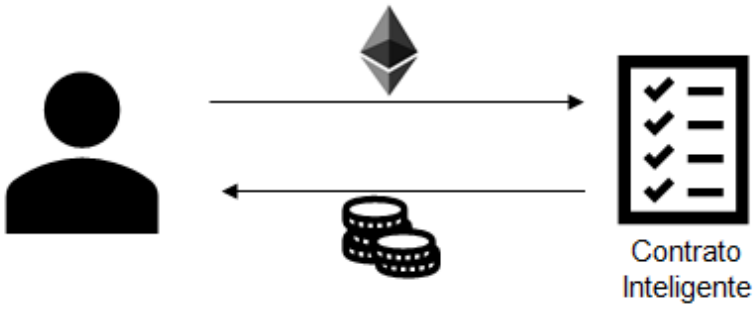
Em abril de 2014, o MaidSafe arrecadou mais de 6 milhões de dólares em um ICO em que foram vendidos tokens de Bitcoin (que posteriormente seriam trocados por Safecoins em uma chain própria).

No ICO havia um bônus para quem comprasse MaidSafe com Mastercoin ao invés de BTC. Após o ICO do MaidSafe, o preço do Mastercoin caiu rapidamente.

Outros grandes ICOs que arrecadaram fundos em BTC foram Lisk e Waves em 2016 (arrecadaram $9 milhões e $16 milhões, respectivamente).

Em julho de 2014 ocorreu um dos ICOs mais importantes da história das criptomoedas: ICO do Ethereum. 1 ETH foi vendido a 0.0005 BTC.

O Ethereum arrecadou mais de 18 milhões de dólares em bitcoins, o maior ICO até então. O panorama de ICOs mudou completamente após a rede do Ethereum entrar em funcionamento.



Ficou muito fácil lançar uma nova criptomoeda: um token baseado no Ethereum ao invés de criar uma nova chain.

O padrão de token ERC-20 tornou simples a programação de um contrato para emissão de novos tokens, que adicionalmente são simples de se incluir em corretoras de criptomoedas.

O próprio processo da venda de tokens (o ICO em si) pode ser feito de forma transparente através de contratos inteligentes no Ethereum.

Figura 34 – ICO na plataforma Ethereum.

Em maio de 2016 um ICO sobre a plataforma do Ethereum arrecadou mais de 150 milhões de dólares (em ETH) de mais de 11 mil investidores: The DAO

(*Decentralized Autonomous Organization*), um sistema puramente de software construído com smart contracts no Ethereum.

A ideia era que esta organização descentralizada serviria para financiar outros projetos, que seriam submetidos a um processo de votação pelos detentores de tokens DAO.

Uma falha de segurança no contrato inteligente do The DAO permitiu que mais de 3.6 milhões de ETH (mais de 50 milhões de dólares na época) fossem indevidamente movidos. Como vimos, levou ao Hard Fork do Ethereum que originou o Ethereum Classic.

Desconsiderando o The DAO, os ICOs em 2016 arrecadaram mais de 102

milhões de dólares. Dentre os tokens de Ethereum (16 ICOs na plataforma em 2016), destacaram-se o ICONOMI (10 milhões) e SingularDTV (7.5 milhões).

Em 2017, mais de 500 ICOs foram bem-sucedidos, totalizando uma arrecadação de mais de 6 bilhões de dólares.

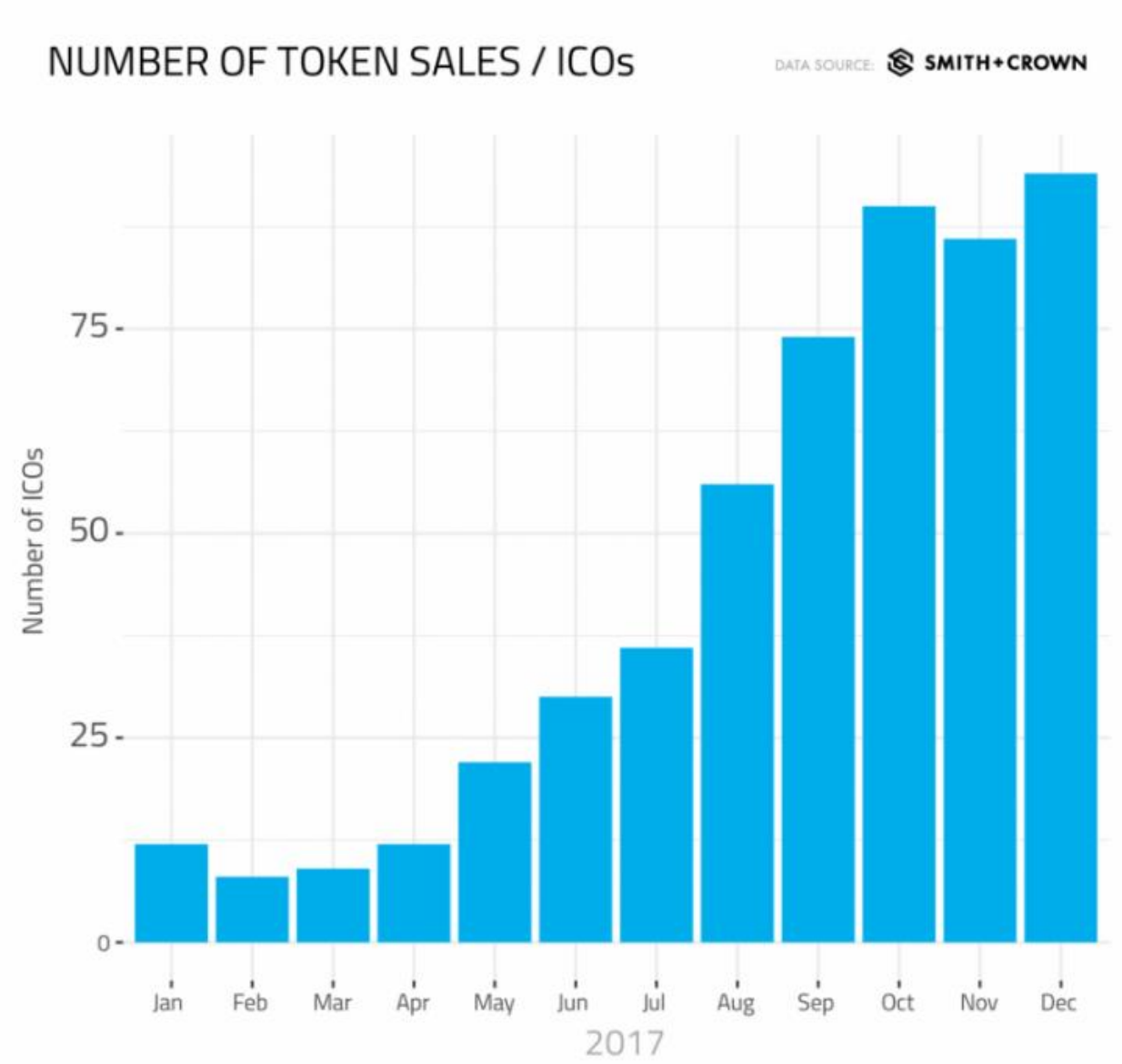
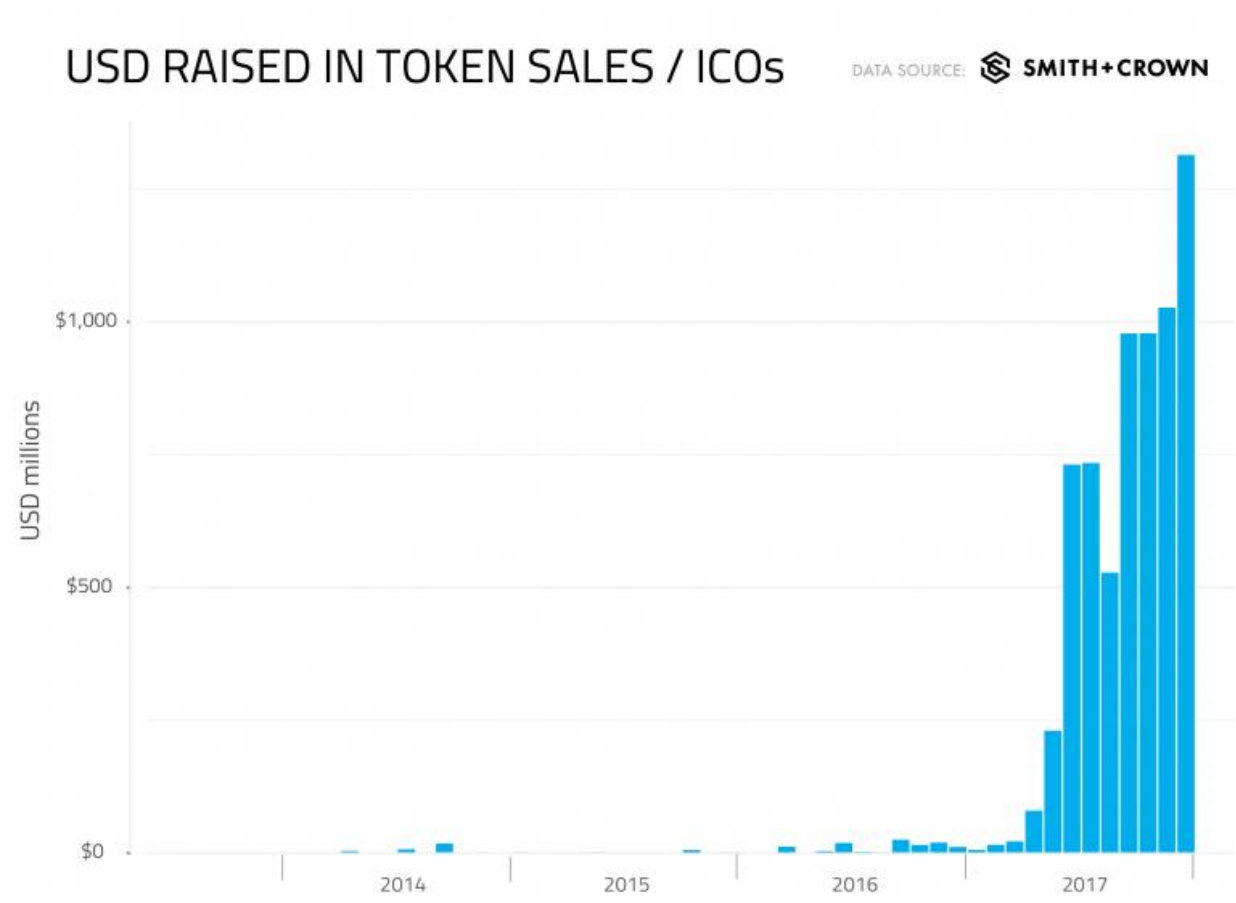


Figura 35 - Evolução dos ICOs em 2017.

Fonte: Smith+Crown.

Figura 36 - 2017 comparado com anos anteriores.



Fonte: Smith+Crown.

Um dos primeiros indícios do novo panorama dos ICOs no ano de 2017 foi o Basic Attention Token (https://basicattentiontoken.org/), em maio, que arrecadou 35

milhões de dólares em cerca de 30 segundos, deixando muitos investidores “de fora”.

O ICO atraiu muita atenção por ter na equipe do projeto o programador Brendan Eich, criador do JavaScript e ex-chefe de escritório na Mozilla Corporation.

Os 20 maiores ICOs de 2017 arrecadaram cerca de 37% do total. Algumas das maiores arrecadações incluem:

▪ Filecoin (mais de 250 milhões de dólares).

▪ Tezos (mais de 230 milhões de dólares).

▪ EOS (mais de 180 milhões de dólares em 2017 e continuou até a metade de 2018).

▪ Bancor (mais de 150 milhões de dólares).

▪ Status (mais de 100 milhões de dólares).

Vale ressaltar que é difícil determinar a quantia exata arrecada por cada ICO

de forma precisa, uma vez que em geral o financiamento é feito através de criptomoedas, principalmente ETH e BTC, que são ativos muito voláteis.

Segundo o site Smith+Crown, no primeiro trimestre de 2018 foram arrecadados 6.7 bilhões de dólares e no segundo trimestre 4.8 bilhões. O EOS, que teve um ICO de um ano, arrecadou quase 3 bilhões nos últimos três meses de seu crowdfunding. A popular plataforma de mensagens instantâneas Telegram também anunciou que faria um ICO e arrecadou $1.7

bilhão em duas rodadas privadas, levando a empresa a desistir de fazer um ICO público.

Com o grande aumento no número de corretoras, o efeito de ganhos exponenciais ao listar novos tokens foi amenizado. Começa-se a falar mais em *security tokens*.

Blockchains Permissionadas

Os exemplos de utilização de Blockchain que vimos até aqui são baseados no modelo do Bitcoin, que corresponde à Blockchain pública:

▪ Protocolo de software aberto;

▪ Rede é descentralizada;

▪ Dados de transações são públicos (qualquer um pode consultar ou auditar);

▪ Qualquer pessoa pode participar:

– Rodar um nó completo;

– Fazer transações;

– Participar do consenso.

▪ Usuários podem permanecer anônimos.

Empresas e indústrias, principalmente, possuem grande interesse em manter um alto nível de confiabilidade em seus dados e agilidade nas operações. Para endereçar essa necessidade foram criados modelos de blockchain permissionada, ou seja, que possui uma camada de autorização de acesso à rede.

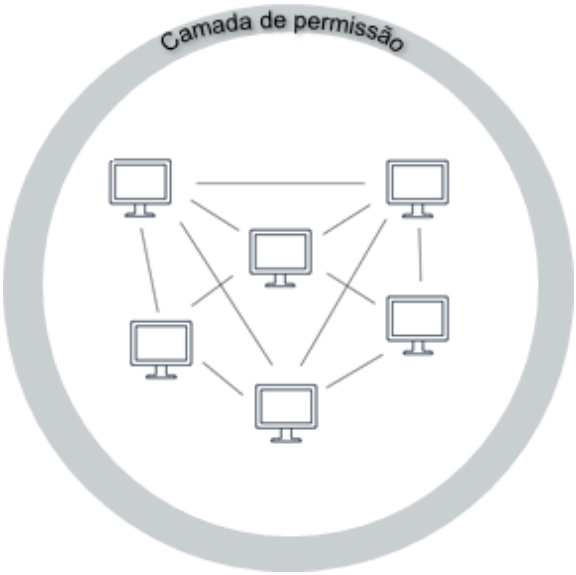


Figura 37 – Blockchains permissionadas.

Os tipos de Blockchains permissionadas podem ser divididos da seguinte forma:

▪ Blockchain privada:

– Acesso controlado por uma entidade central;

– 100% centralizada;

– Autoridade central determina quem pode:

• Ler dados;

• Fazer transações;

• Participar do consenso.

– Apropriada para sandbox, não indicada como aplicação final (ambiente de produção).

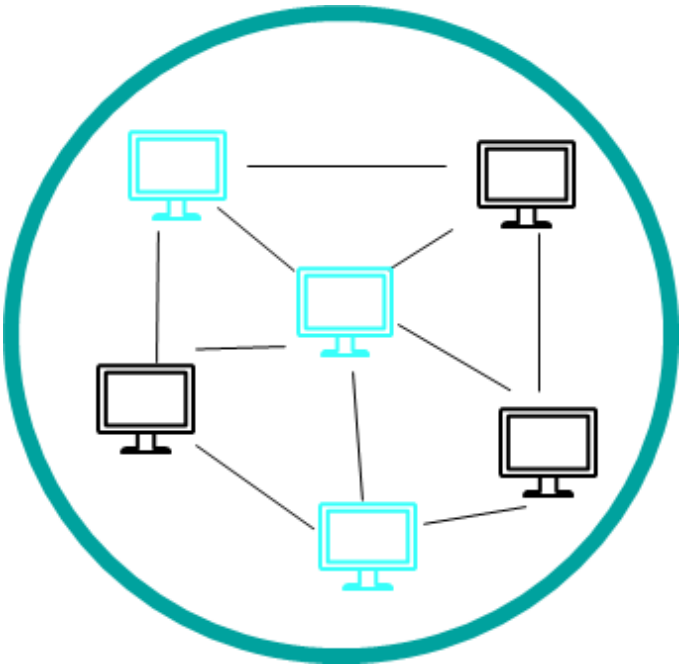
A Blockchain privada traz de volta a autoridade central que o Bitcoin eliminou.

Leitura e escrita são privadas (somente quem for autorizado pode participar).

Essencialmente, é um sistema centralizado tradicional, porém com certa auditabilidade criptográfica acoplada.

▪ Blockchain semiprivada:

– Acesso controlado por uma entidade central;



– Critérios de acesso pré-definidos para qualquer usuário;

– Apropriada para casos de B2B (*business to business*) e aplicações governamentais.

▪ Consórcio Blockchain:

– Parcialmente privada;

– Processo de consenso controlado por um grupo pré-definido (ex: corporações);

– Leitura e escrita podem ser públicos ou restritos;

– Dentre os modelos “com permissão”, em geral é o mais indicado para a maioria das empresas.

Figura 38 - Consórcio Blockchain.

Algumas das principais vantagens que justificam o desenvolvimento e utilização de soluções de Blockchains permissionadas incluem:

▪ Segurança dos dados das empresas;

▪ Transações muito mais rápidas;

▪ Maior grau de escalabilidade;

▪ Rede confiável de participantes;

▪ Menor custo / maior eficiência.

Alguns dos principais casos de uso são:

▪ Cadeia de suprimentos (*supply chain*): possibilita rastrear e verificar a autenticidade de produtos e materiais na cadeia.

▪ Setor público: registro de ativos, propriedades, patentes, processos seguros de votação, registro de documentos.

▪ Serviços públicos: setor energético (venda par a par de energia solar, cobrança automática, etc).

Um dos principais projetos em blockchain permissionada é o Hyperledger Fabric, um projeto da Linux Foundation que foca em desenvolver diversos frameworks e ferramentas *open source* para Blockchain permissionada de forma modular. Várias grandes empresas apoiam o projeto, como Accenture, American Express, IBM, Intel, SAP e Deutsche Bank.

Outra grande iniciativa em Blockchain permissionada é o Corda, desenvolvida pelo grupo R3, que é especializada no setor financeiro. Também possui grandes empresas apoiando, como Oracle, Microsoft, CitiBank e Amazon AWS.

O Bitcoin introduziu a tecnologia Blockchain sendo utilizada para alcançar transparência e descentralização. Com a popularização de ambos, empresas passaram a tentar não ficar de fora do movimento. Para o uso corporativo, industrial e/ou governamental, talvez não faça sentido todos os dados serem públicos e nem deixar que qualquer um escreva no registro de transações, o que fez com que as iniciativas de desenvolvimento de blockchains permissionadas tenham se intensificando nos últimos anos.

Capítulo 3. Aplicações em Blockchain

Como vimos até aqui, a Blockchain surgiu com o Bitcoin e, devido à sua popularização, ganhou outros usos. Muita da atenção recebida pelas criptomoedas está relacionada ao mercado de investimentos e à especulação que existe em torno de seus valores, porém a tecnologia da Blockchain possui aplicações e usos em potencial que vão muito além disso. Neste capítulo iremos ver alguns exemplos de aplicações práticas da tecnologia.

Aplicações baseadas em contratos inteligentes

O termo *smart contract* foi usado pela primeira vez por Nick Szabo (autor do Bit Gold) na década de 1990, antes da invenção da Blockchain.

A ideia básica é que vários tipos de cláusulas de contratos tradicionais podem ser codificados em *hardware* ou *software*, para se adequarem ao mundo digital.

Nick Szabo usou como analogia para explicar o conceito as máquinas de venda automáticas (como máquinas de refrigerante): as regras estão implementadas no dispositivo e não precisa de supervisão humana para funcionar, portanto eram contratos auto executáveis.

A utilização do termo se popularizou com o surgimento do Ethereum em 2014.

Após a associação com a tecnologia Blockchain, o termo “contrato inteligente” passou a não ser mais necessariamente associado aos contratos tradicionais, e sim a qualquer programa de computador na rede descentralizada.

Apesar do termo ter sido adotado no surgimento do Ethereum, o Bitcoin já apresenta uma linguagem de script Turing-completa, que pode ser usada para contratos simples, como contas multi-assinadas e canais de pagamento.

Para explicar o funcionamento de um contrato inteligente simples na plataforma Ethereum, vamos utilizar o exemplo de uma loteria descentralizada.

As regras da loteria são codificadas em um contrato inteligente:

- Valor da aposta.
- Números válidos.
- Limite de tempo para apostas.
- Algoritmo de sorteio.
- Conta(s) que pode executar o sorteio.
- Outras possibilidades: limite de participantes, etc.

Transações que não respeitem as regras falham e não são registradas.

Exemplo:

- Número inválido.
- Valor apostado inválido.
- Sorteio já encerrou.

Somente o fato de se usar contratos inteligentes não garante que a loteria seja justa, mas garante que seja auditável, transparente, imune a fugir das

regras implementadas.

A não ser que exista no contrato uma função para desativá-lo (como uma variável booleana que, se desligada, faz com que todas as apostas falhem, por exemplo) ou um prazo de expiração, a loteria vai continuar existindo na rede funcionando sempre da mesma forma.

Outras aplicações reais de contratos inteligentes no Ethereum incluem empréstimos *peer-to-peer* (exemplo: ETHLend), seguradoras (exemplo: Etherisc),

apostas e mercados de previsões (exemplo: Augur), tokens e ICOs (conforme já discutido), jogos, dentre várias outras possibilidades.

Principais plataformas com suporte a contratos inteligentes: Fundamentos em Blockchain – Página 47 de 60

- Ethereum.
- EOS.
- Stellar.
- Cardano.
- NEO.
- NEM.

Armazenamento descentralizado de dados

Para introduzir o assunto de utilização da tecnologia Blockchain para armazenamento, podemos iniciar analisando alguns casos de uso da própria rede do Bitcoin para fins deste tipo. Alguns exemplos:

▪ O autor Satoshi Nakamoto incluiu uma manchete do jornal The Times de 3

janeiro de 2009, codificada no bloco gênese do Bitcoin.

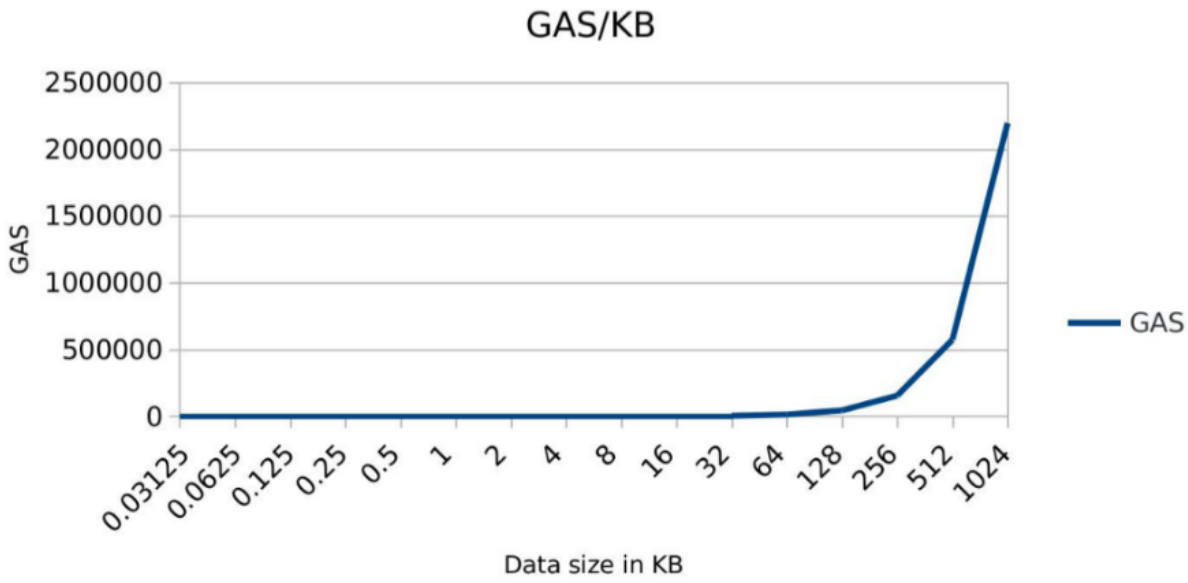
▪ Utilização para armazenar uma “impressão digital” de um documento (por exemplo, um hash do documento) em um dos campos de uma transação.

▪ Proof-of-existence: Serviço que verifica a existência de determinado documento em um dado momento (usando a timestamp da Blockchain).

Uso da Blockchain do Bitcoin para armazenamento é controverso dentro da comunidade. Parte acredita que é um “abuso”, visto que a rede não foi projetada especificamente com este objetivo: causa “inchaço” da Blockchain, penalizando quem roda um nó completo e possui cópia local da cadeia inteira.

Outros encorajam armazenamento de dados diversos, motivados pela demonstração do potencial da tecnologia Blockchain.

Na versão 0.9 do cliente Bitcoin, foi introduzido um campo especificamente para isto (OP_RETURN).



O armazenamento de dados no Ethereum é previsto no projeto da plataforma, e pode ser feito nos próprios *smart contracts*. O usuário paga por isso e o custo aumenta exponencialmente.

Figura 39 - Custo de armazenamento no Ethereum.

Fonte: https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-

costs-922d41d6b316

Existem diversas plataformas que são baseadas em Blockchain, construídas sobre uma Blockchain existente ou inspiradas na tecnologia que possui o propósito específico de se armazenar dados ou arquivos de formas distribuídas.

Alguns exemplos:

- IPFS;
- Filecoin;
- Sai;

▪ MaidSafe;

▪ Storj;

▪ Bluzelle.

dApps – Aplicações descentralizadas

O termo dApp (do inglês *decentralized application*, também escrito como DApp ou Dapp) é usado para se referir a um grupo de aplicações que compartilham algumas características em comum, não sendo um conceito definido formalmente. As aplicações chamadas de dApp em geral apresentam todas ou a maioria das seguintes características:

▪ Código *open source* e gerenciado de forma autônoma.

▪ Dados e registros armazenados em blockchains.

▪ Eliminam ponto único de falha.

▪ Usuários que cedem poder computacional são recompensados.

– Criptomoedas e tokens criptográficos.

▪ Em geral utilizam plataformas como o Ethereum.

Muitos dApps existentes hoje são baseados em sistemas de contratos inteligentes construídos na plataforma Ethereum. Para serem acessíveis pelo público geral, comumente (mas não obrigatoriamente) possuem uma ou mais

camadas de software acima da Blockchain (como um *frontend*). Algumas aplicações são híbridas: não são 100% descentralizadas, pois apesar de utilizarem a Blockchain para registro de transações, as demais camadas são hospedadas em servidores centralizados.

Alguns exemplos de dApps existentes na rede do Ethereum:

• EtherDelta e outras corretoras descentralizadas;

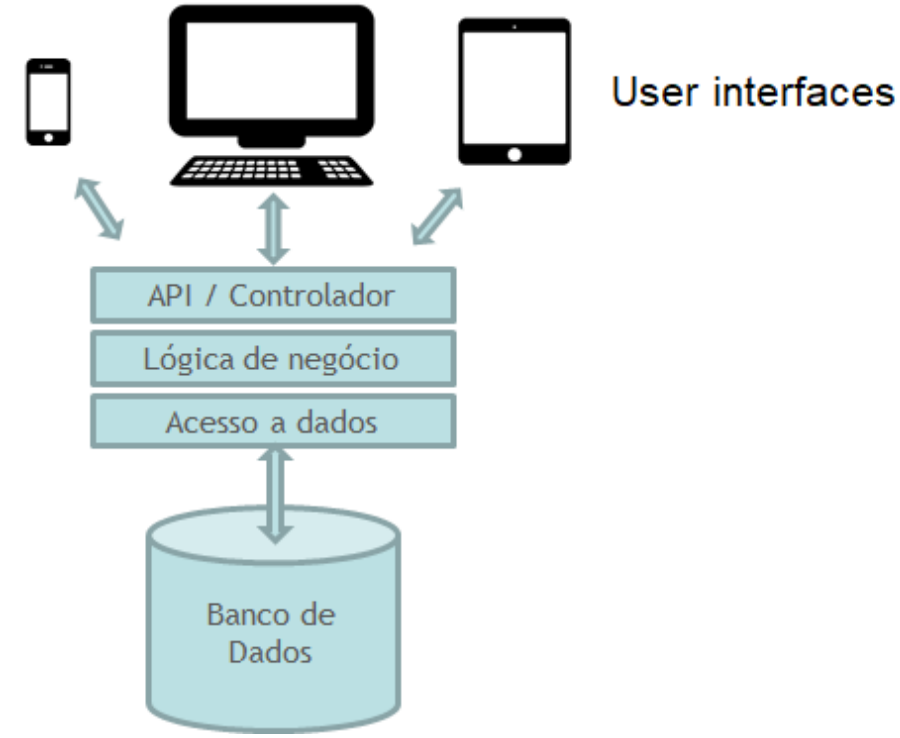
• Maker DAO;

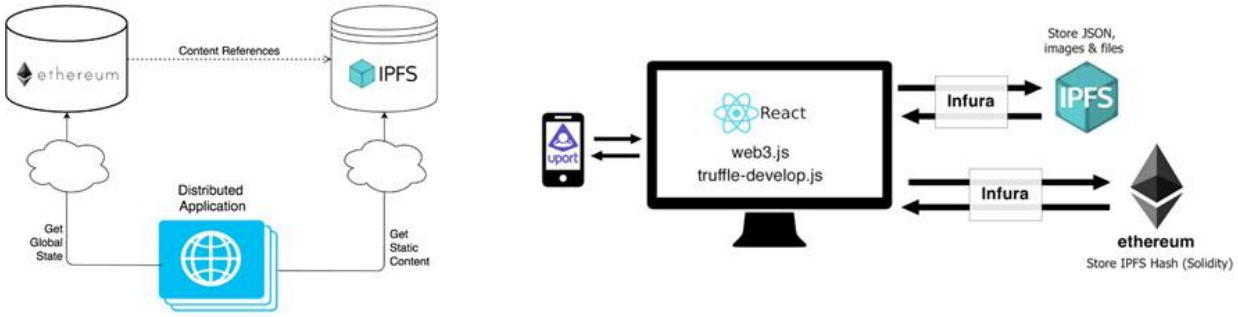
• Augur;

• O clássico The DAO que tinha uma falha que ocasionou na perda de 50

milhões de dólares em ETH e resultou no Hard Fork da rede;

• O jogo CryptoKitties baseado em tokens não-fungíveis.





Conforme pode ser observado nos diagramas de arquitetura simplificados abaixo, as arquiteturas de aplicações descentralizadas são baseadas nas arquiteturas tradicionais, mas ocorre a substituição de componentes tradicionais que são de natureza centralizada por seus correspondentes descentralizados, como o uso do IPFS para arquivos e da própria Blockchain pública para dados, no lugar de um banco relacional tradicional.

Figura 40 - Diagrama de arquitetura em camadas de software tradicional.

Figura 41 - Exemplos de arquiteturas de dApps.

Fontes: https://karl.tech/simple-dapp-architecture/

https://medium.com/coinmonks/a-gentle-intro-to-building-a-full-stack-dapp-

on-ethereum-part-1-c1aedb11fcd2

O potencial das aplicações descentralizadas é enorme, visto que elas são imparáveis uma vez que existem de forma descentralizada, sem um ponto único de falha.

Tokenização de ativos

Um ativo tokenizado é a representação de um ativo real (imóvel, carro, obra de arte e ação de empresa) na forma digital. Com os avanços da criptografia e o surgimento da Blockchain e contratos inteligentes, isto se tornou mais viável.

O maior desafio na tokenização de ativos é garantir que a posse do token criptográfico de fato dê direito à posse do ativo real.

A plataforma do Ethereum e outras plataformas com suporte a smart contracts (Stellar, NEO, EOS, etc.) facilitaram a emissão de tokens para diversas finalidades. A maioria dos tokens mais populares são tokens que funcionam como criptomoedas (transferíveis e fungíveis).

O desenvolvimento de um padrão de tokens não-fungíveis (únicos) no Ethereum foi um passo importante para a tokenização de ativos. O principal padrão deste tipo é o ERC-721, usado em aplicações como o CryptoKitties, um jogo colecionável onde os jogadores podem comprar, vender, colecionar e reproduzir figurinhas digitais de gatinhos.

Figura 42 – Utilização do padrão de tokens ERC-721.

Fonte: https://www.cryptokitties.co/

As vantagens da tokenização incluem:

▪ Acessibilidade global.

▪ Redução de custos e facilitação de transações.

▪ Liquidez.

▪ Fracionamento de ativos.

▪ Fazer uso das vantagens da Blockchain e smart contracts:

– Transparência.

– Regras codificadas imunes a interferência.

– Auditabilidade.

Exemplos de iniciativas de tokenização de ativos reais:

• Edifício de luxo de US$30 milhões em Nova York tokenizado.

• Securitize: emissão de security tokens referentes a valores mobiliários.

• Maecenas: tokenização de obras de artes.

Capítulo 4. Blockchain e o mercado financeiro

Muitas vezes o interesse da mídia e do público geral em relação à Blockchain só é atraído quando o assunto é relacionado aos investimentos e às variações drásticas de preços, não na tecnologia em si. Nosso maior interesse ao estudar Blockchain é compreender o potencial e os diferentes usos da tecnologia, mas o lado de investimentos e a relação com o mercado financeiro tradicional não devem ser ignorados, porque muitas vezes o interesse no investimento impulsiona o desenvolvimento tecnológico. Este capítulo é dedicado a explorar um pouco a história dos investimentos em criptomoedas, os tipos de corretoras e tipos de ativos digitais.

Investimentos em criptomoedas

As primeiras transações de Bitcoin ocorreram entre os próprios desenvolvedores e primeiros mineradores. A moeda não tinha nenhum valor de mercado no início, pois não existe um governo ou banco central controlando seu preço.

Após passado um certo tempo com a rede do Bitcoin em funcionamento, foram surgindo alguns serviços online que aceitavam pagamento em bitcoins, atraídos pela agilidade e privacidade características deste sistema. Um dos primeiros preços registrados foi de 1309.03 BTC por dólar2, na corretora New Liberty Standard (ou cerca de $0.00076 por Bitcoin), que foi um valor baseado em um cálculo do custo energético da mineração na época. Aos poucos começaram a surgir as corretoras especializadas na moeda digital.

Muitas das primeiras corretoras (ou *exchanges*) de bitcoin sofreram com ataques e exploração de falhas de segurança, conforme o resumo a seguir:

2https://web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchang

e+Rate

▪ Março/2010: usuário dwdollar do fórum BitcoinTalk cria a Bitcoin Market, com negociação da moeda por PayPal, de pessoa para pessoa.

▪ Julho/2010: surgimento da Mt.Gox, que se tornaria a maior corretora de Bitcoin no mundo.

▪ Junho/2011: fraudes levam Bitcoin Market a suspender suporte a PayPal.

▪ Junho/2011: primeiro ataque à Mt.Gox, onde o preço foi artificialmente reduzido a $0,01, além de roubo da criptomoeda. O equivalente a quase 9

milhões de dólares foi comprometido.

▪ Julho/2011: o operador da Bitomat é obrigado a vender o serviço para ressarcir aos usuários os cerca de $220.000,00 em Bitcoin que foram roubados em um ataque.

▪ 2012 e 2013: diversos outros ataques e roubos foram relatados, somando perdas de aproximadamente 20 milhões de dólares.

▪ Fevereiro/2014: Mt.Gox, que em 2013 foi responsável por cerca de 70% de todas as transações de bitcoin, declara falência por ter perdido cerca de 390

milhões de dólares em bitcoin, sem uma explicação clara. O CEO foi preso.

Em 2017 o preço do bitcoin foi de menos de mil dólares até próximo de US$20

mil. No auge, o valor de mercado do bitcoin ultrapassou os 300 bilhões de dólares.

Em 2018 o bitcoin passa por uma grande correção, onde o preço caiu no mês de novembro para menos de 5 mil dólares, ou uma queda de aproximadamente 75% em relação ao topo registrado. O valor de mercado (marketcap) em novembro de 2018

oscila em torno de 78 bilhões de dólares, aproximadamente 53% da capitalização total de todas as criptomoedas de acordo com o site CoinMarketCap.

Atualmente mais de 400 corretoras operam com Bitcoin no mundo. As maiores corretoras em volume negociado são Binance, Huobi, Coinbene, Bitfinex e Okex, dentre várias outras. Dentre as corretoras brasileiras, as principais são NegocieCoins, Mercado Bitcoin, FoxBit, BitcoinToYou e Braziliex.

Além de ataques e perdas financeiras, corretoras de criptomoedas também sofrem com restrições regulatórias e governamentais. Em setembro de 2017 o governo da China anuncia o banimento de comércio de criptomoedas do país, forçando suas corretoras a paralisarem suas operações no mesmo mês em que a Coréia do Sul declara banimento aos ICOs no país.

Governos de outros países, como Vietnã, Bangladesh e Bolívia proibiram o Bitcoin ou criptomoedas em geral, e outros países como Rússia e Índia não tem uma regulamentação muito clara e os governos já sinalizaram a intenção de intensificar o controle.

Os problemas com as corretoras tradicionais levam ao aumento da procura por *exchanges* descentralizadas.

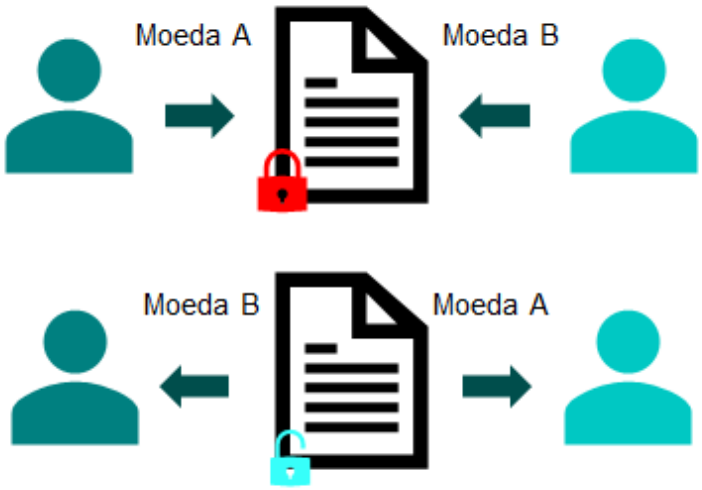
Corretoras descentralizadas

As corretoras descentralizadas surgiram e ganharam popularidade por colocar o investidor no controle de seus próprios fundos, eliminando o ponto único de falha das soluções centralizadas. É uma solução para evitar intervenções de autoridades e minimizar ações de hackers, desde que sejam bem codificadas e sem falhas de segurança no código.

As corretoras descentralizadas não salvam dados das carteiras e transações em um servidor central. Ao invés disso, utiliza da tecnologia dos contratos inteligentes para executar ordens de forma totalmente segura, mantendo o controle da operação nas mãos do usuário.

Cada usuário deposita no contrato inteligente a quantidade a ser trocada, e uma vez que as duas partes completam os as transações, cada uma recebe os valores acordados em sua carteira.

Figura 43 - Funcionamento de corretoras baseadas em contratos inteligentes.



	Corretoras centralizadas	Corretoras descentralizadas
Controle de fundos	Corretora	Usuário
Dificuldade de uso	Fácil	Difícil
Anonimato	Não	Sim
Ponto único de falha (hack ou suspensão)	Sim	Não
Funcionalidades e usabilidade	Avançadas	Básicas
Liquidez	Alta	Baixa

Figura 44 - Comparativo entre tipos de corretoras.

Tipos de ativos digitais

Nem todo ativo digital negociado em corretoras se propõe a ser uma moeda digital, como o Bitcoin. Apesar da característica descentralizada da Blockchain, muitos ativos digitais como criptomoedas e tokens são emitidos por equipes ou empresas registradas sob determinadas jurisdições, que estão sujeitas a regulação local. Além disso, a grande maioria das corretoras centralizadas também pode enfrentar problemas se descumprir restrições regulatórias referentes à comercialização de ativos mobiliários sem licença específica.

Muitas corretoras ou órgãos reguladores exigem que ativos digitais passem pelo chamado Teste de Howey, para verificar que não representam *securities*. Esta Fundamentos em Blockchain – Página 58 de 60

classificação em *securities* e alguns dos outros principais tipos de ativos comumente usados são explicados a seguir:

▪ Moeda: como o Bitcoin, tem o propósito de ser um meio de aquisição de bens e serviços e transferência de valor em geral, contrapondo-se às moedas tradicionais.

▪ Tokens de utilidade (*utility tokens*): são desenhados para concederem acesso a um produto. Regulamentação é mais branda. Muitos dos ICOs em cima do Ethereum emitem tokens deste tipo. O fato de serem *utilities*, na prática, não evitam que sejam sujeitos a especulação.

▪ Tokens de títulos ou ativos reais (*security tokens*): representam ativos “reais”, valores mobiliários ou contratos de investimentos. Excelente caso de uso da Blockchain, mas com muitas barreiras regulatórias.

Fundamentos em Blockchain – Página 59 de 60

Referências

ANTONOPOULOS, Andreas M. *Mastering Bitcoin:* Programming the Open Blockchain. 2. Ed. O'Reilly Media. 2017.

COINMAKERTCAP. *Top 100 Cryptocurrencies by Market Capitalization*. Disponível em: <https://coinmarketcap.com/>. Acesso em: 15 jan. 2021.

HASH FUNCTION. In: *WIKIPÉDIA*, a enciclopédia livre. Flórida: Wikimedia Foundation, 2019. Disponível em: <https://en.wikipedia.org/wiki/Hash_function>.

Acesso em: 15 jan. 2021.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Whitepaper, 2008

ROCHA, Luciano. *eCash:* como a criação de David Chaum deu início ao sonho cypherpunk. Disponível em: <https://www.criptomoedasfacil.com/ecash-como-a-

criacao-de-david-chaum-deu-inicio-ao-sonho-cypherpunk/>. Acesso em: 15 jan.

2021.

ROSSEN, Jake. *Before Bitcoin:* The Rise and Fall of Flooz E-Currency. Disponível em:

<http://mentalfloss.com/article/517911/bitcoin-rise-and-fall-flooz-e-currency>.

Acesso em: 15 jan. 2021.

SWAN, M. *Blockchain: Blueprint for a New Economy*. 1. Ed. O'Reilly Media, 2015.

SZABO, Nick. *Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality*. Disponível em:

<https://bitcoinmagazine.com/articles/smart-

contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/>.

Acesso em: 15 jan. 2021.

TAPSCOTT, Don; TAPSCOTT, Alex . *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 2016.

TERADO, Tom. *What is Decentralized Storage?* . Medium, 2018. Disponível em:

<https://medium.com/bitfwd/what-is-decentralised-storage-ipfs-filecoin-sia-storj-

swarm-5509e476995f>. Acesso em: 15 jan. 2021.

Document Outline

Your gateway to knowledge and culture. Accessible for everyone.