Blockchain

Gabriel Estevam de Oliveira[1]

[1] Departamento de Computação
Universidade Federal de Santa Catarina (UFSC) – Araranguá, SC – Brazil

gabriel.estevam@grad.ufsc.br

Abstract. *The blockchain is a distributed data structures that emerged in 2008 together with a Bitcoin cryptocurrency. As well as Bitcoin, the blockchain is considered, by some authors, like one of the technologies most revolutionary since the Internet. Currently, the blockchain transcended the cryptocurrency branch, and beyond finances applications it is view like able to be used in any application that need safe register datas. With a purely peer-to-peer architecture, it is characterizes like a decentralized technology and fault-point tolerant, it also allows the data immutability, that maybe to be the most relevancy propriety of the yours applications.*

Resumo. *A blockchain é uma estrutura de dados distribuída que surgiu em conjunto com a criptomoeda Bitcoin em 2008. Assim como o Bitcoin, a blockchain é considerada, por alguns autores, como uma das tecnologias mais revolucionárias desde a criação da Internet. Atualmente a blockchain transcendeu o ramo das criptomoedas, e além de aplicações financeiras é vista como capaz de ser utilizada em qualquer aplicação que necessite de registros de dados de forma segura. Com uma arquitetura puramente peer-to-peer, é caracterizada como uma tecnologia descentralizada, sem hierarquia e tolerante a falhas pontuais, além disso permite o imutabilidade dos dados, o que talvez seja a propriedade mais relevante para as aplicações que a utilizam.*

1. Introdução

A tecnologia denominada de Blockchain surgiu pela primeira vez em 2008 no artigo escrito por Satoshi Nakamoto, um pseudônimo para o autor secreto. No artigo o autor apresenta o Bitcoin, uma moeda digital puramente distribuída que permite pagamentos eletrônicos ou transações sem participação de instituição financeira. (Nakamoto, 2008)

A confidencialidade da autoria do artigo que propôs o Bitcoin se tornou um mistério, pois a relevância do trabalho foi logo reconhecido pelas comunidades interessadas em transações *online*, moedas virtuais, criptografia e sistemas distribuídos. Após várias especulações e algumas confissões não comprovadas, ainda hoje não se sabe realmente a verdade por trás do nome.

O mais importante disso tudo é que no mesmo artigo o autor, ou autores, definem o que hoje é chamado de Blockchain. Em resumo a Blockchain é uma estrutura de dados distribuída que permite armazenar dados imutáveis, ou seja, a prova de violações/alterações. No contexto do Bitcoin, permite registrar transações de forma segura e irreversível. (Nakamoto, 2008)

As principais propriedades que caracterizam a estrutura de dados Blockchain são: descentralização do armazenamento e do processamento, compartilhamento dos dados, imutabilidade dos dados, segurança sobre a integridade dos dados e privacidade. Contudo, também suporta aplicações privadas, com necessidade de autorização de acesso e regimentos regulatórios. (Filho, 2018)

Isso é possível pela forma em que a estrutura é construída. A utilização de arquitetura totalmente Peer-to-Peer (P2P) é um dos principais responsáveis, formando uma rede sem hierarquia, descentralizada e tolerante a falhas pontuais. E aliado a isso, baseia-se em encadeamento por hashing e *proof-of-work* (termos que serão definidos mais à frente) para assegurar a imutabilidade dos dados. (Nakamoto, 2008)

Nos próximos capítulos serão definidos alguns conceitos básicos necessários para o entendimento da Blockchain (Capítulo 2), a seguir defini-se propriamente a arquitetura e o funcionamento da Blockchain (Capítulo 3) e por fim algumas das suas possíveis aplicações (Capítulo 4).

2. Conceitos Básicos

Nesta seção serão definidos termos necessários para o entendimento do funcionamento da Blockchain. Entre eles: *hash* e arquitetura de rede *Peer-to-Peer* (P2P). Além desses, Criptografia Assimétrica e Assinatura Digital, que embora não sejam obrigatórios para o desenvolvimento de uma Blockchain, se fazem presente na maioria das aplicações com o objetivo de obter propriedades como segurança e autenticidade.

2.1. Hash

O termo *hash* é definido como conjunto de bits ou uma cadeia de caracteres que de tamanho fixo mapeado por uma função, chamada de *hashing*, a partir de um dados de tamanho variável. (Pfleeger, 2015)

As funções *hasing*, responsáveis pelas gerações dos *hashes*, têm as seguintes propriedades: a probabilidade de entradas distintas gerarem uma mesma saída deve ser a menor possível, quando isso acontece é denominado como colisão; encontrar o dado original a partir de um *hash* gerado deve ser uma operação muito difícil; e, encontrar o *hash* correspondente para uma dada entrada deve ser uma operação de rápida execução. (Pfleeger, 2015)

Um exemplo de uma função *hashing* comumente utilizada em blockchains e criptomoedas é a SHA256. Na Figura 1 pode ser visualizado um *hash* (em hexadecimal) gerado a partir de um texto genérico.

Figura 1. *Hash* gerada em *www.anders.com/blockchain/hash.html*.

2.2. P2P

A arquitetura de peer-to-peer ou ponto-a-ponto é caracterizada por conexões em duplas de hospedeiros, chamados de pares, formando uma rede sem hierarquização. Sendo que os pares não pertencem a provedores de serviços, mas máquinas de usuários comuns da aplicação. (Kurose, 2010)

Corrêa (2017) mostra como a arquitetura ponto-a-ponto é importante para a segurança de aplicações blockchain:

> ... a tecnologia [ponto-a-ponto] provê segurança [para a aplicação] pois há um canal seguro para troca de mensagens. Esta tecnologia é utilizada para conciliar transações, onde na rede do blockchain todos os nós são interligados entre si, após a confecção de um novo bloco toda a rede recebe esta atualização.

Na Figura 2 é possível ver um panôrama de uma rede ponto-a-ponto em uma aplicação blockchain.

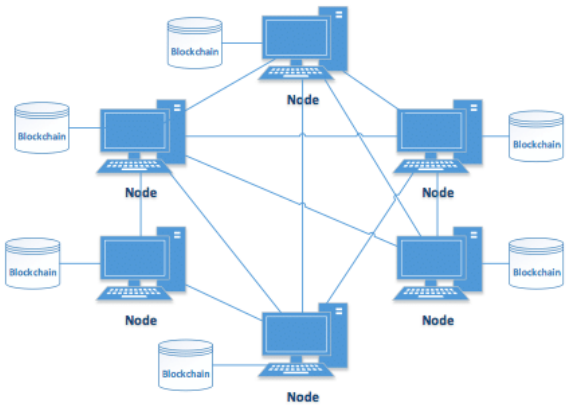

Figura 2. Arquitetura P2P Blockchain.

2.3. Criptografia Assimétrica

A criptografia assimétrica ou criptografia de chave pública é a ferramenta usada atualmente para criptografar mensagens P2P. Constituída de um par de chaves, uma pública na qual todos têm acesso, e uma privada, na qual um usuário tem acesso. Uma dessas chaves pode criptografar a mensagem e a outra descriptografar, ou viceversa. O termo assimétrica vem da ideia de usar duas chaves diferentes para o processo de criptografar e descriptografar o que difere da convencional chave simétrica, na qual a mesma chave criptografa e descriptografa a mensagem. Os algoritmos para gerar as chaves públicas são baseados em problemas matemáticos que atualmente não possui um solução eficiente, como fatoração inteira, logaritmos discretos, Teorema de Euclides para números primos.

2.4. Assinatura Digital

Alguns algoritmos criptográficos de chave-pública podem ser utilizados para gerar o que se denomina de assinaturas digitais. O algoritmo RSA é um desses algoritmos,

assim, além da operação normal de cifrar com a chave-pública e decifrar com a chave-privada, permite que, cifrando-se com a chave-privada, o processo de decifrar com a chave-pública resulte na recuperação da mensagem. (Moreno, 2005)

Portanto, para a aplicação em blockchain, a assinatura digital é a certificação do algoritmo que foi criptografado pela a chave privada, e sua verificação é decifração como a suposta chave pública correspondente. O resultado é válido, se verificando com a chave pública que somente o quem possuía a chave primária o assinou. Por exemplo, Alice manda um documento para Bob, por meio de um canal inseguro, Então Alice cifra-o e envia junto a sua assinatura criptografada, Bob recebe e decifra o documento com a sua chave pública e verifica a assinatura verificando assim que o documento é original.

3. Arquitetura da Blockchain

Inicialmente podemos pensar na blockchain em uma estrutura de dados local, armazenada em um computador, essa estrutura é chamada por algumas aplicações, como a Bitcoin, de ”livro-razão”ou *ledger*. Neste ”livro-razão”estão registrados todas as transações realizadas, documentos, contratos ou qualquer que seja os dados a serem guardados.

3.1. Blocos

Estruturalmente, a blockchain é formada por blocos. Estes blocos possuem alguns campos: identificação do bloco (*Block*), *Nonce* (que será explicado mais a frente), um campo de dados (*Data*), indicador para o bloco anterior (*Previous*) e o um *Hash*.

Na Figura 3 é possível ver um modelo simplificado de um bloco.

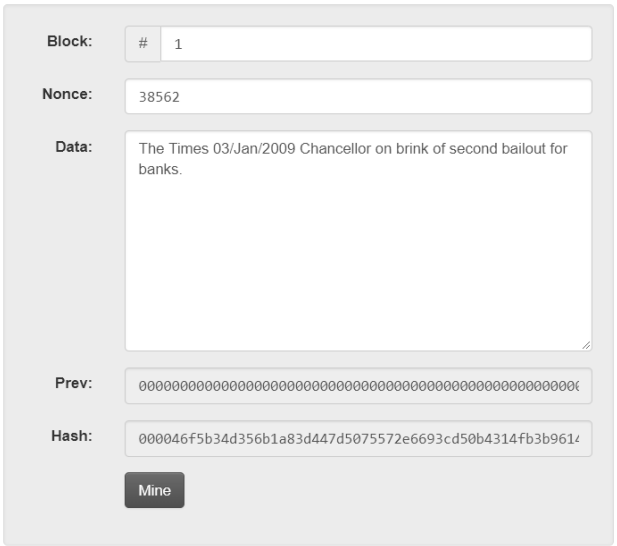

Figura 3. Blockchain *demo* em *www.anders.com/blockchain/hash.html*.

Este é um modelo simplificado, apenas com os itens fundamentais para o funcionamento de uma blockchain. utilizado para o entendimento. Em um aplicação podem ser adicionados outros campos nos blocos.

O *hash* do bloco é encontrado através de uma função de *hashing* como a SHA256 mostrada na seção 2.1. Este *hash* é formada pela junção dos demais campos e identifica unicamente um bloco.

3.2. Cadeia de Blocos

A cadeia ou corrente de blocos é o que dá jus ao nome blockchain. Quando novos conteúdos são inseridos na aplicação, novos blocos podem ser criados e inseridos na cadeia blockchain. Cada aplicação pode ter suas próprias regras de negócio para a inserção de dados na estrutura.

O primeiro bloco da cadeia, também chamado de bloco ”gênesis”, possui o campo *Previous* vazio. Os demais blocos quando inseridos na cadeia preencher o campo *Previous* com o *Hash* do bloco anterior.

Na Figura 4 é possível ver uma cadeia de blocos.

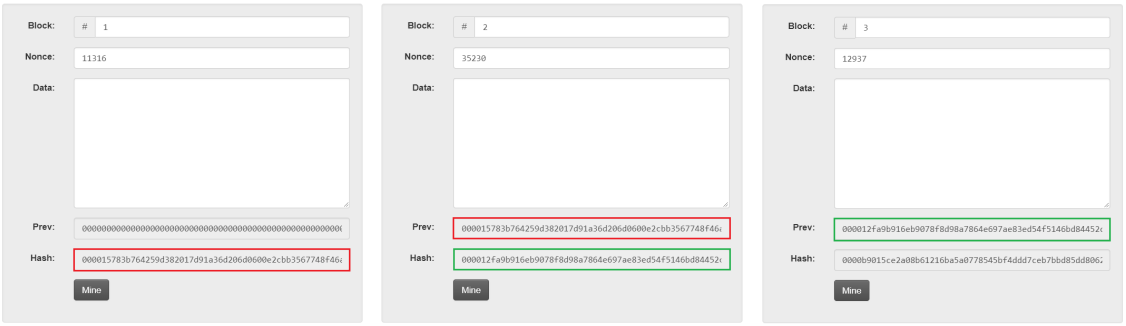

Figura 4. Blockchain *demo* em *www.anders.com/blockchain/hash.html*.

3.3. Distribuíção

Generalizando a blockchain proposta para um modelo distribuído, cada nó da rede *peer-to-peer*, formada pela aplicação, possui uma cópia do ”livro-razão”, a blockchain. Desta forma as características de descentralização, tolerância a falhas individuais e disponibilidade são satisfeitas.

Por definição, aplicação deve estabelecer as regras de negócio para consistência do sistema como um todo. Por exemplo, uma transação pode ser considerada válida se a maioria dos nós concordarem. E além disso, a inserção de novos blocos e transações na blockchain devem ser propagadas para toda a rede.

3.4. Mineração

Para entender o campo *Nonce* é necessário definir Mineração. Minerar um bloco significa encontrar um *Nonce* para o bloco que produza um *hash* com uma sequência de zeros a esquerda (*bits* mais significativo). (Nakamoto, 2008)

No exemplo da Figura 3, o *Nonce* encontrado foi *38562* o qual produziu um *hash* com 4 zeros a esquerda em hexadecimal. Desta forma, diz-se que o bloco foi minerado. O número de zeros a esquerda é um indicativo de quão difícil é minenar o bloco. Dependendo da aplicação pode-se utilizar um número diferente de zeros a esquerda nos *hash* minerados.

Uma técnica de mineração é chamada de prova-de-trabalho ou *proof-of-work* e é executada pelos mineradores. Mineradores são nós da rede (seção 2.2) que guardam cópias da blockchain, executam a mineração e são responsáveis pela inserção de novos registros. (Rodrigues, 2016)

A *proof-of-work* executada pelos mineradores trata-se um tarefa difícil, exigindo bastante poder computacional e consumo de energia elétrica por parte das máquinas que executam o trabalho.

Portanto, é necessário uma motivação para que os mineradores executem suas funções. Assim, uma recompensa é atribuída ao processo de mineração, no caso do Bitcoin o minerador atribui a si mesmo uma quantia de moedas a qual é registrado através de uma transação especial chamada de *coinbase*. Isso não viola a segurança da aplicação pois todas as transações devem ser reconhecidas pelos outros mineradores. (Rodrigues, 2016)

Rodrigues (2016) ainda comenta sobre outra forma de recompensa ao minerador no caso da Bitcoin:

> Outra forma de recompensa é por meio das taxas de transação cobradas pelos mineradores para incluir uma transação em seu bloco. Ela é usada para definir prioridades entre as transações e evitar spam. O autor de uma transação, ao informar o valor total de entrada maior que o valor total de saída, está dando a diferença como taxa para o minerador que incluir aquela transação em seu bloco.

3.5. Imutabilidade

Uma das características mais importantes e relevantes das blockchains é a imutabilidade dos dados, ou seja, não é possível ou é muito improvável que os dados sejam alterados depois de inseridos na blockchain.

Isso se deve ao simples fato de que qualquer modificação nos dados de um bloco altera a sua *hash*. E isso requer que o bloco alterado e todos os blocos seguintes na cadeia sejam minerados novamente.

Segundo Rodrigues (2016):

> O Proof-of-Work também fortalece a segurança da rede, pois para fraudar um bloco é sempre necessário refazer o trabalho de encontrar o nonce e, conforme a blockchain cresce e se espalha pela rede confirmando o consenso, mais difícil a fraude.

4. Aplicações

O blockchain do Bitcoin foi desenvolvido para a validação da moeda digital. Com o aprofundamento das pesquisas sobre a moeda digital, a tecnologia Blockchain foi separada do Bitcoin e foi se incorporando as tecnologias já existentes, como criptografia, topologia de rede e algoritmos de consenso. (Zheng, 2018).

Conforme a popularização das moedas virtuais, o uso de blockchains em outras aplicações tais como na área de entretenimento como o jogo “Beyond the Void” uma *startup* incentivada pela Ubisoft. O Spotify, com uso de bancos de dados descentralizados,

por meio da *startup* blockchain Mediachain Labs, Guts, que é um sistema de bilheteria que objetiva a eliminar fraudes e o mercado negro de ingressos.

A *startup* alemã Slock (*www.slock.it*) oferece um aplicativo usando a plataforma blockchain Ethereum onde a abertura da porta de apartamentos que foram alugados por prazos específicos sejam abertas e fechadas automaticamente de acordo com os dados disponível nos blocos, que possuem a informação do prazo de aluguel do apartamento. No site da empresa Slock, já se pode ver a mesma aplicação desenvolvida para aluguéis de armários e bicicletas.

5. Considerações Finais

Em outubro de 2018 a criptomoeda Bitcoin e tecnologia por trás, a blockchain completam 10 anos desde a proposta inicial. Nesse tempo, surgiu uma grande repercussão com a criação do mercado de criptomoedas alavancados pelo Bitcoin e novas moedas que surgiram como derivações desta, indo em contrapartida aos sistemas monetários dominados pelos bancos tradicionais.

Em destaque neste trabalho a blockchain, uma tecnologia que trancendeu o cenário financeiro das criptomoedas e se mostrou capaz fornecer inúmeras aplicações. Isso se deve as suas propriedades de descentralização com a arquitetura *peer-to-peer* e principalmente a característica de imutabilidade dos dados, decorrente da cadeia de *hashing* e *proof-of-work*.

Das aplicações, além do Bitcoin e criptomoedas, a plataforma Ethereum que com seus *smart contracts* fornece suporte a criação de aplicações como registros civis de bens e documentos, serviços de compartilhamento multimídia e serviços de transparências governamentais e de empresas.

Além disso, a blockchain é uma estrutura ou modelo banco de dados livre para qualquer usuário a sua própria versão voltada uma aplicação específica, usufruindo das características da arquitetura.

Por fim, a blockchain se mostrou como uma tecnologia muito útil e eficaz, despertando interesse de diversas áreas, principalmente o ramo de sistemas distribuídos. Ainda muito jovem mas com grande potencial, a Blockchain promete estar mais presente e difundida nas mais diversas aplicações nos próximos anos.

6. Referências

Lista de referências.

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: www.bitcoin.org/bitcoin.pdf. Acesso em: 2018. out.

[2] Filho J. R. F., Braga A. M, Leal R. L. V. Tecnologia Blockchain: uma visão geral. Disponível em: www.cpqd.com.br. Acesso em: 2018. out.

[3] Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. [S.l.]: Prentice Hall PTR, 2015.

[4] Kurose, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2010. 614 p.

[5] Corrêa O. A. Estudo da Aplicação de Estrutura de Blockchain com *proof of stake* para Arquivamento de Documentos com Registro de Tempo. TCC (Graduação) - Sistemas de Informação. Universidade Federal de Santa Catarina, Florianópolis, 2017.

[6] Rodrigues E. I. Estudo sobre Bitcoin: escalabilidade da blockchain. TCC (Graduação) - Ciências da Computação. Universidade de São Paulo, São Carlos, 2016.

[7] Moreno E. D., Pereira F. D., Chiaramonte R. B. Criptografia em Software e Hardware. Novatec Editora, 2005.

[8] Zheng Z. et al. Blockchain Challenges and Opportunities: A Survey. Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.

[9] Marr. B. 35 exemplos práticos da aplicação de blockchain. Disponível em: https://forbes.uol.com.br/negocios/2018/05/30-exemplos-praticos-da-aplicacao-de-blockchain/. Acesso em: 2018. Nov.