Análise do risco de segurança do sistema Blockchain em uma realidade com computadores quânticos

Bruno Arthur Cesconetto

Orientador: Raul Ikeda Gomes da Silva

INSPER 2018/2019

1. Introdução
    1.1. História
        1.1.1. Contexto econômico
        1.1.2. Fóruns alternativos e Ideias
    1.2. O Bitcoin
    1.3. A Blockchain
        1.3.1. O sistema
        1.3.2. Inalterabilidade
        1.3.3. Coinbase e participação no sistema
        1.3.4. A confiança no sistema e sua auditabilidade
    1.4. O Sistema
        1.4.1. O poder computacional e recompensas
        1.4.2. A criptografia
    1.5. Os problemas
        1.5.1. Problemas no Sistema
        1.5.2. Problemas nas tecnologias
2. Nova Tecnologia
        2.1. Criptografia
        2.2. Supercomputadores
        2.3. Técnicas de Fatoração atuais
        2.4. Funcionamento em computadores quânticos
3. Conclusão
4. Bibliografia

1 INTRODUÇÃO

Nesta sessão abaixo contarei um pouco sobre as bases do bitcoin e como surgiu a ideia de uma blockchain.

1.1.1 CONTEXTO ECONÔMICO

O conceito de blockchain assim como conhecemos hoje surgiu publicamente com a aparição do Bitcoin em meados de 2008 e chegava com a promessa de ser uma nova moeda na qual os governos não pudessem intervir por meio da blockchain por meio de um “torrent de moedas”, em que ninguém tem o controle total do sistema. (Nakamoto, Satoshi. 2008)

A blockchain, a qual dá forças ao Bitcoin vem se desenvolvendo muito nestes últimos anos e é uma das tecnologias que vem para marcar a década, como vem acontecendo nas ultimas décadas, como nos 90 o computador nos anos 2000 a internet e talvez agora a blockchain, em várias áreas como é o caso da econômica. (Vigna, P. 2016)

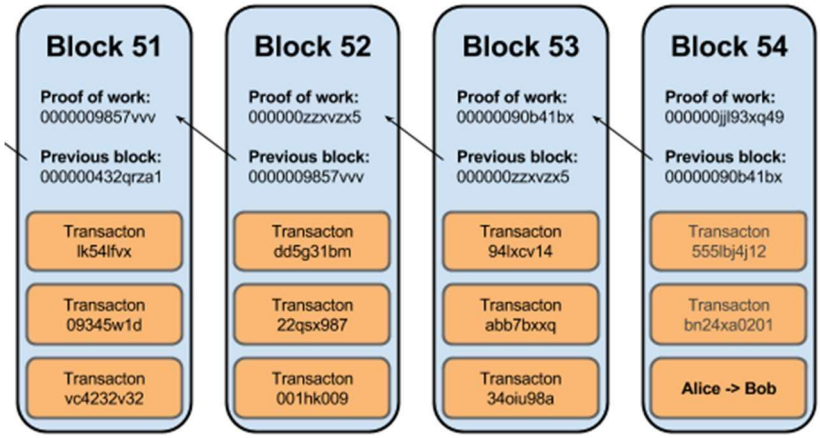
A blockchain, mais especificamente o Bitcoin surgia nessa época, após uma das piores crises econômicas dos últimos tempos, a crise de 2008. Os bancos não eram opções mais tão confiáveis para ficar com o dinheiro e o governo não fazia seu papel para que o dinheiro físico tivesse seu valor garantido.

1.1.2 IDEIAS E FORUMS ALTERNATIVOS

Foi então que em um fórum de discussões de tecnologia alternativas, aparece alguém com pseudônimo de Satoshi Nakamoto, um cypherpunk, que estudava criptografia, tinha ideias anarquistas e decidiu dar um novo propósito para o sistema do HashCash, um que livrasse as pessoas de seus governos. (Back, Adam. 2002)

Surge então um de uma moeda que resolveria todos os problemas causado pelos bancos e governos, que não dependeria de ninguém para ter credibilidade, nenhum banco ou governo, a qual se chamaria Bitcoin. E que seria possível devido a uma tecnologia chamada Blockchain, a qual se baseava nas tecnologias do HashCash e de um Sequential database como mostrado na Figura 1. (Nakamoto, Satoshi. 2008)

Figura 1: Sistema de database sequencial com o sistema do hashcash



https://www.ybrikman.com/assets/img/blog/bitcoin/bitcoinblock-chain-verified.png

1.2 O BITCOIN

O bitcoin não é apenas uma tecnologia só, e baseada em diversas outras tecnologias, as quais já existiam anteriormente ao Bitcoin, como é o caso de um sistema que permitia que se usa o tempo de processamento como uma moeda de troca, uma criptografia assimétrica para autenticação, e uma tecnologia de informações sequenciais imutáveis, que formam o Blockchain.

1.3 A BLOCKCHAIN

Este sistema que faz parte do bitcoin, é um sistema de armazenamento de dados, que é distribuído, baseado no sistema de conexões P2P (Peer-to-peer), que já é usado há muitos anos em tecnologias tipo o “torrent”(Figura 2b), também não contam com uma unidade central que detenha todo o poder sobre o sistema, sendo feita individualmente por usuário “ativo” no sistema, inclui em diversas partes do seu código um sistema de criptografia para assegurar a segurança do sistema como um todo, como uma maneira de impedir mudanças indesejadas, ou a alteração de dados.

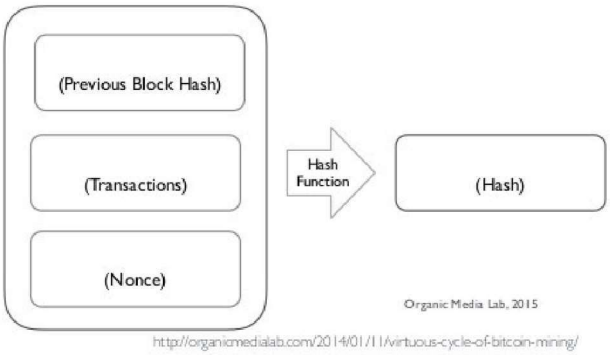
Figura 2a: Exemplo de uma rede peer-to-peer

Figura 2b: Exemplo de uma rede baseada em cliente-server

1.3.1 O SISTEMA

O sistema além de usar a criptografia para que os dados sejam inalteráveis por si só conta com um sistema de trabalho computacional em que é necessário que se gaste energia, mais especificamente poder de processamento para que uma informação seja efetivada no sistema, baseado na tecnologia do hashcash, este conceito é chamado de prova de trabalho “proof of work”, no qual muitos computadores trabalham gerando “assinaturas” [hashes] das informações mudando um número da sorte (Figura 3) para chegar a uma assinatura especial e conseguir efetivar suas informações.

Figura 3: Estrutura de um bloco minerado contendo o número da sorte (nounce)



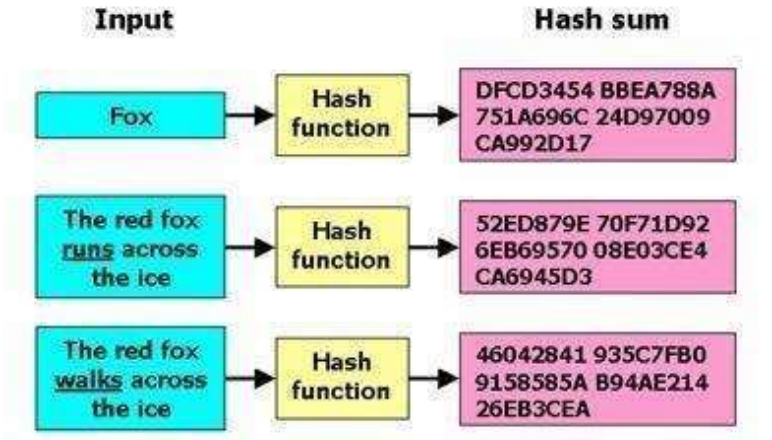
https://organicmedialab.com/2014/01/11/virtuous-cycleof-bitcoin-mining/

1.3.2 INALTERABILIDADE

A confiabilidade das informações, diferentemente dos bancos de dados atuais com redundância e múltiplos datacenters, que se baseia em uma empresa a qual garante que as informações não sejam alteradas por terceiros, é baseada no fato que informações guardadas na blockchain tem dois mecanismos de proteção contra mudanças, o tempo e a criptografia, no qual as informações do bloco, que é um conjunto de informações a serem colocados na blockchain, tem uma fingerprint que se chama hash.

Esse hash é referenciado no bloco de informações subsequente montando uma cadeia cronológica de informações. O hash é como uma cadeia de caracteres com tamanho fixo, que provém de uma mensagem com um tamanho qualquer, podendo acarretar uma possível sobreposição de dois fingerprints para mensagens diferentes.

Figura 4: Exemplo de um algoritmo de hash qualquer



https://www.sqa.org.uk/e-learning/WebTech04CD/images/ pic002.jpg

1.3.3 COINBASE E PARTICIPAÇÃO NO SISTEMA

Para que essas informações tenham algum valor na blockchain, os mineradores que são usuários da blockchain que possuem um no da rede, os quais recebem as informações da rede.

Esses usuários específicos fazem um papel importante na rede, tentando reunir essas informações em um conjunto chamado de bloco, o qual precisa estar em uma sequência especifica, a qual se baseia em regras do tempo, e das informações.

Para gerar esses blocos os mineradores devem mudar as informações, que estão contida no bloco, mais especificamente o nonce, um número manipulável para conseguir gerar uma identidade do bloco compatível com as regras do tempo da mineração.

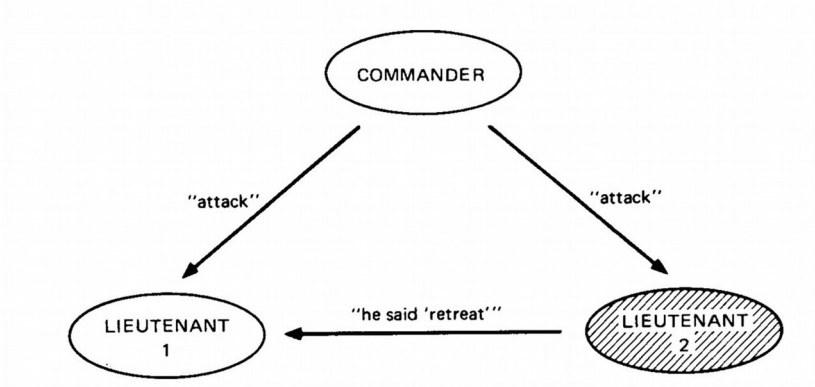
E pra isso os computadores mineradores vão testando muitos números diferentes, para chegar no resultado desejado, que neste caso é um número com uma quantidade de zeros maior em sua assinatura, para isso os computadores gastam poder computacional e tempo para gerar uma assinatura hash digital. Que é um número que equivale a um certo texto, garantido que está colocando esforço computacional para gerar aquele bloco, o que dificulta com que alguém gere um novo bloco mudando a cadeia a fim de inserir informações falsas.

1.3.4 CONFIANÇA NO SISTEMA E SUA AUDITABILIDADE

Um dos problemas que qualquer sistema social-econômico sempre enfrentou foi a falta de confiança em suas partes e o fato que algum dos participantes poderia mentir, como é o caso do antigo problema dos generais bizantinos. (Erkens, D, 2012)

Neste problema, havia 5 generais contra uma vila, mas eles só conseguiriam vencer a vila caso atacassem ao mesmo tempo, e isso ocorreria se todos falassem a verdade, o que nem sempre acontece como demonstrado na Figura 5. (Lamport, L, 1982)

Figura 5: Exemplo do problema dos genreais bizantinos na qual um dos integrantes do sistema está mentindo



https://blog.cdemi.io/content/images/2017/06/TheTraitorousMessenger.png

Com este problema em mente e a crise de 2008, o sistema Bitcoin procurou uma maneira para resolver esses problemas, ao contrário do sistema bancário que possui uma entidade central que controla as transações, e tem o poder sobre as informações, e consequentemente o poder.

1.4 O SISTEMA

O sistema da blockchain tem sua principal tecnologia a ideia de descentralização para que seja possível se livrar de unidades centrais não tão confiáveis e enviesados, ou seja, um sistema com poder

concentrado, e para isso é utilizada uma tecnologia de rede descentralizada, a qual é usada nos sistemas de Peer-to-peer (P2P).

Outra tecnologia, mais especificamente na criptografia, está presente na Blockchain, para garantir que a informação contida no sistema está de acordo com o usuário que colocou a informação, utilizando do sistema de criptografia assimétrica e assinaturas digitais e que está de acordo com toda a rede, ou, pelo menos, a maioria, pelo sistema de hashes e da cadeia de dados.

1.4.1 O PODER COMPUTACIONAL E AS RECOMPENSAS

Porém ainda temos o problema dos integrantes do sistema maliciosos, e com isso chegamos ao algoritmo de consenso da blockchain, o PoW que foi introduzido pelo HashCash, e é mais utilizado atualmente, na blockchain.

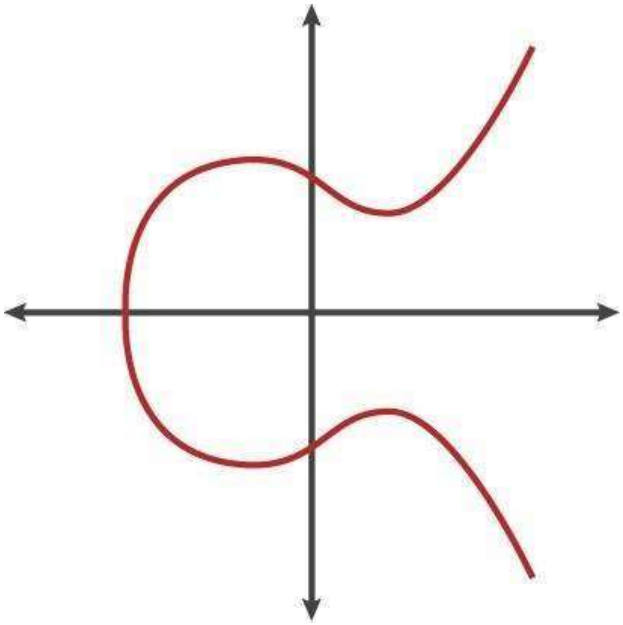
Nele o número de identificação do bloco tem que atender uma série de pré-requisitos para ser aprovado, o que demanda uma grande quantidade de processamento, desencorajando usuários mal-intencionados a fraudarem a rede, e encorajando os usuários bem-intencionados a manterem a rede forte ao dar incentivos monetários a cada número gerado que atende os pré-requisitos, o chamado Coinbase, e quanto mais usuários inseridos no sistema maior é a dificuldade para os malintencionados fraudarem o sistema.

1.4.2 A CRIPTOGRAFIA & ASSINATURA DIGITAL

Por último com os sistemas de confiança, consenso e autenticidade para podermos saber quem será o destinatário e o remetente de cada ação, como por exemplo o envio de Bitcoin entre duas pessoas, quem seria o destinatário e o remetente, e sua validade na rede. A criptografia solucionou esses problemas, a criptografia assimétrica, que por meio de assinaturas digitais autenticassem que as ações fossem assinadas e verificadas pelo autor.

A assinatura digital é possível a partir do sistema de ECDSA (Eliptic curve digital signature algorithm), o qual tem uma chave publica gerada a partir de uma curva elíptica (Figura 6) e é possível utilizá-la para assinar uma transação e outra publica com a qual é possível verificar se aquela assinatura é válida. Para que uma transação seja repassada na rede deve-se mandar o script de transação, que diz ao sistema o que está acontecendo, com a assinatura do proprietário dessa carteira, que é o script codificado que quando submetido a chave de verificação, dá o script original, assim garantindo a veracidade daquela ação por qualquer usuário na rede.

Figura 6: Curva usada no algoritimo assimétrico de criptografia do Bitcoin



https://blog.cloudflare.com/content/images/image02_1.png

1.5 OS PROBLEMAS

Mesmo com todas estas tecnologias e precauções, o blockchain ainda não é desprovido de falhas, já que existem diversos ataques que ainda se aplicam a rede do Bitcoin como descritos nessa sessão.

1.5.1 PROBLEMAS NO SISTEMA

Um dos problemas enfrentados pela rede é, por exemplo, quando se domina 51% do poder de processamento da rede, e pode-se montar uma cadeia por si só, nesse caso tendo o poder de apagar informações da blockchain principal.

Ou até mesmo quando uma parte da rede se rebela e decide que a cadeia de dados deles é a correta como aconteceu no ethereum classic (ETC, 2016)

1.5.2 PROBLEMAS NAS TECNOLOGIAS

Mas a utilização deste sistema, o ECDSA, acarreta vários problemas com a integridade do funcionamento do Bitcoin, conforme a tecnologia vai evoluindo e novas tecnologias vão emergindo como é o caso dos supercomputadores como o computador quântico, o computador biológico e até mesmo a clusterização (Kukh et at, 1986)

Atualmente temos alguns algoritmos capazes de fatorar números grandes, alguns desses exemplos são Lenstra elliptic-curve factorization o qual é perfeito para um número que não exceda os 60 dígitos, sendo assim um algoritmo fraco contra criptografias como o RSA, o algoritmo baseiam-se na mesma tecnologia da qual é feito o ECDSA, as curvas elípticas.

Outro exemplo de algoritmo para este tipo de fatoração de primos é chamado de General number field sieve ou GNFS, ele é considerado o algoritmo mais eficiente para a resolução deste problema (Lenstra, et al. 1993) ele tem uma complexidade atualmente de

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)\ln(n)^{\frac{1}{3}}\ln(\ln(n))^{\frac{2}{3}}\right)$$

Com a introdução do computador quântico no mercado será possível utilizar de algoritmos com um tempo hábil e de complexidade melhores como é o caso do algoritmo de Shor, criado pelo matemático Peter Shor, conseguindo resolver em tempo polinomial, ou seja, no tempo de um problema polinomial N log(n) este grande aumento de eficiência se dá ao fato de ser possível utilizar da Transformada de Fourier quântica (Shor, Peter W. 1999)

2. NOVA TECNOLOGIA

As tecnologias mencionadas acima foram estudadas, demonstrando a conexão entre os algoritmos criptográficos e os principais modelos de Blockchain. Juntamente com o estudo sobre supercomputadores, para se estudar a complexidade dos algoritmos de quebra de criptografia disponíveis atualmente, e definir uma vaga ideia de como o que estamos lidando, concluindo assim qual seria uma possível escala de ganho substituindo os computadores tradicionais por computadores quânticos.

2.1 CRIPTOGRAFIA

O método como parte da criptografia é implementada, principalmente o modelo de chave pública (Stalins, 2017), não permite uma quebra estrutural imediata. Para tal, é necessário fatorar a multiplicação de dois números primos grandes, e o problema da fatoração de primos é conhecido por ser RP (Hopcroft, 2008), o que o torna um problema praticamente inviável de ser resolvido em tempo hábil. Por exemplo o algoritmo RSA utiliza-se das duas equações abaixo para criptografar e de criptografar respectivamente (Rivest et al, 1987):

$$m^e \bmod (m)$$

$$(m^e)^d \bmod m$$

onde e é a chave para criptografar e d a chave para de criptografar. Ambos comumente são números primos na ordem de 2^{100} escolhidos de forma aleatória.

Ou seja, com um computador comum, com a arquitetura de Von Neumman demoraria muito tempo para quebrar, chegando até a décadas dependendo da complexidade e do nível de criptografia utilizado pelo algoritmo.

2.2 SUPERCOMPUTADORES

O computador quântico é um dispositivo que consegue trabalhar com uma quantidade de informações muito maior que o computador da arquitetura de von Neumann. Devido as suas propriedades quânticas, enquanto um bit do computador normal pode armazenar dois tipos de informação 0 ou 1 independentemente da quantidade de bits, um bit quântico armazena quantidades diferentes de estados dependendo de quantos qubits estarão disponíveis.

Sendo assim uma melhoria significativa na realização de cálculos e consequentemente na quebra da criptografia assimétrica utilizada em vários pontos cruciais dos sistemas.

Um qubit armazena a mesma quantidade de informação que 1 bit, já 2 qubits consegue armazenar o mesmo que 4 bits, devido ao estado de superposição que ele pode assumir. Logo, n qubits é equivalente a 2^n bits (Yanofsky, 2008). Os modelos em desenvolvimento ainda são muito específicos e servem somente como protótipos para pesquisadores e cientistas, mesmo os disponíveis comercialmente, como é o caso do IBM Q System One de 20-qubits, anunciado em 2019 na CES (IBM Corp, 2019), enquanto isso há apenas alguns emuladores que permitem simular a sua programação. Atualmente um computador quântico possui em torno de 2000 qubits e os chips quânticos, aproximadamente 72 qubits. Tais modelos ainda não conseguem aproveitar a sua totalidade, aguardando ainda alguns avanços de outros mecanismos periféricos (Alphabet Inc, 2018).

2.3 TÉCNICAS DE FATORAÇÃO ATUAIS

Como já mencionado anteriormente para se quebrar a criptografia assimétrica, temos que primeiramente conseguir resolver o problema de fatoração de números primos de uma maneira rápida. Uma alternativa para a fatoração é pelo método do brute-force sendo utilizado em muitos algoritmos e com outras técnicas que ajudam a diminuir o espaço amostral, como por exemplo o Algoritmo de Pollards Rho, Quadratic Sieve e General Number field Sieve, todos esses utilizam um método de achar um número randômico inicial para montar uma sequência finita de multiplicações desse número usando álgebra modular e a propriedade de multiplicação de inteiros em grupos cíclicos (Riesel, H. "The Structure of the Group M_n."),

Na qual para achar um dos números não precisam achar necessariamente os primos e podem achar os co-primos do número n, e então eventualmente chegar nos primos p e q que são a chave utilizando o método de Euclides. Esse método para chegarmos em um dos co-primos se baseia no fato matemático que dois números que não tem um fator em comum têm uma relação, a qual podemos multiplicar um dos valores por ele mesmo n vezes até chegar no outro número vezes um m mais 1. Assumindo isso, podemos utilizar por exemplo o número N e o co-primo g que queremos descobrir e com isso chegamos na equação $m \cdot N = g + 1$ ou $(g^{-}) + 1) \cdot (g\_ - 1) = m \cdot N$, O N sendo o resultado da multiplicação dos primos, g sendo um chute que que vai melhorando ao longo das tentativas, esse é o princípio do algoritmo de Shor (Shor, Peter 1999)

2.4 FUNCIONAMENTO EM COMPUTADOR QUÂNTICO

O algoritmo pode ser executado em um computador tentando diversos números P com a arquitetura de von Neumann mas não seria mais rápido que um simples algoritmo de brute force, com um computador quântico podemos tentar vários números P ao mesmo tempo, utilizando de um princípio da quântica chamado de superposição, em que a equação é calculada para vários P diferentes e as respostas que não satisfazem a equação vão interferir entre si e se "cancelarem", usando de um fato matemático que se o P estiver errado ele dará um número quando colocado na fórmula $m \cdot N = g + 1$ não resultará em um 1 e sim algum outro número diferente de 1 que se repete de tempos em tempos com uma frequência de P.

Podemos então com essa frequência definida aplicar os dados a uma Fourier quântica, que assim como na Fourier normal serve para calcular a frequência de um dado, no nosso caso a frequência na qual o número errado de P retorna, em um computador quântico essas frequências de erros são representadas como se fossem um seno e interferem entre si destrutivamente resultando em um único resultado a qual satisfaz a $m \cdot N = g +$.

Caso o resultado não seja o mais adequado pegamos o valor resultante de P e refazemos todos os passos acima com um G novo igual a $g \pm 1$ até chegar num valor mais adequado

2.5 ALTERNATIVAS PÓS-QUANTICA

Quando a tecnologia da supercomputação estiver disponível comercialmente, e a segurança da blockchain estiver em risco pelas vulnerabilidades, uma das soluções seria mudar a tecnologia que proporciona a assinatura de transações de criptografia assimétrica para na criptografia pôs quântica como é o exemplo de algumas alternativas que já existem como o qBitcoin (Ikeda, K, 2018).

3. CONCLUSÃO

As tecnologias como a Blockchain, cartões de crédito e mesmo a internet como um todo que dependem da criptografia assimétrica estão seguras por mais algum tempo enquanto novas tecnologias capazes de utilizar a capacidade completa de mecânicas quânticas.

Ainda existem diversas barreiras para que surja uma era de supercomputadores, atualmente não existem memorias quânticas suficientemente grandes para quebrar números maiores que 4 dígitos com o algoritmo de Shor, existem alguns outros algoritmos com a mesma finalidade que acabam sendo um pouco melhores. Os computadores atuais também são focados para laboratórios, devido a sua especialização e seu preço, mesmo com avanços ainda levara um tempo para que essa tecnologia se torne mais comum no dia a dia.

4. BIBLIOGRAFIA

Alphabet Inc. <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>. Último acesso em: 06/06/2018.

Antonopoulos A. M., Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1 ed, 2014, O' Reilly Media.

Back, Adam., "Hashcash – A denial of Service Counter-Measure". Web 1 Ago 2002.

Erkens, D. H., Hung, M., & Matos, P. (2012). Corporate governance in the 2007–2008 financial crisis: Evidence from financial institutions worldwide. Journal of Corporate Finance, 18(2), 389411.

ETC Ethereum Classic <https://ethereumclassic.github.io/> Ultimo acesso em: 26/02/2019

Gottesman, D. et al., Security of quantum key distribution with imperfect devices, International Symposium on Information Theory, 2004. ISIT 2004. Proceedings., 2004, pp. 136

Hopcroft, John E. Introduction to automata theory, languages, and computation. Pearson Education India, 2008.

IBM Corp. <https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-IntegratedQuantum-Computing-System-for-Commercial-Use#assets_115:1612>. Último acesso em: 17/02/2019.

Nakamoto, Satoshi. N.d. "Bitcoin: A Peer-to-Peer Electronic Cash System.", Web Out 2008.

Lenstra, Arjen K., and W. Hendrik Jr. The development of the number field sieve. Vol. 1554. Springer Science & Business Media, 1993.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382-401.

Rivest, R. L.; Shamir A.; e Adleman L. 1978. A method for obtaining digital signatures and publickey cryptosystems. Commun. ACM 21, Fev 1978, 120-126.

Riesel, H. "The Structure of the Group M_n." Prime Numbers and Computer Methods for Factorization, 2nd ed. Boston, MA: Birkhäuser, pp. 270-272, 1994.

Swan M., Blockchain: Blueprint for a new economy, 1 ed, 2015, O' Reilly Media

Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

Ikeda, Kazuki. "qBitcoin: a peer-to-peer quantum cash system." *Science and Information Conference*. Springer, Cham, 2018.

Vigna, P., & Casey, M. J. (2016). The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order. Macmillan.

KUCK, DAVID J. et al., Parallel Supercomputing Today and the Cedar Approach, Science, American Association for the Advancement of Science, pp. 967-974