UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM COMPUTACIONAL DE SISTEMAS

Cleórbete Santos

Tecnologia Blockchain:
Uma proposta de implementação na Universidade Federal do Tocantins

Palmas - Brasil
2018

Cleórbete Santos

Tecnologia Blockchain:
Uma proposta de implementação na Universidade Federal do Tocantins

Dissertação apresentada ao Programa de Pós-Graduação em Modelagem Computacional de Sistemas da Universidade Federal do Tocantins, como requisito parcial para obtenção do título de Mestre em Modelagem Computacional de Sistemas. Orientador: Prof. Dr. Humberto Xavier de Araújo Coorientador: Prof. Dr. David Nadler Prata

Palmas - Brasil
2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

S237t Santos, Cleorbete.

Tecnologia Blockchain: Uma proposta de implementação na Universidade Federal do Tocantins . / Cleorbete Santos. – Palmas, TO, 2019.

75 f.

Dissertação (Mestrado Acadêmico) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) em Modelagem Computacional de Sistemas, 2019.

Orientador: Humberto Xavier de Araújo

Coorientador: David Nadler Prata

1. Computação. 2. Blockchain. 3. Criptografia. 4. Tecnologia. I. Título

CDD 4

Elaborado pelo sistema de geração automatica de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO TOCANTINS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
COORDENAÇÃO DO PROGRAMA DE PÓS-GRADUAÇÃO
MODELAGEM COMPUTACIONAL DE SISTEMAS

Palmas, 28 de setembro de 2018.

Aos 28 (vinte e oito) dias do mês de setembro de 2018, realizou-se a defesa de dissertação do aluno **CLEORBETE SANTOS**, do Curso de Mestrado em Modelagem Computacional de Sistemas, da Universidade Federal do Tocantins (UFT), intitulada: "***TECNOLOGIA BLOCKCHAIN: UMA PROPOSTA DE IMPLEMENTAÇÃO NA UNIVERSIDADE FEDERAL DO TOCANTINS***", realizada sob a Orientação do Professor Dr. **HUMBERTO XAVIER DE ARAÚJO**, tendo como banca avaliadora, os professores abaixo relacionados.

Atribuíram a Nota Final A (APROVADO COM LOUVOR.) pelo trabalho, tendo sido considerado _____. Nada mais tendo a constar, assinam esta Ata os professores componentes da banca.

Professor Humberto Xavier de Araújo, Dr.
PPGMCS – Orientador

Professor David Nadler Prata, Dr.
PPGMCS – Coorientador

Professora Ana Lúcia de Medeiros, Dra.
UFT – Membro Externo

Professora Leila Chevtchuk, M.Sc.
Universidade Mackenzie – Membro Externo

Professor Coriolano Camargo, Dr.
Universidade Mackenzie – Membro Externo

Agradecimentos

Aos meus pais, por seu amor incondicional.
À minha esposa, por sua compreensão.
Aos meus filhos, por me fazerem renascer todos os dias.
E ao Goku, por salvar aTerra.

“Aquilo que você sabe não importa. O que importa é aquilo que você faz com o que sabe.” (Bruce Lee)

Resumo

O presente trabalho tem como propósito implementar uma infraestrutura de blockchain privada para o armazenamento de dados, especificamente, os certificados de conclusão ou participação emitidos pela Universidade Federal do Tocantins, Campus Palmas-TO, Brasil, com vistas a evitar sua falsificação por meio de validação usando criptografia (hashing). Algumas instituições de ensino, como o Massachusetts Institute of Technology e a Holberton School, em San Francisco (EUA), utilizam a blockchain pública da Bitcoin para manter e validar seus certificados, porém, mediante pagamento de taxas. A implementação de Blockchain adotada para esse projeto foi a Multichain, solução que, por ser código aberto, diminui custos de implantação, propicia facilidade de instalação e manutenção de sua infraestrutura e dispensa cobranças de quaisquer taxas ou valores para armazenamento de informações, o que a torna adequada perante o caráter público da Universidade Federal do Tocantins. Por conta de suas características de segurança e transparência no armazenamento de dados, a Blockchain tem sido utilizada em diversas tecnologias, como a criptomoeda Bitcoin, contratos inteligentes, economia compartilhada, governança corporativa, proteção de propriedade intelectual, Internet das Coisas (IoT), gerenciamento de identidade, entre outros, e também na Educação, foco desse trabalho.

Palavras-chave: Educação, Tecnologia, Blockchain, Criptografia.

Abstract

The purpose of the present work is to implement a private blockchain infrastructure for data storage, specifically the certificates of completion or participation issued by the Federal University of Tocantins, Campus Palmas-TO, Brazil, with a view to avoiding their falsification by means of validation using hashing. Some institutions, such as the Massachusetts Institute of Technology and Holberton School in San Francisco, use Bitcoin's public blockchain to maintain and validate their certificates, but for fees. The Blockchain implementation adopted for this project was Multichain, a solution that, because it is open source, reduces deployment costs, facilitates easy installation and maintenance of its infrastructure, and waives any fees or amounts for information storage. makes it appropriate to the public character of the Federal University of Tocantins. Because of its security features and transparency in data storage, Blockchain has been used in a number of technologies, such as the Bitcoin cryptomoeda, smart contracts, shared economy, corporate governance, intellectual property protection, Internet of Things (IoT), management of identity, among others, and also in Education, the focus of this work.

Keywords: Education, Technology, Blockchain, Criptography.

Sumário

Lista de Figuras e Tabelas

1. INTRODUÇÃO

Blockchain - originalmente chamado de block chain - é uma tecnologia de banco de dados distribuído que permite manter uma lista crescente de registros, chamados de blocos. Cada bloco contém uma informação de data e hora de criação e um link que aponta para um bloco anterior. Uma blockchain é tipicamente gerenciada por uma rede cliente-a-cliente (peer-to-peer) que usa um protocolo específico para validar novos blocos de maneira coletiva (ANTONOPOULOS, 2010). Por definições de projeto, blockchains são inerentemente resistentes à modificação não autorizada de seus dados. Uma vez gravados, os dados em qualquer bloco não podem ser alterados retroativamente sem a alteração de todos os blocos subsequentes e a validação de toda a rede de blocos interligados. Em termos funcionais, uma cadeia de blocos pode servir como um "livro-razão" (*ledger*) aberto e distribuído que pode gravar as transações entre duas partes de forma eficiente e de forma verificável e permanente. O próprio livro-razão também pode ser programado para disparar as transações automaticamente (WATTENHOFFER, 2016). A primeira blockchain foi conceitualizada por Satoshi Nakamoto no ano de 2008 e implementada, nos anos seguintes, como componente principal da moeda digital Bitcoin, onde serve como livro-razão público para todas as transações relativas a essa criptomoeda (NAKAMOTO, 2008).

Satoshi Nakamoto é o apelido virtual do desconhecido fundador (ou fundadores) da moeda virtual Bitcoin e criador do *Original Bitcoin Client* (aplicação que permite as transações em Bitcoin). Nakamoto inventou o protocolo Bitcoin e publicou um artigo sobre o assunto na *Cryptography Mailing List* em 01 de novembro de 2008 (PÉREZ-MARCO, 2016). Dizia o resumo do artigo que "uma versão pura de dinheiro eletrônico cliente-a-cliente (*peer-to-peer*) permitiria que pagamentos online fossem enviados de uma parte a outra na Internet sem as burocracias existentes em instituições financeiras" (estas dispensadas na estrutura vislumbrada por Satoshi Nakamoto). Nakamoto trabalhou com outras pessoas pela Web, porém nunca revelou sua real identidade, deixando o projeto "para se dedicar a outras atividades", como manifestou em 2011 (PEARSON, 2017).

Blockchains usam o paradigma de “Segurança por projeto” (*Security by design*), ou seja, desde sua concepção, e durante seu desenvolvimento, são levados em consideração aspectos de Segurança da Informação, como confidencialidade, integridade e disponibilidade, e padrões de tolerância a falhas (*Fault-tolerance*), que pregam, em sua essência, que uma tecnologia deve estar apta a continuar funcionando de maneira satisfatória, mesmo quando da ocorrência de falhas.

Blockchain, tecnicamente, é banco de dados distribuído, espalhado por muitos dispositivos eletrônicos sem controle centralizado, que tem impactado na Governança, na Economia, nos negócios em geral e no funcionamento das organizações do mundo inteiro, e também na Educação. Blockchain pode ser implementada em instituições educacionais individuais, grupos de instituições educacionais e em organizações educacionais nacionais e internacionais. De fato, qualquer interessado em armazenar informações de forma segura - e tornar tais informações acessíveis para terceiros - pode considerar o uso da tecnologia Blockchain. À medida que a educação se torna mais diversificada, democratizada, descentralizada e desintermediada, torna-se necessário manter a reputação, a confiança na certificação e prova de aprendizado. A Blockchain pode fornecer uma infraestrutura que atenda a essas necessidades: um banco de dados aberto, *online* e seguro.

Soluções de Blockchain aplicadas à Educação estão presentes em instituições renomadas, como no *Massachusetts Institute of Technology* e na *Holberton School*, em *San Francisco* (EUA), onde o armazenamento e a entrega de certificados emitidos são feitos utilizando-se a blockchain pública da Bitcoin, por meio de pagamento de um pequeno valor a cada certificado gerado, como medida para evitar falsificação desses documentos. Neste trabalho, diferentemente, é utilizada uma blockchain privada (Multichain) como repositório dos certificados emitidos pela Universidade Federal do Tocantins. Por seu caráter particular e por ser código aberto, essa versão (privada) de blockchain torna-se uma alternativa mais econômica para as instituições que a adotem, gerando confiabilidade, segurança e transparência no armazenamento de seus artefatos digitais.

1.1 Motivação

A tecnologia Blockchain nasceu com os objetivos de descentralizar o armazenamento de dados, oferecer maior transparência às transações efetuadas em seu bojo, além de utilizar conceitos e paradigmas da Segurança da Informação como o princípio da irretratabilidade e a criptografia. Estudar e implementar soluções baseadas em Blockchain, com vistas à utilização de suas características e vantagens, torna-se natural, haja vista sua aplicabilidade atual e futura nos mais diversos campos do conhecimento humano, como Educação, Direito (contratos inteligentes, etc.), *E-government*, logística, entre diversos outros.

1.2 Objetivos

1.2.1 Objetivo geral

O objetivo principal desse trabalho é implantar uma blockchain privada, usando a implementação de código aberto *Multichain* para armazenar, de maneira segura, certificados eletrônicos emitidos pela Universidade Federal do Tocantins.

1.2.2 Objetivos específicos

- Realizar uma revisão bibliográfica sobre a tecnologia Blockchain.
- Explanar sobre os conceitos principais da tecnologia Blockchain.
- Listar as principais aplicações possíveis com uso da tecnologia Blockchain.
- Propor a implantação de uma blockchain privada usando Multichain objetivando o armazenamento seguro de certificados eletrônicos da Universidade Federal do Tocantins.

1.3 Organização

O trabalho está dividido em quatro capítulos. No capítulo 1 está descrita a introdução. No capítulo 2 são apresentados os conceitos e tecnologias que compõem ou estão relacionados à Blockchain, como Criptografia de Chave Pública, Funções Hash, Assinatura Digital e Redes p2p. Neste capítulo, também estão descritas as operações básicas dessas redes (cadeias de blocos de dados, transações, mineração, etc.) e questões relacionadas à Segurança da Informação pertinentes.

No capítulo 3 encontram-se tópicos que tratam da aplicabilidade da tecnologia Blockchain à Educação, como a emissão de certificados à prova de falsificação, registros de proficiência de alunos, portfólios eletrônicos, redes comunitárias digitais de professores e alunos, entre outros. No capítulo 4 é apresentada a solução Blockchain de código-aberto Multichain, bem como os passos necessários para sua instalação, configuração e uso, objetivando o armazenamento de certificados eletrônicos emitidos pela Universidade Federal do Tocantins. O capítulo 4 finaliza com a demonstração de uma interface feita em linguagem PHP para interação com a Multichain. Já no capítulo 5 estão descritas as conclusões do trabalho.

2. REVISÃO BIBLIOGRÁFICA

Para maior didática e mais clareza no presente estudo, a revisão bibliográfica foi segregada em algumas partes. O tópico 2.1 tratará de conceitos elementares relacionados à tecnologia Blockchain, como Criptografia de Chave Pública, Hash, Assinatura Digital e Redes p2p. O tópico 2.2, por sua vez, explanará sobre o funcionamento da Blockchain e sua estrutura (cadeia de blocos, transações, mineração). E, por fim, o tópico 2.3 tratará de questões de segurança atinentes à Blockchain, com o ataque conhecido como "> 51%", conceitos de chaves e aleatoriedade, e confidencialidade e anonimato.

2.1 Conceitos básicos

Este tópico visa esclarecer conceitos basilares relativos às implementações da tecnologia Blockchain.

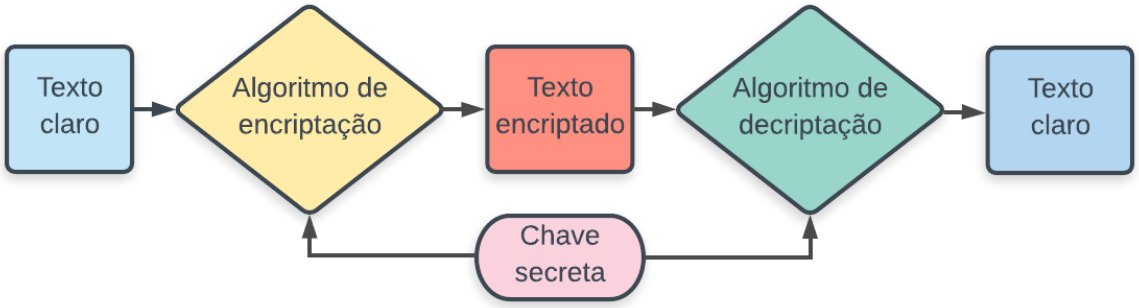
2.1.1 Criptografia de chave pública

Criptografia é área de estudo que engloba as diversas estratégias de encriptação e decriptação de informações, sendo encriptação a transformação de um texto claro (texto original) em texto cifrado (encriptado), e decriptação a recuperação do texto claro (texto original) a partir do texto cifrado (POINTCHEVAL, 2002).

No modelo de criptografia dita simétrica, utiliza-se apenas uma chave, chamada de chave secreta. A chave secreta é fornecida, juntamente com o texto claro (texto original), a um algoritmo de encriptação, que gerará como saída um arquivo encriptado (que será diferente conforme a utilização de chaves secretas também diferentes). Chama-se algoritmo de decriptação o código computacional a ser utilizado para reverter o processo de encriptação, ou seja, a obtenção do texto claro (texto original) a partir do texto encriptado, desde que fornecida a chave secreta utilizada no processo de encriptação. A segurança na utilização da

criptografia simétrica depende de algoritmos fortes (que não sejam vulneráveis a criptoanálise) e que as chaves secretas envolvidas nos processos de encriptação e decriptação sejam armazenadas e compartilhadas pelos usuários autorizados de maneira confidencial. Na Figura 1 é possível observar o funcionamento da criptografia simétrica.

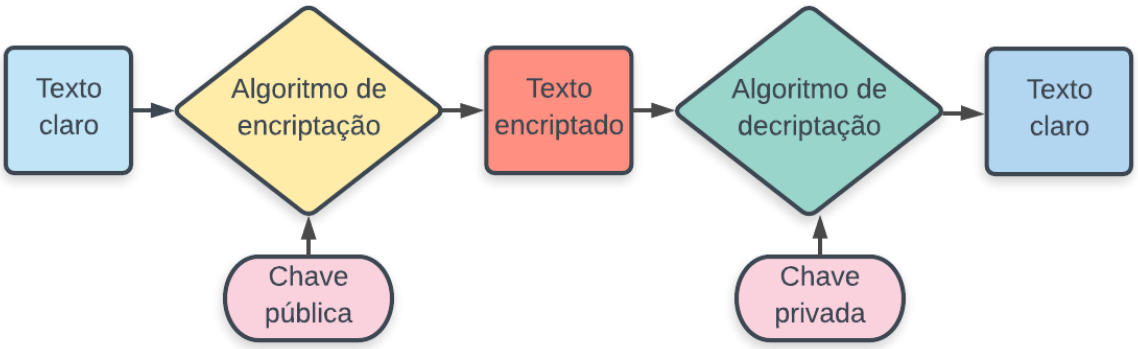
Figura 1 - Criptografia simétrica (ou de chave secreta).



Fonte: Tanenbaum (adaptado pelo autor).

Por outro lado, a criptografia de chave pública, foco desse tópico, é assimétrica, pois utiliza duas chaves distintas, porém relacionadas (chave pública e chave privada), o que a distingue da criptografia simétrica, que usa apenas uma mesma chave, chamada de chave secreta, para suas operações de encriptar e decriptar. A utilização de chaves separadas tem vantagens em relação à utilização de uma única chave, principalmente no tocante aos princípios da confidencialidade, da autenticidade e de estratégias de armazenamento e compartilhamento de chaves. O funcionamento da criptografia assimétrica é exibido na Figura 2.

Figura 2 - Criptografia assimétrica ou de chave pública.



Fonte: Tanenbaum (adaptado pelo autor).

A seguir estão listadas algumas terminologias relacionadas à criptografia de chave pública (STALLINGS, 2014):

- Chaves assimétricas: são chaves que se complementam em operações relativas à codificação (encriptação) e decodificação (decriptação) de informações, e também à criação e validação de assinaturas digitais.

- Certificado de chave pública: é um documento digital, assinado pela chave privada de uma Autoridade de Certificação, que associa o nome de um usuário a uma chave pública. O certificado sinaliza que o usuário possui domínio sobre a chave privada relacionada.

- Algoritmo criptográfico de chave pública (assimétrica): é o código computacional que utiliza as chaves pública e privada em operações relacionadas à criptografia, com a propriedade de ser inexequível computacionalmente a obtenção da chave privada a partir da chave pública.

- Infraestrutura de chave pública (PKI): é uma infraestrutura composta por processos, políticas, serviços de rede, entre outros itens, utilizada para a administração de certificados digitais e chaves públicas e privadas relacionadas.

Em se tratando de confidencialidade, a criptografia de chave pública (assimétrica) funciona com a encriptação da informação usando-se a chave pública do usuário que receberá a informação. Esse mesmo usuário, assim que recebê-la, fará uso de sua chave privada para decriptar a informação para dela fazer uso. Por exemplo: se Maria deseja enviar uma mensagem sigilosa (confidencial) a Gilberto, Maria codificará (encriptará) a mensagem usando a chave pública de Gilberto, e Gilberto, por sua vez, usará sua chave privada para decriptar (decodificar) a mesma mensagem.

A autenticação é outro princípio da Segurança da Informação, que é garantido pela criptografia de chave pública. Se um usuário deseja enviar conteúdo assinado digitalmente a outrem, deverá, para tanto, utilizar-se de sua chave privada aplicada à informação original. O usuário de destino deverá, por sua vez, utilizar a chave pública do usuário de origem para validar o arquivo. Ressalve-se que somente o usuário de origem poderia ter gerado o arquivo assinado digitalmente, haja vista a utilização de sua chave privada. Esse processo, repise-se, respeita o princípio da autenticidade e também o da irretratabilidade (o usuário que gerou o arquivo assinado digitalmente não poderá negar a autoria em relação ao mesmo).

Como já aludido, a criptografia assimétrica colabora com a segurança no que diz respeito à disponibilidade das chaves: a chave pública fica disponível a qualquer interessado, e a chave privada fica disponível apenas ao seu proprietário.

Em contrapartida, a criptografia simétrica usa apenas uma chave, sendo que esta tem que ser de conhecimento, tanto do emissor, como do receptor. E ainda, por conta disso, essa chave deverá ser, em algum momento, compartilhada entre esses usuários. Essa troca de informação da chave simétrica entre os usuários antes dos dados serem criptografados gera insegurança, uma vez que um atacante pode interceptar essa comunicação que não está ainda criptografada e ter acesso à chave de criptografia durante seu trânsito ou recebimento pelo canal de comunicação.

Um dos maiores problemas relacionados à utilização de chaves criptográficas diz respeito ao tráfego de informação em um canal de comunicação inseguro, como a Internet. Por conta disso, algoritmos criptográficos foram criados para que uma sessão de comunicação segura possa ser gerada e utilizada pelos envolvidos. Um

desses algoritmos é o Diffie-Hellman, cujo título é oriundo dos nomes de seus criadores (Whitfield Diffie e Martin Hellman), com publicação original sobre sua utilização remontando ao ano de 1976 (CARTS, 2001). O algoritmo (de troca de chave) Diffie-Hellman permite que dois ou mais usuários estabeleçam uma sessão de comunicação criptografada em um canal inseguro por meio da criação de uma chave secreta de sessão (em uma espécie de criptografia simétrica aplicada à segurança do meio de comunicação). O algoritmo Diffie-Hellman é utilizado apenas para troca de chave, ou seja, não permite a criptografia de informações e nem assinatura digital.

O RSA, criado na década de setenta pelos pesquisadores Ronald Rivest, Adi Shamir e Leonard Adleman (imortalizados por suas iniciais que dão nome ao algoritmo) e o Curva Elíptica, criado por Neal Koblitz e Victor S.Miller em 1985 e conhecido também por Criptografia de Curvas Elípticas (JANSMA, 2004), são dois algoritmos que permitem a troca de chave (criação de sessão de comunicação segura em um canal inseguro) e também as operações de criptografia de encriptação e decriptação de informações, além de permitir a utilização de assinatura digital.

O RSA trabalha com o produto de números primos em suas operações de criptografia, onde os números primos compõem a chave secreta e seu produto resulta na chave pública e, por conta disso, exige a utilização de chaves cada vez maiores para evitar a fatoração dos números envolvidos (o que inviabiliza a quebra da segurança do algoritmo). A Criptografia de Curvas Elípticas (CCE), por sua vez, utiliza chaves menores, o que a torna mais eficiente. Essa criptografia baseia-se na estrutura algébrica de curvas elípticas sobre campos finitos por meio da equação $y^2 = x^3 + ax + b$, sendo este o algoritmo criptográfico mais utilizado em Blockchain (MILLER, 2017).

2.1.2 Função Hash

Uma função hash (ou função de hashing) é uma função criptográfica que recebe qualquer informação de tamanho variável e oferece, como resultado, uma informação de tamanho fixo (cujo tamanho normalmente varia entre 128 e 256 bits).

Ao resultado gerado pela operação de hashing dá-se o nome de Hash. Esse tipo de criptografia não é utilizado para assinar digitalmente documentos inteiros, apenas seu resumo, tornando-a mais eficiente (em se tratando de assinatura digital) do que os algoritmos criptográficos assimétricos apresentados no tópico anterior, como RSA, Curvas Elípticas, etc. (MORENO et al, 2005).

Uma função hash é tida como eficaz quando recebe grandes quantidades de dados e consegue gerar resultados bem distribuídos de forma randômica (STALLINGS, 2014). E, além disso, para ter funcionalidade no campo da criptografia, funções hash devem possuir as seguintes características (BURNETT, 2001):

- Ser simples, porém operar com eficiência e rapidez nas operações de geração de hash das informações que receber.

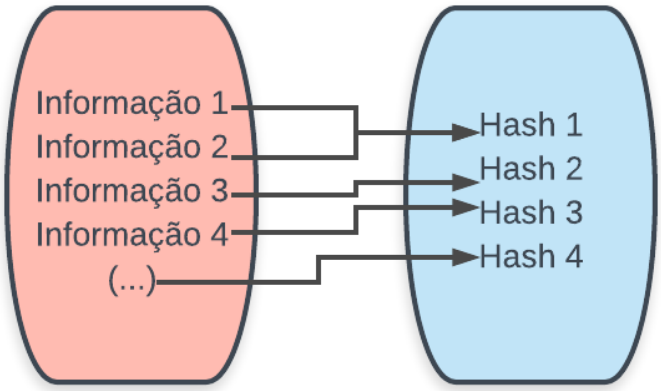
- Impossibilitar a engenharia reversa dos hashs gerados resultando na descoberta das informações originais.

- Impossibilitar a descoberta de uma informação original que possa gerar o mesmo hash oriundo de outra informação original (colisão).

- Permitir a geração de hashs por equiprobabilidade estatística, ou seja, que apresentem as mesmas probabilidades de ocorrência.

A colisão acontece quando o mesmo hash é gerado a partir de informações diferentes fornecidas ao algoritmo de hash. E, mesmo com a exigência de baixa probabilidade de colisão, para que um algoritmo figure como eficiente e seja considerado robusto, deduz-se que não há como eliminar esse fenômeno, pois é infinito o conjunto de informações que podem ser enviadas à função de hash e finito o conjunto de hashs resultantes, como demonstrado na Figura 3.

Figura 3 - Exemplo de colisão em operações de hashing.



Fonte: Drescher (adaptado pelo autor).

Respeitar o princípio da integridade dos dados também é um dos objetivos das funções hash, pois qualquer alteração efetuada em uma informação original poderá ser comprovada pela geração de um novo hash. Por exemplo: Pedro gera um hash de uma informação e envia a informação e o hash a Marta, que, por sua vez, ao receber ambos, gera um novo hash, que deverá ser igual ao enviado por Pedro (caso contrário, a informação terá sido modificada durante seu trajeto de um usuário a outro).

Os algoritmos de hash mais utilizados em aplicações do mundo inteiro são o MD4, MD5 e o SHA (BURR, 2008), sendo que os dois primeiros geram hashs com 128 bits de tamanho, e o último, 160 bits. A seguir, seguem outros algoritmos de hashing com seus respectivos tamanhos de hash (onde podemos observar que 128 bits é o tamanho mais comum):

- Abreast Bavies-Meyer (c/IDEA): 128 bits;
- Davies-Meyer (c/DES): 64 bits;
- GOST-Hash: 256 bits;
- NAVAL (3 passos): tamanho variável;

- NAVAL (4 passos): tamanho variável;
- NAVAL (5 passos): tamanho variável;
- N-HASH (12 voltas): 128 bits;
- N-HASH (15 voltas): 128 bits;
- RIPE-MD: 128 bits;
- RIPE-MD-160: 160 bits;
- SNEFRU (4 passos): 128 bits;
- SNEFRU (8 passos): 128 bits;

Para fins didáticos, na Tabela I são demonstrados valores hash gerados utilizando-se o algoritmo de hashing SHA-256, criado pela Agência de Segurança Nacional dos Estados Unidos (*NSA - National Security Agency*), que faz parte do conjunto de algoritmos criptográficos SHA-2 e que é o mais empregado em implementações Blockchain na atualidade (SHA-256 é utilizado no processo de mineração pelo algoritmo “Proof of work” e para a criação de endereços Bitcoin - neste caso, para prover maior segurança e privacidade).

Tabela I - Exemplos de hashs gerados com SHA-256.

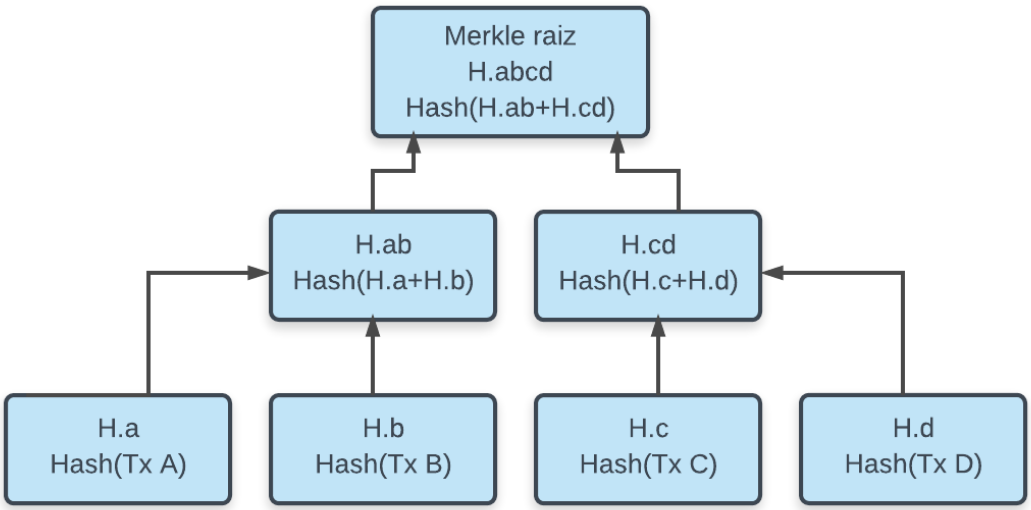
Informação	Hash gerado com SHA-256
Olá	5251C3C68010BCA32F4DBEDB142270F720FA84A0599816524C85D50C3F589365
Hello	185F8DB32271FE25F561A6FC938B2E264306EC304EDA518007D1764826381969
hello	2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824

Fonte: Drescher (adaptado pelo autor).

É interessante notar que qualquer alteração nas palavras citadas na primeira coluna da tabela, que são entradas da função de hashing, gerará hashs diferentes, como no caso da palavra “Hello” (com h maiúsculo) e “hello” (com a mesma letra em minúsculo). Outro ponto a ser observado diz respeito ao tamanho do hash gerado: sempre será de 256 bits, ou seja, tem tamanho fixo, como anteriormente afirmado.

Em implementações da tecnologia Blockchain, hashs são muito utilizados para a definição de *Merkle Trees*. Árvores, no âmbito da computação, são estruturas de dados não lineares (FORBELLONE, 2005). Diferem das listas, que armazenam dados em sequência (forma linear), por estocar dados de maneira hierarquizada, ou seja, nas árvores as informações residem abaixo ou acima de outras informações (LAUREANO, 2008). *Merkle Trees*, ou árvores de dispersão, são árvores nas quais cada nó folha (elemento sem ramos) possui o hash de um bloco de dados, e onde cada nó que não é folha (elemento com ramos) possui o hash criptografado de seus nós filhos. *Merkle Trees* são consideradas como solução adequada para a verificação eficiente e segura de conteúdo em grandes quantidades de dados. A conceituação de *Merkle Trees* foi feita por Ralph Merkle no ano de 1979 (NAYARANAN, 2015). Na Figura 4, podemos ver a estrutura de uma *Merkle Tree* implementada em uma blockchain.

Figura 4 - Exemplo de Merkle Tree utilizada em Blockchain.



Fonte: Drescher (adaptado pelo autor).

2.1.3 Assinatura Digital

Assinatura digital é um dos produtos da criptografia que leva, ao mundo eletrônico, os atributos de uma assinatura feita a punho no mundo *offline*, quais sejam:

- Legitimidade: afeta ao Princípio da Autenticidade, dita que terceiros poderão ter conhecimento de quem produziu a assinatura, mas somente uma pessoa deverá saber produzi-la.

- Aval: a assinatura produzida deve estar relacionada apenas à informação que se quer dar aval e a nenhuma outra.

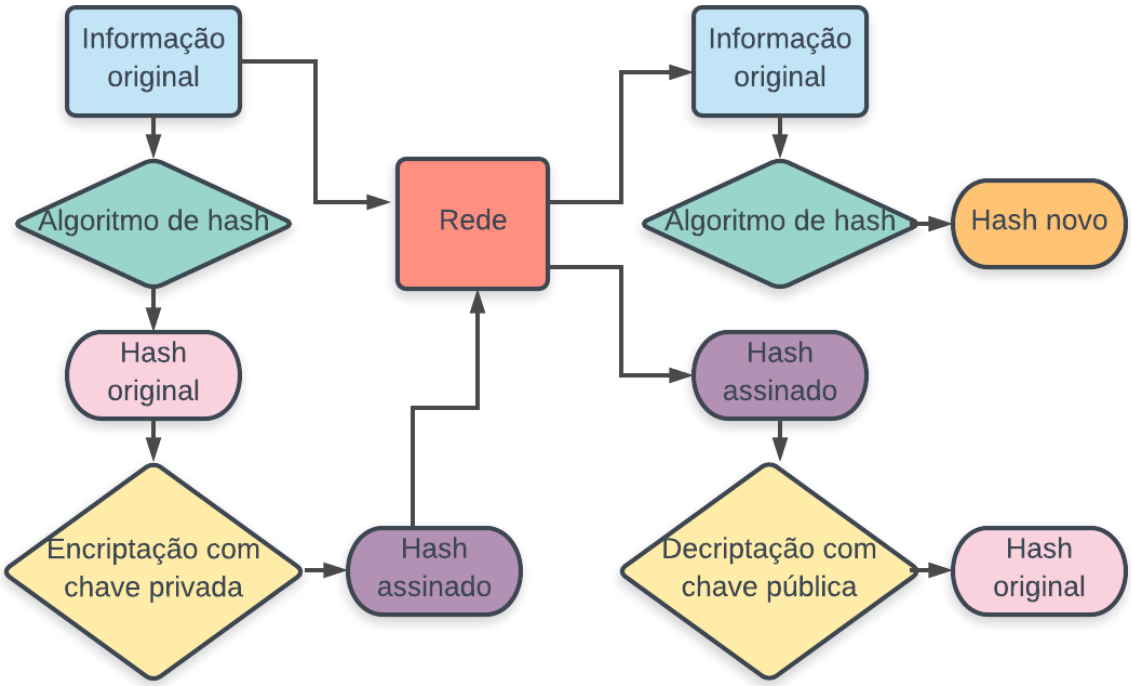
Com os atributos acima, anseia-se que uma dada assinatura possa ser utilizada de maneira segura, isto é, que não seja passível de falsificação e que não venha a ser relacionada a uma informação à qual não tenha sido previamente vinculada. Em termos de assinatura digital, esses mesmos atributos devem ser respeitados, e utiliza-se a criptografia de chave pública para garantir sua plena aplicabilidade em termos práticos.

Em tópicos anteriores foi dito que o Princípio da Confidencialidade é alcançado pela encriptação da informação, utilizando-se a chave pública de um determinado usuário, situação na qual este somente terá acesso à informação original se utilizar sua chave privada para decifrar a informação que foi encriptada. No caso da Assinatura Digital, o princípio a ser venerado é o da Autenticidade, contexto alcançado pelo processo inverso, ou seja, pela utilização da chave privada para criptografar (assinar digitalmente) a informação e posterior validação da assinatura, por terceiros, pela utilização da chave pública de quem assinou a informação. Dessa forma, no primeiro processo (uso da chave pública para criptografar), o objetivo é o sigilo da informação. Neste outro processo (uso da chave privada para criptografar), o objetivo é garantir que somente determinado usuário poderia ter assinado determinada informação (BURNETT, 2001).

Uma maneira de tornar a utilização de assinaturas digitais mais otimizada em termos computacionais é por meio das funções hash. Foi visto que as funções hash geram saída de tamanho fixo a partir de quaisquer entradas de tamanho variável e que um bom algoritmo de hash teria a propriedade de possuir baixos índices de colisão (a geração do mesmo hash como resultado para informações de entrada distintas). A otimização mencionada será alcançada por meio da assinatura digital aplicada apenas ao hash da informação. Ou seja, em vez de assinar a informação

inteira, assina-se apenas seu resumo (hash). Naturalmente, terceiros interessados em validar a autenticidade da mensagem poderão fazê-lo, gerando um novo hash da informação e comparando com o hash original (CURRY, 2001), como exibido na Figura 5.

Figura 5 - Assinatura Digital aplicada apenas ao hash da informação.



Fonte: Tanenbaum (adaptado pelo autor).

Na Figura 6, temos o processo de assinatura digital aplicado apenas ao hash de uma informação, conforme os passos abaixo:

1. O usuário remetente gera um resumo (hash) da informação utilizando um algoritmo de hash.

2. O usuário remetente assina digitalmente o hash utilizando sua chave privada.

3. O usuário remetente envia a informação e o hash assinado pela rede de computadores.

4. O usuário destinatário recebe a informação e o hash assinado pelo usuário remetente.

5. O usuário destinatário gera um novo resumo (hash) da informação utilizando um algoritmo de hash.

6. O usuário destinatário obtém o hash original utilizando a chave pública do usuário remetente contra o hash assinado.

7. O usuário destinatário compara o hash novo com o hash original, comprovando, se iguais, que não houve alteração da informação, confirmando que a informação chegou íntegra.

A tecnologia Blockchain, em sua versão pública, funciona com a característica de ter transparência em relação aos dados que armazena e, por isso, dispensa a aplicação do Princípio da Confidencialidade: os dados nela disponíveis são acessíveis a qualquer interessado. Por outro lado, opera com total respeito ao Princípio da Autenticidade, ao exigir que todo aquele que insira informações em seus blocos de dados possa ser identificado por meio de assinaturas digitais (OKUPSKI, 2016).

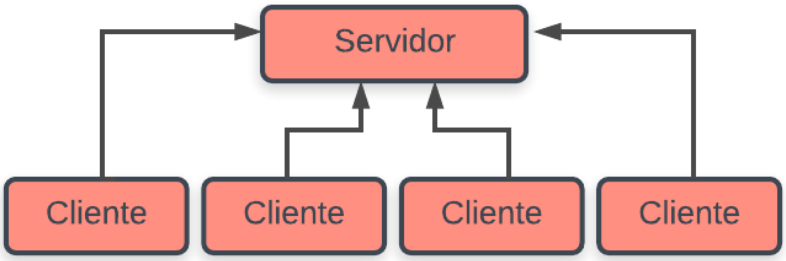
A implementação de tecnologia Blockchain empregada na rede Bitcoin utiliza, para as assinaturas digitais de seus usuários, um algoritmo de Curvas Elípticas (*ECDSA - Elliptic Curve Digital Signature Algorithm*) próprio, chamado “Secp256k1”, definido e mantido pelo *Standards for Efficient Cryptography Group (SECG)*, consórcio fundado em 1998, composto por diversas corporações, que objetiva facilitar a adoção de tecnologias de criptografia eficientes e promover a interoperabilidade em meio ao vasto complexo de plataformas computacionais existente (ANTONOPOULOS, 2010).

2.1.4 Redes p2p

Computação p2p ou redes p2p (do inglês *“peer-to-peer”*, ou seja, “cliente-a-cliente”) diz respeito, na literatura de redes de computadores, à arquitetura de aplicações distribuída que particiona tarefas ou cargas de trabalho entre dispositivos participantes.

Nessa arquitetura, os participantes (*peers*) funcionam, ao mesmo tempo, como clientes e servidores, diferentemente da arquitetura cliente-servidor (demonstrada na Figura 6), em que cada cliente faz requisições e aguarda as respostas do servidor a eles conectado. A interação entre clientes e servidores é também conhecida como “comportamento de requisição-resposta” (TANENBAUM, 2007).

Figura 6 - Arquitetura cliente-servidor.



Fonte: Tanenbaum (adaptado pelo autor).

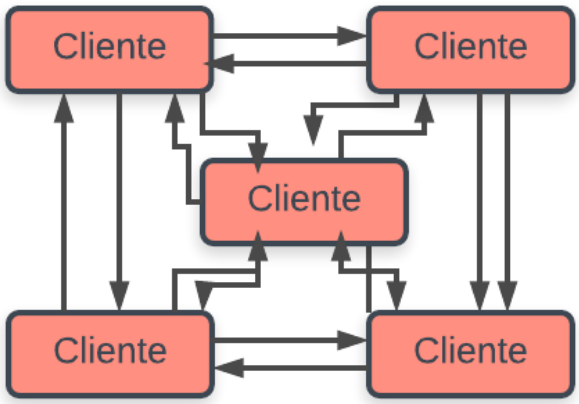
A comunicação entre clientes e servidores na arquitetura cliente-servidor pode ser implementada por meio de um protocolo simples não orientado a conexão (*connectionless*), quando a infraestrutura de rede for suficientemente confiável (o que geralmente acontece nas redes locais). Nesses casos, quando um cliente requisita um serviço de rede, ele simplesmente empacota uma mensagem para o servidor, com a identificação do serviço que deseja consumir, além dos dados necessários para a operação. A mensagem, então, é enviada ao servidor que, por sua vez, processa as requisições e retorna um pacote de resposta que é enviado ao cliente requisitante (TANENBAUM, 2002).

Com a quantidade de clientes aumentando e, por conseguinte, aumentando, também, as requisições e respostas entre clientes e servidor em uma arquitetura cliente-servidor, o desempenho da rede vai diminuindo, ao contrário do que ocorre em arquiteturas p2p, onde o desempenho aumenta conforme aumenta o número de

clientes (*peers*) conectados entre si. É natural que nessa arquitetura (p2p) os clientes (*peers*) possam enviar e receber informações de forma simultânea, ao passo que podem conectar e desconectar da rede sem ferir a disponibilidade da mesma, caracterizando uma alta tolerância a falhas, distintamente da arquitetura cliente-servidor, onde indisponibilidade do servidor gera indisponibilidade para os clientes.

Além do que foi explanado, as redes p2p, também utilizadas em implementações da tecnologia Blockchain, possuem como uma de suas características principais a descentralização, que implica na cópia de uma informação enviada à rede para inúmeros clientes em diferentes partes do mundo (sem intermediários), tornando impraticável a exclusão ou modificação indevida de dados sem que os demais clientes da rede, em sua totalidade, também sejam afetados. Abaixo, a Figura 7 retratando clientes interconectados em uma arquitetura p2p (DONET, 2014).

Figura 7 - Arquitetura p2p (Peer-to-peer).



Fonte: Tanenbaum (adaptado pelo autor).

A tecnologia Blockchain é também conhecida por ser um repositório de registros criptografado (*distributed ledger*), compartilhado entre todos os clientes participantes de uma rede p2p, onde cada transação efetuada com sucesso (e validada na rede) é armazenada. Nas próximas seções será demonstrado, com mais profundidade, como a Blockchain funciona.

2.2. Blockchain

Nos tópicos anteriores foram explicados conceitos básicos de tecnologias presentes em Blockchain. Para esse tópico usaremos como exemplo a implementação de Blockchain utilizada na rede Bitcoin, a qual é a primeira criptomoeda digital do mundo e, também, um sistema de pagamentos global e descentralizado (nos moldes das supracitadas redes p2p). Por oportuno, não há que se olvidar que a blockchain utilizada na Bitcoin é pública, muito embora também haja, no universo digital, soluções privadas, como a Multichain, solução adotada para o projeto de blockchain desse trabalho, que será explicado em momento oportuno.

Blockchains privadas são inerentemente mais rápidas que as públicas, pois nas primeiras a descentralização real não é exigida e seus participantes não precisam minerar blocos de dados, devendo, ao invés, apenas validar transações (GUEGAN, 2017). De qualquer forma, deve ser destacado que blockchains privadas têm sua aplicabilidade restrita a determinadas situações, e, do mesmo modo, as públicas (GARZIK, 2015).

2.2.1 Cadeias de blocos

Na rede Bitcoin, a tecnologia Blockchain é uma estrutura de registros pública, temporizada, ou seja, *timestamped*, ordenada e imutável de transações realizadas. Cada bloco de informações é identificado por um hash na cadeia de blocos e é conectado aos blocos anteriores por meio de referências aos seus hashs.

A seguir, na Tabela II, é demonstrada a estrutura de um bloco pertencente à blockchain da Bitcoin.

Tabela II - Estrutura de um bloco Blockchain.

Quantidade de Bytes	Nome	Descrição
80	Cabeçalho do bloco	Descrição
variável	Contador de transações	Contém um conjunto de informações de cabeçalho

variável	Transações	Contém todas as transações do bloco

Fonte: Drescher (adaptado pelo autor).

A Tabela III demonstra os campos que compõem o cabeçalho de um bloco integrante da Blockchain/Bitcoin.

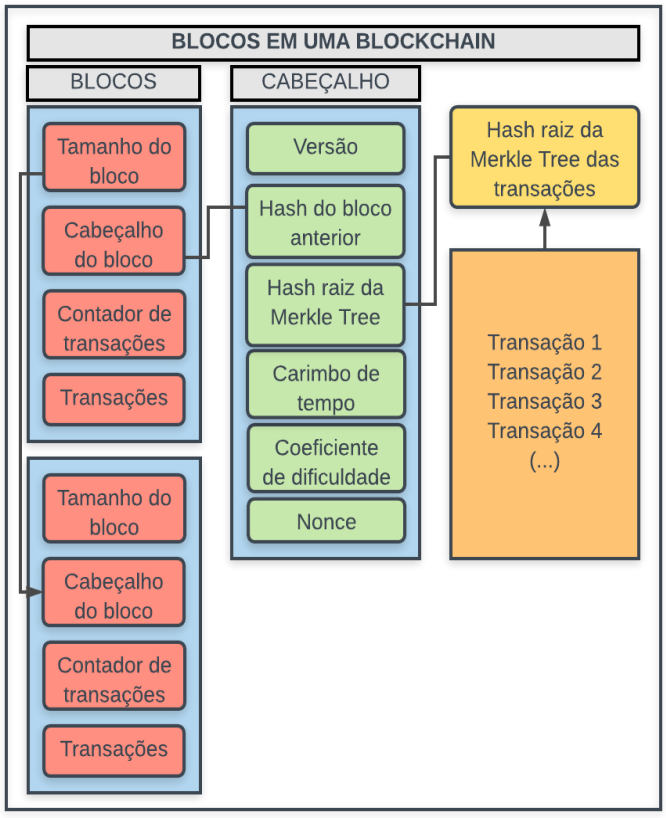
Tabela III - Estrutura de um cabeçalho Blockchain.

Quantidade de Bytes	Nome	Descrição
4	Versão	Contém a versão do bloco que define as regras de validação a serem seguidas
32	Hash do bloco anterior	Contém um hash SHA256 duplo do bloco anterior
32	Hash raiz da Merkle Tree	Contém um hash SHA256 douplo da Merkle Tree que armazena todas as transações do bloco
4	Carimbo de tempo (timestamp)	Contém a data e hora de criação do bloco
4	Coeficiente de dificuldade	Contém o coeficiente de dificuldade
4	Nonce	Contém um número arbitrário que os mineradores atualizam repetidamente para gerar um hash que respeite o limite exigido pelo coeficiente de dificuldade

Fonte: Drescher (adaptado pelo autor).

Na Figura 8, por sua vez, estão ilustrados os blocos de uma blockchain interligados por meio de seus cabeçalhos (hashs) e, também, de um dos cabeçalhos dos blocos.

Figura 8 - Blocos em uma Blockchain.



Fonte: Drescher (adaptado pelo autor).

Como demonstrado na Figura 9, uma blockchain é uma cadeia de blocos, onde cada bloco é conectado ao bloco imediatamente anterior por meio de uma referência ao seu hash de cabeçalho. Uma outra função dessa conexão, por meio de cabeçalhos, é assegurar que nenhuma transação pode ser modificada a menos que o bloco que a registre e todos os demais blocos que o sucedem, também sejam alterados.

É interessante destacar que o primeiro bloco de uma blockchain não é conectado a um bloco prévio e é conhecido como *"genesis block"*, definido inalteradamente, ou seja, *hardcoded* no código-fonte da Bitcoin, especificamente no arquivo chainparams.cpp. A Figura 9 ilustra parte do código que cria o "*genesis block*" da blockchain da Bitcoin. No caso, a função CreateGenesisBlock retorna um objeto CBlock, que é uma implementação de CBlockHeader, que representa o cabeçalho de um bloco da blockchain.

Figura 9 - Criação do "genesis block" no arquivo chainparams.cpp da Bitcoin.

```
static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce,uint32_t nBits,
        int32_t nVersion, const CAmount& genesisReward){
  const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink ...";
  const CScript genesisOutputScript = CScript() << ParseHex("04678afdb...") << OP_CHECKSIG;
  return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion,
         genesisReward);
}
```

Fonte: https://github.com/bitcoin

Na blockchain da Bitcoin há, também, os blocos obsoletos, do inglês *stale blocks* e os órfãos, *orphaned blocks*. Os primeiros são assim classificados por serem minerados (explicado em 2.2.3) com sucesso, porém não entram na cadeia de blocos porque outros mineradores conseguiram adicionar blocos primeiro. Blocos órfãos (*orphaned* ou *detached blocks*) são blocos válidos que não fazem parte da cadeia de blocos. Ocorrem geralmente quando dois mineradores produzem blocos ao mesmo tempo, ou quando um atacante (com poder computacional suficiente) tenta reverter transações.

Novos blocos são adicionados à blockchain da rede Bitcoin aproximadamente a cada 10 minutos e o coeficiente de dificuldade é ajustado dinamicamente a cada 2016 blocos para que a média de blocos adicionados por hora seja uma constante (ANTONOPOULOS, 2010).

2.2.2 Transações

A rede Bitcoin provê proteção contra duplo gasto (*double spending*) por meio da utilização de regras fortes de validação das transações e por meio da mineração. Os blocos são adicionados à blockchain somente após a checagem de terem respeitado as regras de inclusão e resolverem o chamado *Proof of Work* (PoW). Duplo gasto (double spending) é um fenômeno que pode acontecer pela utilização de uma mesma bitcoin já utilizada em outra transação. Essa falha é resolvida através do mecanismo de *Proof of Work (PoW)*, que consiste na solução de um problema matemático por quem for eleito para adicionar o próximo bloco na blockchain.

Dado que as funções hash utilizadas nas operações dos blocos são criptograficamente seguras, a única forma de solucionar o problema matemático requisitado pelo mecanismo de *Proof of Work* é a força bruta (testar todas as combinações de hash possíveis), ou seja, em termos probabilísticos, quem consegue solucionar o problema primeiro é quem possui o maior poder computacional naquele dado momento (para efetuar os cálculos de hash). Esses solucionadores de *Proof of Work* são conhecidos como mineradores (de Bitcoin) (NARAYANAN, 2010).

2.2.3 Mineração

Mineração é o processo de utilização intensa de recursos pelo qual novos blocos são adicionados à blockchain. Blocos, como dito, contém transações que são validadas via processos de mineração pelos mineradores. Estes, em seu turno, são recompensados com moedas à medida que executam tarefas de mineração. Quando iniciada, a rede Bitcoin recompensava mineradores com 50 bitcoins; em 2012, esse valor foi reduzido para 25 moedas, e em 2016 o valor da recompensa desceu para 12 moedas e meia (12,5 bitcoin). Estima-se que haverá outro reajuste em Julho de 2020, que fará a recompensa por mineração ser de apenas 6 bitcoins (ROBERTS, 2018).

São gerados cerca de 144 blocos por dia (cerca de 1.728 bitcoins), porém, aproximadamente no ano de 2140 as quase 21 milhões de bitcoins serão finalmente criadas e nenhuma bitcoin nova poderá ser gerada a partir de então. Os

mineradores de bitcoin, no entanto, ainda poderão obter lucro a partir do ecossistema Bitcoin, cobrando taxas das transações efetuadas.

Uma vez que um novo minerador conecta à rede Bitcoin, ele faz uma cópia (*download*) da blockchain inteira por meio de uma requisição de blocos de histórico para os demais mineradores.

Entre as tarefas dos mineradores, estão:

- Validação de transações: transações difundidas (*broadcasting*) pela rede são confirmadas por full nodes (nós da rede Bitcoin que verificam todas as regras de validação necessárias) pela verificação e validação de assinaturas e saídas.

- Validação de blocos: mineradores e full nodes validam blocos confirmando se os mesmos respeitam as regras da rede, como por exemplo a verificação do valor “nonce” a cada transação.

- Criação de novos blocos: mineradores podem criar novos blocos pela combinação de transações difundidas pela rede após a devida validação.

- Executar Proof of Work (PoW): é a competição para a geração de um novo bloco por meio da solução de um desafio matemático lançado aos mineradores. Na Bitcoin, o *Proof of Work* é resolvido quando um minerador encontra um valor nonce, cujo valor de hash do cabeçalho do bloco seja menor que um dado coeficiente de dificuldade (target).

- Receber recompensas: uma vez que resolve o desafio matemático, imediatamente o minerador envia o bloco validado para difusão na rede, para verificação e aceitação dos outros mineradores. Uma vez que o bloco é aceito na rede, o minerador que o enviou receberá, como prêmio, 12.5 bitcoins (em tempos de hoje).

O processo de mineração é efetuado por meio de um algoritmo, que consiste nos seguintes passos:

1. O hash do último bloco da blockchain é lido a partir da rede Bitcoin.

2. Potenciais transações (a serem validadas) são juntadas em um potencial novo bloco.

3. É computado o hash duplo do cabeçalho do bloco com um valor nonce e o hash do bloco anterior da blockchain utilizando-se o algoritmo SHA256.

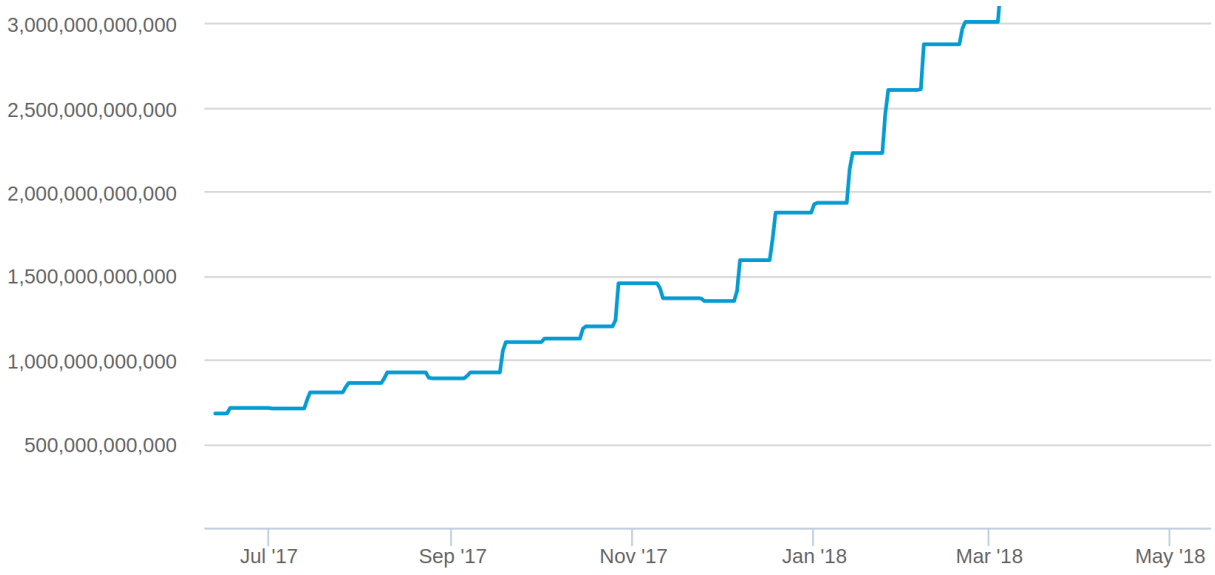
4. Se o hash resultante é menor que o atual coeficiente de dificuldade (*target*), o processo para.

5. Se o hash resultante é maior que o atual coeficiente de dificuldade (*target*), então repete-se o processo com o incremento do valor *nonce*.

O coeficiente de dificuldade utilizado na mineração tem aumentado com o passar do tempo; e bitcoins que poderiam ser mineradas por simples CPUs disponíveis em notebooks agora requerem centros computacionais inteiramente dedicados a resolver desafios matemáticos.

No gráfico exibido pela Figura 10 é possível observar o aumento da dificuldade na mineração com o passar do tempo.

Figura 10 - Aumento do coeficiente de dificuldade no tempo.



Fonte: https://blockchain.info/charts/difficulty

2.3 Segurança em Blockchain

Como toda tecnologia, as implementações baseadas em Blockchain possuem vulnerabilidades e vetores de ameaças que podem comprometer suas estruturas e dados que armazenam. Nos tópicos a seguir são detalhados algumas das principais adversidades que podem ser enfrentadas por essas redes de dados.

2.3.1 Ataque de 51%

Esse ataque refere-se a investidas de agentes maliciosos contra redes blockchain por grupos de mineradores, controlando mais de 50% do poder computacional de mineração (*mining hashrate*) do restante da rede. Sob esse prisma, os atacantes poderiam estar aptos a evitar que novas transações fossem validadas na blockchain, permitindo, também, que pagamentos entre alguns ou todos os usuários da rede fossem bloqueados. Enquanto controlando a rede por meio desse ataque, poderiam também reverter transações já completadas, resultando em gasto duplo (*double spending*) de moedas. Entretanto, autores desse tipo de fraude não poderiam criar novas moedas e nem tampouco alterar bloco já existentes, a despeito dos demais danos potencialmente possíveis.

As criptomoedas Krypton e Shift, ambas baseadas em blockchain, sofreram distúrbios por conta de uma variante do ataque 51% em agosto do ano de 2016. A exploração dessa vulnerabilidade de rede consistiu de duas fases: a primeira foi o aumento de poder de processamento da rede para mais da metade do poder dos demais nós em prol de reverter transações e gerar duplicidade no gasto de moedas, e a segunda fase foi atacar, por meio de ataques de negação de serviço (DDoS), os demais nós da rede. No caso da Bitcoin, o ataque de 51% torna-se inviável, por conta de seu alto poder computacional, que requereria de atacantes, atualmente, bilhões de dólares para processar duplos gastos, por exemplo (ANTONOPOULOS, 2018).

Por outro lado, recentemente a Bitcoin Gold perdeu cerca de 18 milhões de dólares em um ataque de 51%. Essa rede é uma ramificação (*fork* ou *spin-off*) da Bitcoin original, que compartilha muito do mesmo código-fonte e trabalha de maneira similar à sua ancestral, com mineradores de Bitcoin Gold contribuindo com poder computacional para processar novas transações que surgem em sua blockchain. Isso significa que a Bitcoin Gold enfrenta praticamente as mesmas ameaças e possui as mesmas vulnerabilidades da Bitcoin original, mas sem as proteções oriundas dos grupos de pessoas e corporações que fornecem poder computacional à blockchain de sua irmã mais velha.

A possibilidade de ocorrência de ataques de 51% tem sido uma das preocupações de instituições bancárias, de tecnologia, entre diversas outras, quando consideram a utilização de blockchain em seus processos. Porém, caso ocorra de um minerador possuir mais de 50% do poder de processamento na rede, pesquisadores acreditam que seria mais lucrativo para esse agente receber as recompensas da mineração em vez de sabotar a estrutura blockchain vigente (NAKAMOTO, 2008). Um outro ponto-de-vista com o fito de dirimir ataques como esse se dá pela utilização de rede blockchain operando em esquemas centralizados (UK GOVERNMENT, 2015), embora a adoção dessa estratégia retire uma das principais características das blockchains públicas, a descentralização.

2.3.2 Chaves e aleatoriedade

Uma das vulnerabilidades presentes no algoritmo DSA e seus derivados, como o *ECDSA - Elliptic Curve Digital Sign Algorithm*, implementado na Blockchain, utilizados para assinar dados digitalmente, é o acesso não autorizado de suas chaves criptográficas. Para evitar esse problema, é necessário que a fonte randômica que alimenta o algoritmo seja eficiente. Exatamente por essa razão, o PGP (*Pretty Good Privacy*) e outras soluções que empregam o DSA pedem aos seus utilizadores que façam movimentos com seus cursores de mouse ou que fiquem apertando teclas de maneira arbitrária em seus teclados durante a geração de chave do algoritmo (THOMAS, 2003), a fim de evitar o vazamento da chave privada e com isso comprometer a segurança das operações como um todo.

Em se tratando da blockchain da criptomoeda Bitcoin e de outras soluções digitais, entende-se que a maior fonte de vulnerabilidades não se encontra na infraestrutura tecnológica (algoritmos, protocolos, etc.), mas no elo mais fraco, o ser humano. Pesquisas demonstram que pelo menos 10% dos usuários de redes Bitcoin já sofreu perdas de moedas eletrônicas ou outros valores similares (KROMBHOLZ, 2016) por conta, a título exemplificativo, de ataques direcionados por meio dos chamados *endpoints*, quer dizer, as camadas de acesso “casca” que intermediam os utilizadores com a própria rede, como por exemplo, uma corretora de Bitcoin falsa ou fraudulenta.

2.3.3 Ausência de padrões e regulações

Uma das ameaças que podem levar à exploração de vulnerabilidades no mundo da tecnologia Blockchain é a ausência de padrões de indústria e de regulações governamentais que gerenciem as atividades daqueles que a desenvolvem e a mantém. Certo é que a mera menção à criação de regras põe os mais puristas em estado de alerta. Entretanto, sob pontos-de-vista contrários, uma versão sem intermediários e descentralizada de blockchain como a Bitcoin pode ser considerada uma antítese aos preceitos tão em voga de Governança e Compliance, exatamente por seu caráter autônomo e sem regulação (FORBES, 2017).

Um dos argumentos de quem é contrário à regulação são as vantagens que dizem respeito ao uso do anonimato nas blockchains e que serviu de alimento para seu crescimento nos últimos anos. Enquanto outros, especialmente reguladores do governo e instituições financeiras, argumentam que as criptomoedas devem ser reguladas, sob pena de não efetividade jurídica, intempéries na esfera econômica, favorecimento e promoção da criminalidade, entre outros tantos campos afetos a esse contexto. Outro aspecto diz respeito à própria tecnologia, pois a ausência de padrões acarreta, por exemplo, em dificuldades de compatibilidade entre soluções, além de aumentar os riscos de segurança relacionados às mesmas (DESHPANDE, 2017).

3 BLOCKCHAIN APLICADA À EDUCAÇÃO

3.1 Aplicações diversas

A seguir são listadas e explicadas diversas aplicações, em diversas partes do mundo, que utilizam tecnologia Blockchain como infraestrutura para armazenamento de seus dados, de maneira a promover a transparência e a segurança.

3.1.1 Emissão de certificados à prova de falsificação

A Holberton School, em San Francisco (EUA), uma escola de desenvolvimento de software que oferece educação baseada em projetos como alternativa aos cursos universitários, tem usado Blockchain para armazenar e entregar seus certificados emitidos. Essa estratégia é vista como uma medida para evitar a utilização de certificados falsificados. A criptografia e a autenticação em dois fatores são usados para criar, assinar e adicionar os certificados ao banco de dados blockchain. A escola ainda dá cópias em papel aos alunos, mas é gerado um número de identificação descentralizado (*DCN - Decentralized Clearing Number*) para os certificados, criado pelo sistema e que permite a autenticação pelos empregadores (HOLBERTON SCHOOL, 2015).

O *Massachusetts Institute of Technology (MIT)* também tem adotado Blockchain para a emissão de seus certificados por meio de um projeto chamado *“Blockchain certificates”* (MIT MEDIA LAB, 2016). O projeto é composto por um conjunto de ferramentas que permitem o armazenamento e o gerenciamento de credenciais digitais. Uma iniciativa de código aberto desenvolvida pelo mesmo instituto está disponível para uso por qualquer interessado, inclusive para fins comerciais, no site http://www.blockcerts.org. A comunidade Blockcerts fornece, de maneira aberta (*open-sourcing*), bibliotecas de software, ferramentas e aplicações prontas que permitem a implementação de ecossistemas computacionais descentralizados, padronizados e seguros por meio da Blockchain e tecnologias

relacionadas. Alguns exemplos de instituições que usam certificados criados e mantidos com ferramentas da comunidade Blockcerts são: o próprio MIT (certificando seus alunos), a empresa Learning Machine (que gera certificados para seus empregados), e o Laboratorio para la Ciudad, do México, que certifica participantes de seus workshops (BLOCKCERTS, 2016).

Outra instituição educacional que adotou certificados armazenados e gerenciados em blockchains foi a Universidade de Nicósia, que relata que nenhuma outra tecnologia, além da Blockchain, foi utilizada para o projeto, que dessa forma qualquer indivíduo pode autenticar certificados emitidos pela universidade sem contato com a instituição, e que os registros, por estarem distribuídos, permanecerão disponíveis mesmo que o site esteja fora do ar ou que a universidade venha a não mais existir (UNIVERSITY OF NICOSIA, 2016).

3.1.2 Registros de proficiência

A *Sony Global Education Inc*, do conglomerado de empresas da Sony, anunciou que adaptou a tecnologia blockchain ao campo educacional e desenvolveu uma tecnologia que permite o compartilhamento aberto e seguro de registros de proficiência e progresso acadêmico de seus alunos. A empresa desenvolveu uma tecnologia que aplica a blockchain ao campo educacional, alavancando as propriedades seguras do blockchain para realizar a transmissão criptografada de dados - como registros de proficiência acadêmica de um indivíduo e medidas de progresso. A tecnologia tem o potencial de realizar um sistema de infraestrutura totalmente novo para compartilhar registros de forma segura na rede, abrindo novas possibilidades de armazenamento eletrônico de registros acadêmicos e novas formas de avaliá-los. Por exemplo, depois de fazer um exame para demonstrar seu nível de proficiência acadêmica, um indivíduo poderia requisitar à organização que aplicou o teste para compartilhar os resultados com uma ou mais organizações de avaliação terceirizadas.

À medida que os paradigmas da educação evoluem, espera-se que a inovação tecnológica diversifique as formas em que os testes são projetados e os indivíduos são avaliados. Com esta diversificação e as mudanças que ela traz,

diferentes instituições de avaliação podem vir a utilizar os resultados dos testes dos indivíduos de diferentes maneiras, cada um de acordo com seus próprios métodos de avaliação. O gerenciamento aberto e seguro de dados acadêmicos será possível através da adoção de programas de aplicação que alavanquem a nova tecnologia da *Sony Global Education*, levando ao surgimento de novos serviços educacionais no futuro. Com esta infraestrutura instalada, cada organização avaliadora envia registros de teste de um indivíduo para avaliar os resultados e calcular uma pontuação de acordo com seus próprios métodos. Além disso, a criação de uma infraestrutura aberta e segura tem o potencial de atrair muitas instituições educacionais para a rede, resultando em alta credibilidade na administração de testes. Finalmente, dada a sua força como um protocolo de troca de dados aberto, a nova tecnologia da *Sony Global Education* pode ser aplicada não só na arena educacional, mas também em uma gama mais ampla de indústrias, desde a área médica até serviços ambientais e energia. A empresa vê o blockchain como uma tecnologia básica que tem o potencial de moldar, significativamente, a paisagem educacional do futuro (SONY, 2016).

3.1.3 Portfólios eletrônicos

Em um futuro não muito distante, o gerenciamento e a validação de qualificações não acontecerá, exclusivamente, pelas mãos das instituições de ensino ou dos empregadores, permitindo que professores, estudantes e outros interessados manuseiem essas informações a partir de qualquer ponto do planeta de maneira distribuída, segura e com maior acessibilidade. O atual modelo centralizado de gerenciamento de informações está tornando-se insustentável: o aprendizado cada vez menos acontece dentro das quatro paredes das salas de aula das instituições de ensino, dada a maior adoção de plataformas online de aprendizagem, comunidades de colaboração, uso de dispositivos cada vez mais portáteis e avançados, etc.

No mundo em rede, com o poder digital do século XXI, os provedores de educação, muitas vezes, não têm os meios e a capacidade de cobrir a gama de atividades que os alunos envolvem, o que atesta suas conquistas, conhecimentos e

habilidades. Nesse contexto, as tecnologias blockchain podem conter uma resposta para reunir os resultados desta nova realidade de aprendizagem distribuída.

Em um cenário de educação típico, os alunos aprendem por meio de uma série de atividades pedagógicas e são avaliados e recebem *feedback* dos professores. A aprendizagem ocorre presencialmente, ou online (ou ambos), tudo sob o controle de uma instituição educacional que presta qualidade, credibilidade, governança e funções administrativas. Enquanto a instituição educacional emite documentação que certifica a realização de marcos importantes de estudo (certificados, diplomas, etc.), os alunos são responsáveis por preservar e armazenar os trabalhos realizados em seus cursos (ensaios, experimentos de laboratório, projetos, softwares, etc.), além de informações manifestadas pelos professores para uso posterior (para mostrar aos potenciais empregadores, solicitar um programa de estudo, estágio, bolsa de estudos, etc.). Isso cria uma alta sobrecarga para os alunos, pois os mesmos precisam acompanhar, organizar e arquivar com segurança as informações relevantes, que, muitas vezes, incluem muitos trabalhos individuais, armazenados em mídias diferentes (e-mails, arquivos de imagem, arquivos de som, códigos-fonte, etc.), criados ao longo de meses ou anos de estudo. Ao mesmo tempo, o destinatário dessas informações (um potencial empregador, o time de admissão de instituições de ensino, etc.) tem meios muito limitados para verificar as evidências apresentadas ou para avaliar o candidato, pois também não sabem se os trabalhos realizados pelo candidato têm pouco ou nenhum contexto de relevância para as qualificações exigidas e para o conjunto de habilidades necessárias.

Os ePortfolios baseados em Blockchain podem enfrentar esses desafios através do desenvolvimento de uma plataforma aberta, descentralizada, peer-to-peer, em que o controle e a responsabilidade por esse fluxo de informação são radicalmente desintermediados, separando instituições educacionais de estudantes e professores, porém atendendo a todos. Isso é possível usando-se registros digitais distribuídos em blockchains, permitindo o gerenciamento seguro e resiliente de dados distribuídos em combinação com técnicas de análise de dados que agregam escala e flexibilidade à forma como os níveis de qualificação são definidos e concedidos (OPEN BLOCKCHAIN, 2014).

3.1.4 Redes comunitárias de alunos e profissionais

A *Blockchain Education Network*, anteriormente conhecida como *College Cryptocurrency Network*, é uma rede global de estudantes e jovens profissionais que lideram o movimento da educação usando blockchains. A Blockchain Education Network organiza eventos intercampus, hackathons locais e globais e fornece recursos educacionais para estudantes que iniciam seus estudos em seus câmpus. A rede *College Cryptocurrency Network (CCN)* mudou recentemente de nome para *Blockchain Education Network (BEN)* para refletir as mudanças da indústria. A alteração de Cryptocurrency para Blockchain deu-se porque o escopo da indústria ficou mais amplo. O nome Cryptocurrency, por exemplo, estava mais ligado a dinheiro e transações financeiras. O nome College (Faculdade) foi mudado para Education (Educação) para alcançar, também, aqueles que já se formaram e pretendem continuar interagindo com *Blockchain Education Network*. O projeto iniciou como College para inicialmente agregar participantes de faculdades, mas atualmente o foco é englobar crianças que estão no ensino médio, estudantes das universidades, crianças que abandonaram os cursos ou recém-formados que, ainda, estão interessados em participar do movimento de educação blockchain.

Recentemente, o processo de inscrição passou por reformulação e tornou-se mais fácil para estudantes do ensino médio e graduação se juntarem à comunidade *Blockchain Education Network*. Assim que os alunos se inscrevem, são convidados para a comunidade privada, e uma vez que se formem e tornam-se ex-alunos, podem permanecer na rede. Os graduados que desejam participar da comunidade podem entrar em contato, e após uma análise curricular podem ser convidados para agregar valor à rede educacional. Este processo tem sido bem-sucedido na criação de uma comunidade ativa que compartilha ideias de educação disruptiva para seus membros e para suas faculdades ou escolas de origem. Todos usam seu nome real, adicionam uma imagem de seu rosto (avatar) e fornecem informações de seus vínculos a escolas ou faculdades, o que facilita o contato por parte de outros membros da comunidade, como líderes estudantis da rede. Atualmente, a comunidade executa atividades com membros oriundos dos Estados Unidos e Canadá, embora haja uma participação pequena, mas crescente, de estudantes da Ásia e da Europa.

A colaboração na rede acontece em um ambiente em que os alunos podem facilmente abrir um diálogo com os líderes estudantis que acessam sites de notícias populares da Bitcoin e que tratam de projetos que estão acontecendo em campus universitários do mundo todo. O sistema permite que os alunos tragam casos de sucesso de seu câmpus e interajam diretamente com os líderes estudantis presentes na comunidade online privada da *Blockchain Education Network*. Há, também, a criação de eventos que encorajam os estudantes nos chamados “clubes” de Bitcoin e blockchain a colaborar uns com os outros com mais frequência para que a *Blockchain Education Network* permaneça atualizada e com os projetos de outros clubes e para que as ideias do universo blockchain se propaguem com maior velocidade e acessibilidade pelos demais membros da rede. A título de exemplo, há um evento chamado *Blockchain Madness*, que coloca 3 câmpus nos Estados Unidos e 3 câmpus no Canadá um contra o outro em um torneio de blockchain com fases eliminatórias baseadas em projetos. Embora o evento seja bastante competitivo, o mesmo cria diálogos interessantes entre essas comunidades, motivando os clubes estudantis a se reunirem em prol de um objetivo em comum e incentivando a futura colaboração entre os câmpus. Entre os participantes estão os câmpus que acolhem clubes Bitcoin / blockchain ativos e que desejam mostrar seus projetos no cenário internacional. Alguns clubes como o MIT, Berkeley e a Universidade de Toronto já estão estabelecidos nesse tipo de evento, enquanto os outros, de diversas localidades, estão constantemente manifestando interesse em participar. Outro evento que é organizado e mantido pela *Blockchain Education Network* é o hackathon global, que foi baseado no sucesso oriundo de outro evento chamado *Borderless Block Party Hackaton*. A *Blockchain Education Network* é mantida e acessível pelo endereço eletrônico https://blockchainedu.org/ (BITCOIN MAGAZINE, 2015).

3.1.5 Gamificação na educação

A gamificação na educação, ou gamificação no aprendizado, é, alguma vezes, descrita usando outros termos: pensamento baseado em jogos (*gameful thinking*), princípios de jogos para a educação, design baseado em motivação,

design de engajamento, etc. É diferente da aprendizagem baseada em jogos, na medida em que não envolve estudantes produzindo seus próprios jogos, ou jogando videogames comerciais. Funciona sob o pressuposto de que o tipo de engajamento que os jogadores experimentam com os jogos pode ser traduzido para um contexto educacional voltado para os objetivos de facilitar a aprendizagem e influenciar o comportamento dos alunos. Uma vez que os jogadores, voluntariamente, passam inúmeras horas jogando jogos e resolvendo problemas, pesquisadores e educadores têm explorado formas de aproveitar o poder de motivação dos videogames e aplicá-los à sala de aula.

A gamificação no aprendizado envolve a incorporação de elementos de jogos para motivar os alunos. Alguns desses elementos incluem os seguintes:

- Narrativa.
- Retorno imediato (immediate feedback).
- Diversão.
- Aprendizado esquematizado com desafios focados no desenvolvimento.
- Domínio das técnicas utilizadas.
- Indicadores de progresso.
- Interação social entre os jogadores/aprendizes.
- Controle do jogo pelo usuário/aprendiz.

Uma sala de aula que possui alguns dos elementos acima pode ser considerada “gamificada”. As melhores combinações dos elementos citados são as que criam engajamento dos jogadores, consideram as necessidades peculiares dos aprendizes e fazem mais do que apenas usar pontos e níveis para motivá-los.

Dentre os benefícios do uso da gamificação, podemos citar:

- Os aprendizes sentem pertencimento ao processo de aprendizagem.
- Maior atmosfera de relaxamento em caso de falha, haja vista que os aprendizes podem simplesmente tentar novamente.
- Mais diversão nas aulas.
- O aprendizado torna-se mais visível por meio dos indicadores de progresso.
- Os aprendizes podem experimentar diversas identidades por meio de diferentes perfis disponíveis no jogo.
- Os aprendizes sentem-se mais confortáveis em ambientes gamificados.

Os sistemas de gamificação mais efetivos fazem uso de outros elementos, a depender de cada caso, para fazer com que os aprendizes mantenham o interesse e o envolvimento durante o processo de aprendizagem (LEARNING THEORIES, 2016).

A tecnologia Blockchain também tem sido aplicada com a gamificação para proporcionar métodos mais eficazes de aprendizado, como na iniciativa de colaboração *DBS Accelerator*, criada e mantida pelo DBS Bank e a Nest, esta última uma incubadora de startups, ambos de Hong Kong, China. (FINEWS, 2016).

4 ARMAZENAMENTO DE CERTIFICADOS EM BLOCKCHAIN PARA A UNIVERSIDADE FEDERAL DO TOCANTINS

O foco desse trabalho é o armazenamento de certificados emitidos pela Universidade Federal do Tocantins em uma blockchain Multichain, visando escalabilidade, segurança e economia de recursos (a solução é código aberto, e por isso, sem custos à instituição). Além disso, esse projeto pretende, principalmente, evitar a falsificação de certificados emitidos pela Universidade Federal do Tocantins por meio da validação dos mesmos, por qualquer interessado, na blockchain a ser criada para esse fim.

Diferentemente dos projetos Open Standard for Blockchain Credentials, criados e mantidos pelo MIT - Massachusetts Institute of Technology, e do repositório de certificados da Holbert School, de San Francisco (EUA), que usam, mediante pagamento de determinados valores, a blockchain pública e *permissionless* da Bitcoin, esse projeto é baseado em uma blockchain privada e *permissioned* da solução de código aberto Multichain, que permite facilidade de implantação, manutenção e escalabilidade, sem custos, na infraestrutura já existente na Universidade Federal do Tocantins.

4.1 Classificação das blockchains

Como demonstrado nos capítulos anteriores, a tecnologia Blockchain é uma espécie de banco de dados distribuído projetado para processar e armazenar transações. E, embora a maioria das implementações blockchain da atualidade sejam utilizadas em operações financeiras (TOKENMARKET, 2018), tais infraestruturas servem para armazenar informações diversas, como carimbos de tempo (*timestamp*) de documentos com vistas a proteger sua integridade.

Em se tratando de privilégios de acesso, as blockchains podem ser classificadas em públicas e privadas. Uma blockchain pública é aquela em que não há restrições para a leitura de dados da blockchain e nem para inclusão de transações em sua infraestrutura. Um dos mais famosos exemplos de

implementação pública de blockchain é a criptomoeda Bitcoin. Diferentemente, as blockchains privadas exigem, por meio de controle de acesso, privilégios determinados para usuários específicos, tanto para leitura dos dados existentes na blockchain, quanto para incluir novos dados, ou seja, transações (GARZIK, 2015).

Uma das principais críticas à blockchain da Bitcoin é que a mesma é impossível de ser regulada por órgãos governamentais, além de ser lenta e tecnicamente inferior a implementações de blockchain mais recentes (GUADAMUZ, 2015). As instituições bancárias, por exemplo, estão interessadas em utilizar blockchain em seus ambientes computacionais com vistas a dar maior segurança no armazenamento de seus dados, em principal às transações bancárias de seus clientes. Nesse caso, os bancos terão que implantar seus próprios sistemas distribuídos, é dizer, suas próprias versões de blockchain, que serão, além de privadas, gerenciadas sob regras de utilização internas, inaugurando outra classificação: a das blockchains reguladas, ressalvando-se que esta, também, podem ser implementadas de maneira pública (GUEGAN, 2017). Um exemplo de versão de blockchain em uso por cerca de 25 bancos internacionais foi criada pela empresa norte-american R3 CEV (https://www.r3.com).

Outra classificação aplicável às blockchains diz respeito à permissão para validar blocos que serão inseridos na rede. Quando a cadeia de blocos é configurada para que somente determinados usuários tenham privilégios de validação de blocos, essa blockchain é chamada de *permissioned*, ou seja, possui regras de permissão (atinentes, repita-se, à validação de blocos). Por outro lado, quando a validação de blocos pode ser feita por qualquer usuário da rede, tem-se uma blockchain do tipo *permissionless*, ou seja, uma rede onde qualquer interessado pode ingressar e minerar dados. Novamente a Bitcoin figura como exemplo notório de blockchain *permissionless* (GARZIK, 2015).

Uma diferença de performance entre blockchains *permissionless* e *permissioned* é que as primeiras usam mineração baseada em *Proof of Work* (PoW), a qual exige poder computacional dos mineradores e a torna mais lenta que as blockchains do tipo *permissioned*. Estas não precisam de mineração baseada em poder computacional para alcançar o consenso das transações geradas por seus

usuários, haja vista que são todos previamente cadastrados no sistema e por essa razão, conhecidos e com poderes de mineração garantidos (ANTONOPOULOS, 2016). Alguns algoritmos de consenso geralmente utilizados em blockchains *permissioned* são o RAFT, o Paxos e o PBFT.

Outras questões relevantes a serem consideradas quando da escolha de qual tipo de blockchain deve-se utilizar dizem respeito à privacidade dos dados, à entidade responsável pela rede, à escalabilidade e ao controle de acesso. Em blockchains públicas os dados são acessíveis por qualquer interessado, e caso isso não seja desejado o ideal é a adoção de uma blockchain privada. Porém, quando da escolha desta, necessariamente deverá haver uma entidade centralizadora, que manterá a rede e tirará o caráter descentralizado, característica tipicamente pertencente a blockchains públicas. No tocante à escalabilidade, saem-se melhor as blockchains *permissioned* em relação às *permissionless*, por não precisarem, incrementalmente, de poder computacional para processar suas transações. Finalmente, se o objetivo é o controle de acesso refinado, novamente a melhor escolha dar-se-ia pelas blockchains privadas e permissioned, que atribuem privilégios em nível de usuários, para leitura e escrita de dados, e em nível de mineradores, para validação de blocos (ANNAMALAI, 2016).

Abaixo, a tabela IV com a comparação das implementações públicas e privadas da tecnologia Blockchain.

Tabela IV - Comparativo entre implementações de Blockchain.

Característica	Blockchain Pública	Blockchain Privada
Disponível em código aberto	X	X
Possui controle de leitura		X
Possui controle de escrita		X
Facilidade de regulamentação		X
Possui controle de validação de blocos		X
Exige Proof of Work (PoW)	X	
Possui privacidade dos dados		X
Descentralizada	X	
Garante imutabilidade dos dados	X	X
Garante persistência dos dados	X	X

Fonte: Drescher (adaptado pelo autor).

Repise-se que, para esse projeto, será utilizada a solução de código aberto Multichain, implementação de blockchain privada e *permissioned*, que resultará em economia de recursos para a Universidade Federal do Tocantins.

4.2 Multichain

Multichain é uma plataforma de código aberto para criação de blockchains privadas. Ao usuário é permitido definir parâmetros da blockchain a ser criada, e esta, por sua vez, permite o armazenamento de diversos tipos de conteúdos digitais, chamados de *assets*, ou “ativos”, na documentação da solução. A plataforma está disponível para download e instalação em máquinas Windows e Linux, e seu código-fonte pode ser acessado no Github, precisamente em https://github.com/MultiChain/multichain. A Multichain estende a APIs (*Application Programming Interfaces*) da Bitcoin e tem um formato de protocolo e transação similar. Um dispositivo cliente (nó) da Multichain pode atuar como nó das redes Bitcoin e Bitcoin testnet (esta é uma versão da Bitcoin utilizada apenas para testes - suas moedas não possuem valor algum, por sinal). A seguir algumas das principais características da plataforma de código aberto Multichain.

Para blocos criados usando Multichain, o protocolo permite aos criadores determinar quais permissões um novo participante terá sem que precise recebê-las diretamente de um dos administradores da rede. Quando da inicialização da blockchain, seus criadores determinam os poderes dos administradores, bem como se qualquer interessado poderá se conectar, sem restrições, à rede. Administradores podem também controlar dinamicamente as permissões para usuários específicos da blockchain enquanto esta está em funcionamento. Tais permissões incluem ações de envio, recebimento e criação de conteúdo (assets), assim como criação de blocos. Decisões posteriores de alteração de permissões são feitas por meio de consenso entre os administradores. A proporção de administradores que devem aceitar a modificação de privilégios dos usuários é definida antes da blockchain entrar em funcionamento.

Por seu caráter de blockchain privada, a Multichain resolve as questões atinentes à mineração e privacidade de dados por meio de um controle de acesso

integrado à própria solução. A solução objetiva: a) assegurar que toda e qualquer atividade na blockchain seja visível apenas para participantes autorizados, b) permitir a gerencia de privilégios e definições de quais transações são permitidas na rede, e c) permitir que a mineração ocorra sem *Proof of Work (PoW)* e, com isso, recursos computacionais e energéticos não precisem ser alocados. Além disso, a Multichain permite que várias blockchains sejam implantadas em um mesmo servidor e que vários servidores trabalhem em conjunto para manter a rede.

Outro aspecto levado em consideração para a escolha da Multichain como solução a ser adotada para esse projeto é que a mesma deriva (via *fork*) do código oficial da blockchain Bitcoin, e, por conseguinte, sua manutenção e atualização são praticamente transparentes para a comunidade de desenvolvedores mundial, resultando em melhor escalabilidade e maior compatibilidade com os padrões e infraestruturas existentes. A tabela V detalha alguns dos recursos presentes na implementação de blockchain de código aberto Multichain.

Tabela V - Recursos da Multichain.

Recurso	Informações
Estabilidade	A Multichain é um fork da blockchain da Bitcoin, e por isso herda sua estabilidade, validada pela chamada Internet Aberta (pública).
Facilidade de uso	A criação de uma blockchain ou de várias blockchains na Multichain leva apenas alguns minutos. Não utiliza container externo, apenas três executáveis e um arquivo “leiame”.
Atualização constante	O time que mantém o projeto Multichain fomenta a participação dos usuários no que tange ao envio de sugestões e críticas, alterando o projeto conforme a necessidade.
Compatibilidade com a Bitcoin	A Multichain é projetada para ser compatível com a Bitcoin, inclusive sendo possível de ser configurada como um de seus nós de rede.
Modo interativo	Como uma bifurcação da Bitcoin, a MultiChain herdou a ferramenta bitcoin-cli, que foi renomeada para multichain-cli. Essa ferramenta fornece uma interface de linha de comando para a API JSON-RPC da MultiChain, permitindo que chamadas de API sejam enviadas a partir da linha de comando do sistema.
Validação sem Proof of Work (PoW)	O consenso na validação de blocos de dados na Multichain não é feito por meio de Proof of Work (PoW), economizando recursos computacionais e energia elétrica, além de taxas outras.
Streams	A Multichain possui objetos nativamente criados para o armazenamento de dados, chamados streams.
Controle de acesso	A Multichain possui controle de acesso em nível de usuário e de validação de blocos, fazendo-a ter natureza de blockchain privada e garantir privacidade no armazenamento dos dados.

Fonte: Multichain (adaptado pelo autor).

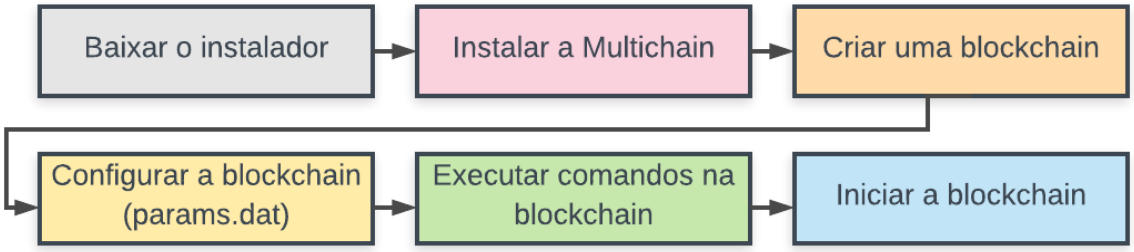
4.3 Aplicação da Blockchain Multichain

O primeiro passo para que se possa utilizar a Multichain é fazer sua instalação em algum computador servidor disponível, a partir do endereço de Internet https://www.multichain.com/download-install/, respeitando os requisitos abaixo:

- Linux: 64 bits; Distribuições compatíveis: Ubuntu 12.04+, CentOS 6.2+, Debian 7+, Fedora 15+, RHEL 6.2+.
- Windows: 64 bits; Versões compatíveis: 7, 8, 10, Server 2008 e posteriores.
- Mac: 64 bits; Versão compatível: OS X 10.12.
- 512 MB de memória RAM ou superior.
- 1 GIGA de espaço em disco ou superior.

Para esse trabalho, assume-se que o computador servidor a ser utilizado para instalação e configuração da tecnologia Multichain tem como sistema operacional o Linux Mint 64 bits, versão 18.3 codinome “Sylvia”, com 16 GIGA de memória RAM e 1 TERA de espaço em disco. Na figura 11 há a sequência de passos a serem executados para instalação e uso da Multichain.

Figura 11 - Sequência de instalação e uso da Multichain.



Fonte: adaptado pelo autor.

A instalação da Multichain é feita de maneira tradicional para ambientes Linux. Primeiro faz-se o download do pacote desejado, extrai-se o mesmo e copia-se os binários da Multichain para o diretório /usr/local/bin. Após a instalação deve-se criar uma ou mais blockchains executando-se o utilitário “multichain-util” (seguido de seus parâmetros). Com a execução desse comando será exibida a mensagem *“Blockchain parameter set was successfully generated. You can edit it in <caminho>/.multichain/chain1/params.dat before running multichaind for the first time”*, sinalizando que a nova blockchain foi criada com sucesso e indicando o caminho para seu arquivo de configuração (params.dat), que pode ser modificado com a utilização de um editor de textos tradicional, como o Vim. O params.dat é um arquivo de propriedades (*properties*) que possui diversas chaves (parâmetros) seguidos de seus valores.

Criadas as blockchains, pode-se iniciar a execução das mesmas com o utilitário “multichaind” (seguido de seus parâmetros). Caso objetive-se a alta disponibilidade da rede, outros servidores podem ser adicionados à blockchain. Esse procedimento é feito com a geração de um número de carteira (Wallet, que identificará o novo servidor na rede), com a autorização da nova carteira do servidor principal da blockchain, e, finalmente, com a conexão do novo servidor à rede.

A tecnologia Multichain permite que os comandos do usuário sejam enviados em *prompt* próprio, por meio de um modo interativo, disponível por meio do utilitário “multichain-cli”. A listagem a seguir demonstra alguns comandos auxiliares da Multichain, executáveis, também, em modo interativo, que visam facilitar sua utilização:

- getblockchainparams: Exibe uma lista com os parâmetros da blockchain (oriundos do arquivo params.dat).

- getpeerinfo: Exibe uma lista de clientes conectados à blockchain.

- grant: Dá permissões aos endereços dos nós.

- revoke: Revoga permissões dos endereços dos nós.

- listpermissions: Exibe uma lista de permissões que tenham sido explicitamente garantidas aos endereços dos nós.

- liststreams: Exibe uma lista contendo todos os streams da blockchain.

- listblocks: Exibe uma lista dos blocos constantes na blockchain.

- getnetworkinfo: Exibe uma lista contendo informações de rede, como a porta à qual o nó está conectado, bem como seu endereço IP.

- getinfo: Exibe informações gerais sobre o nó onde foi executado o comando e sobre a blockchain em execução.

- help: Exibe uma lista de comandos disponíveis ao usuário.

Streams na Multichain permitem que a blockchain seja utilizada como repositório de arquivos, provendo carimbo de tempo (*timestamping*), notarização (registro notarial) e imutabilidade. Uma blockchain Multichain pode conter inúmeros streams, onde os dados armazenados nos mesmos estarão armazenados, por conseguintes, em todos os nós que mantém a rede. Cada stream na Multichain é uma lista ordenada de itens, onde cada item possui as seguintes características:

- Um ou mais publicadores (publishers) que tenham assinado o item.

- Uma chave (key) com tamanho entre 0 e 256 bytes.

- Informações sobre transações do item e do bloco.

A criação de streams respeita o controle de acesso embutido na Multichain. Pode-se, por exemplo, criar streams que somente aceitem informações enviadas por usuários com privilégios de escrita. Frise-se que nomes de stream são sensíveis ao uso de minúsculas e maiúsculas (*case sensitives*) e não podem ser repetidos na mesma blockchain. Na Multichain, a ação de enviar arquivos (upload) para um

stream é chamada de “publicar” (itens), e “inscrever” é a operação que resulta em acesso ao stream e, por consequência, aos seus itens.

Em se tratando dos certificados emitidos pela Universidade Federal do Tocantins, serão gravados em streams da Multichain o hash dos mesmos, utilizando-se o algoritmo SHA256 (no Linux o comando para geração de hash é o “sha256sum”). Posteriormente, caso algum interessado queira conferir a genuinidade dos certificados, poderá fazê-lo por meio das seguintes operações:

1. Gerar um hash do certificado a ser validado.

2. Comparar o hash gerado com o hash existente na blockchain.

A tabela VI resume os passos necessários para instalação, configuração, criação de objetos e utilização da Multichain num ambiente Linux.

Tabela VI - Instalação, configuração e uso da Multichain.

Ação	Comando
Download e instalação	wget https://www.multichain.com/download/multichain-1.0.3.tar.gz tar -xvzf multichain-1.0.3.tar.gz cd multichain-1.0.3 sudo mv multichaind multichain-cli multichain-util /usr/local/bin
Criação da blockchain	multichain-util create chain1
Alteração do arquivo de configuração	vim /home/cleorbete/.multichain/chain1/params.dat
Algumas propriedades do arquivo de configuração	# Parâmetros básicos da blockchain chain-protocol = multichain # Protocolo: multichain ou bitcoin chain-description = MultiChain chain1 # Descrição da blockchain target-block-time = 15 # Tempo entre cada transação, em segundos (2 - 86400) maximum-block-size = 8388608 # Tamanho máximo de cada bloco, em bytes. (1000 - 1000000000) # Permissões globais anyone-can-connect = false # Qualquer interessado pode conectar á blockchain anyone-can-send = false # Qualquer interessado pode enviar

	transações anyone-can-receive = false # Qualquer interessado pode receber transações anyone-can-create = false # Qualquer interessado pode criar novos stream anyone-can-mine = false # Qualquer interessado pode minerar blocos (confirmar transações) anyone-can-admin = false # Qualquer interessado pode dar ou revogar permissões de usuários. default-network-port = 6475 # Porta TCP/IP padrão para comunicação p2p pelos nós default-rpc-port = 6474 # Porta TCP/IP padrão para requisições JSON-RPC chain-name = chain1 # Nome da blockchain, usado como primeiro argumento para os comandos multichaind e multichain-cli
Execução da blockchain	multichaind chain1 -daemon
	X
Adição de outro servidor à blockchain	multichaind chain1@10.27.70.215:4803
Garantindo o acesso ao novo servidor	multichain-cli chain1 grant <numero de wallet exibido no segundo servidor> connect
Conectando o novo servidor à blockchain	multichaind chain1 -daemon
Executando o modo interativo	multichain-cli chain1
Criação de streams	create stream stream1 false
Manipulação de streams	• Listar permissões do stream: chain1 listpermissions stream1.*; • Publicar no stream: publish stream1 key1 73747265616d2064617461; • Inscrever-se no stream: subscribe stream1; • Listar itens do stream: liststreamitems stream1; • Listar itens de uma chave específica do stream: liststreamkeyitems stream1 key1;
Criação de hash em Linux	Sha256sum certificado.jpg
Exclusão de streams	multichain-cli chain1 stop rm -rf /home/cleorbete/multichain/chain1

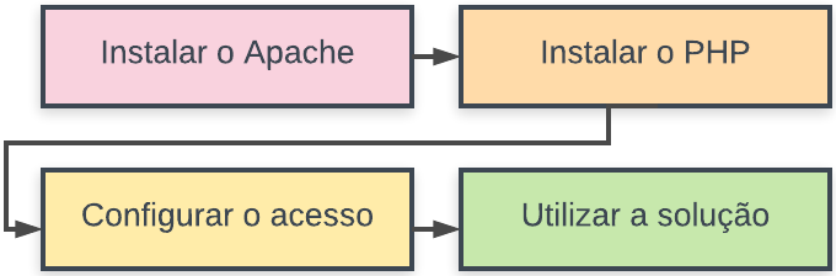
Fonte: Multichain (adaptado pelo autor).

4.4 Configuração da Interface Web

A interface Web a ser utilizada para envio de dados às streams da blockchain da Universidade Federal do Tocantins é feita em PHP versão 5, ou superior, com a biblioteca de transferência de dados Curl rodando em um servidor Apache2. O passo

a passo para a configuração da solução é demonstrado na Figura 12 e detalhado logo em seguida.

Figura 12 - Sequência de configuração da interface Web.



Fonte: Multichain (adaptado pelo autor).

A instalação do Apache 2.0, servidor Web onde a interface Web será hospedada, é feita por meio do comando:

```
sudo aptitude install apache2
```

A interface Web desse projeto feita em PHP a partir da demonstração disponível no site oficial da Multichain (www.multichain.com), utiliza a biblioteca Curl para transmitir dados com a Blockchain. Abaixo os comandos para instalação do PHP e do Curl para PHP.

```
sudo aptitude install php5
sudo aptitude install php5-curl
```

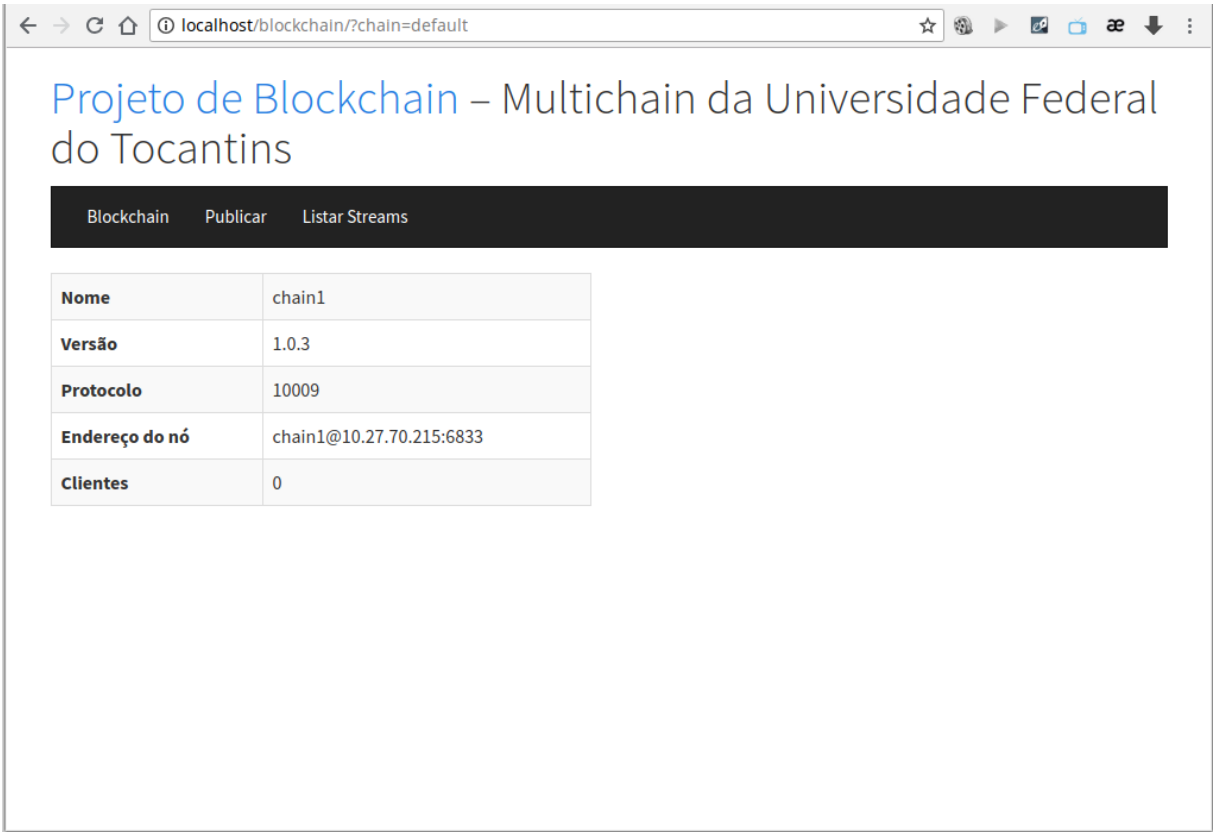
As configurações para conectar a solução em PHP à Multichain são feitas no arquivo config.txt, composto por propriedades que definem chaves e valores, como exibido nas linhas que seguem.

```
default.name=Multichain da UFT        # Nome a ser mostrado na interface Web
default.rpchost=127.0.0.1             # IP do nó MultiChain
default.rpcport=6726                  # Valor default-rpc-port do params.dat
default.rpcuser=multichainrpc         # Nome de usuário do multichain.conf
default.rpcpassword=senha             # Senha para o RPC do multichain.conf
```

É interessante notar que a comunicação é feita via chamada de procedimento remoto (*RPC - Remote Procedure Call*), sendo exigida a porta RPC, definida no arquivo params.dat e usuário e senha, fornecidos no arquivo multichain.conf.

Todas as telas da solução contêm um menu com links, sendo o primeiro link chamado “Blockchain”, que leva a uma página que exibe o nome da blockchain criada, bem como a versão da Multichain utilizada, a versão do protocolo, o endereço do nó de rede e a quantidade de clientes conectados, conforme exibido na Figura 13.

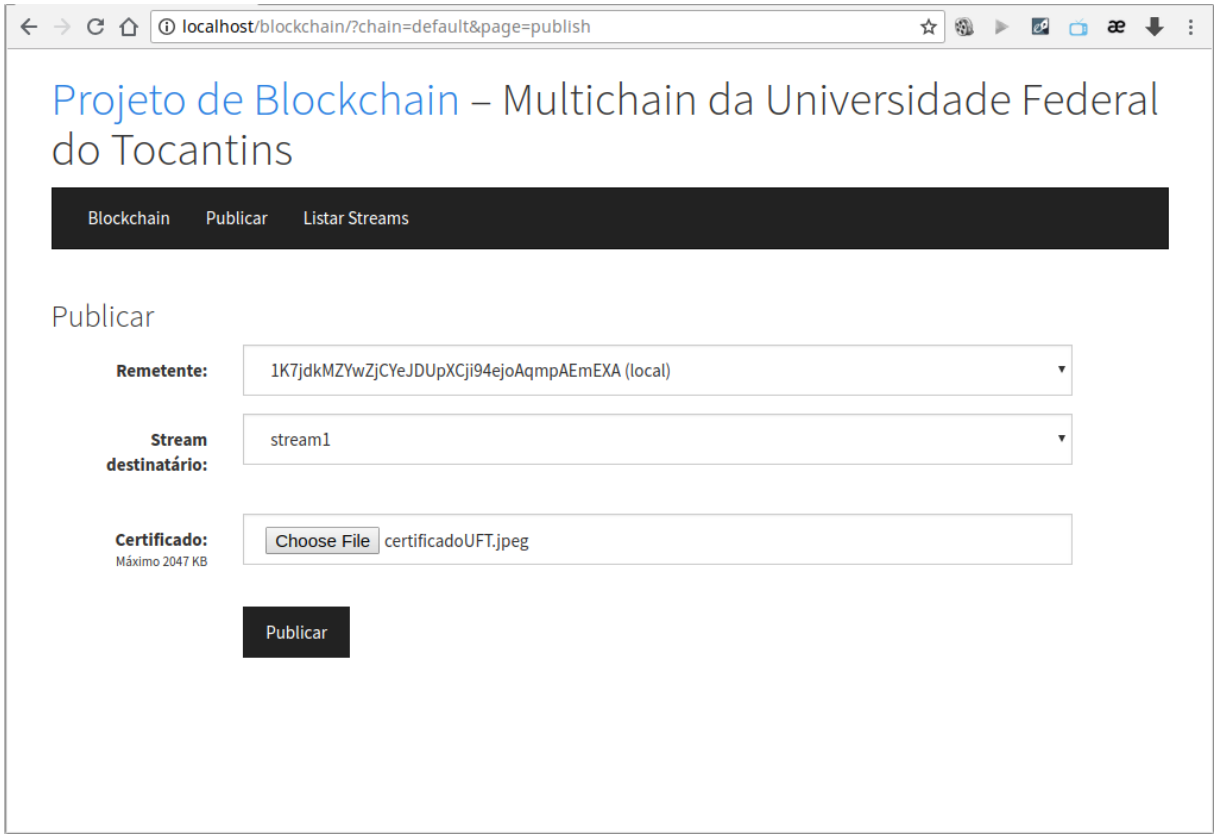
Figura 13. Página “Blockchain” da interface Web.



Fonte: autor.

O link “Publicar” leva a uma página onde é possível enviar certificados à blockchain, selecionando-se o remetente e o stream de destino (vide Figura 14), com a geração do hash do certificado sendo feita de maneira transparente por meio da função hash_file do PHP: hash_file('sha256', $upload_file).

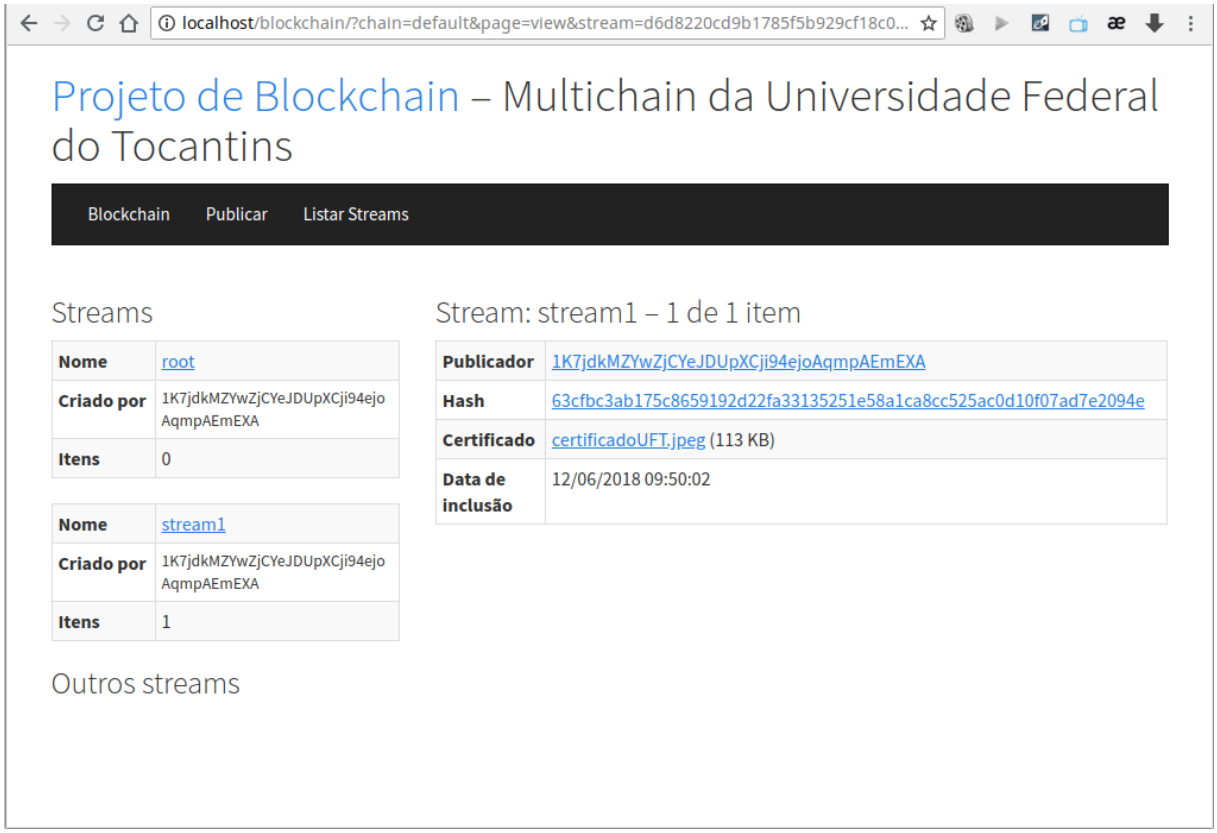
Figura 14. Página “Publicar” da interface Web.



Fonte: autor.

Clicando-se em “Listar Streams” (Figura 15), será exibida uma página que lista todos os streams da blockchain, bem como dos seus respectivos dados, incluindo o hash dos certificados, que poderá ser comparado por meio de ferramentas de geração de sha256 a partir de arquivos, como a “SHA256 File Checksum”, disponível no link https://goo.gl/FGUqkZ.

Figura 15. Página “Listar Streams” da interface Web.



Fonte: autor.

Finalmente, se utilizado o link disponível no campo “Certificado” da página “Listar Streams” (Figura 15), será possível acessar o arquivo original, armazenado na blockchain (Figura 16).

Figura 16. Página exibindo um certificado armazenado na blockchain.

Fonte: autor.

Os princípios da confidencialidade, integridade e disponibilidade dos dados são considerações críticas para uma solução que vise ao armazenamento de ativos digitais, particularmente no âmbito público, caso da Universidade Federal do Tocantins. Partindo desse pressuposto, foi escolhida para esse trabalho a implementação de blockchain Multichain, haja vista sua natureza de rede distribuída, seus atributos peculiares de inalterabilidade e persistência de informações e seus recursos de segurança, como controle de acesso baseado em permissões em nível de blocos de dados. Ademais, a Multichain é uma solução de código aberto, o que leva à economia de recursos computacionais e financeiros para sua implantação. Além do exposto, visando-se facilitar a utilização da Multichain, adotou-se uma interface Web feita na linguagem PHP, levando-se em consideração questões atinentes à usabilidade, escalabilidade, compatibilidade e manutenção. Ambas as tecnologias, Multichain e PHP, são mantidas por comunidades do mundo inteiro, que é de onde saem atualizações e documentação para seus usuários.

5. CONCLUSÕES

Blockchain é uma das mais inovadoras tecnologias da atualidade, conhecida, principalmente, por ser a malha digital por trás da famosa criptomoeda Bitcoin. Trabalha como banco de dados de registro de transações seguro e robusto, compartilhado por usuários de todas as partes do globo e por dispositivos diversos, conectados entre si por meio do paradigma de uma rede distribuída em larga escala.

Para esse trabalho foi explanado sobre a criação de uma blockchain privada para uso na Universidade Federal do Tocantins com o fito primordial de armazenar certificados emitidos pela instituição, bem como de seus respectivos hashes, para que, com isso, qualquer interessado possa validá-los e afastar a possibilidade de falsificação.

Projeto similares a esse foram desenvolvidos em instituições de renome, como o MIT - Massachusetts Institute of Technology e a Holberton School, de San Francisco (EUA), mas ambos utilizam a blockchain pública da Bitcoin, mediante pagamento de taxas. Esse projeto utiliza uma blockchain privada, com controle de acesso (*permissioned*) utilizando uma solução de código aberto, a Multichain, garantindo escalabilidade, compatibilidade e baixo custo de implantação e manuteanção para a Universidade Federal do Tocantins.

Nas implementações públicas de Blockchain impera a descentralização, enquanto nas privadas há um intermediário mantendo a rede em operação e decidindo quais usuários e dispositivos participarão da estrutura e sob quais privilégios de acesso. Outro aspecto a ser levado em consideração é que a solução de blockchain privada apresentada nesse trabalho não exige validação de blocos de dados por meio de *Proof of Work (PoW)*. Com isso, torna-se desnecessário alocar ativos computacionais e dispender energia elétrica para o processo de mineração, resultando em mais economia e maior eficiência na utilização de recursos.

Por fim, inúmeras são as soluções que podem ser feitas a partir dos estudos e das tecnologias utilizadas no projeto objeto do presente estudo, tais como:

- Banco de dados distribuído.
- Repositório e edição de arquivos.
- Contratos Inteligentes (Smart Contracts).
- Economia compartilhada (ao estilo Airbnb).
- Financiamento coletivo (Crowdfunding).
- Governança.
- Cadeia de suprimento (Supply chain).
- Mercados preditivos.
- Soluções de proteção à propriedade intelectual.
- Internet das Coisas (IoT).
- Sistemas de prevenção a lavagem de dinheiro.
- Registros de imóveis.
- Gerenciamento de dados pessoais.
- Compliance.

Referências

ANTONOPOULOS, Andreas M. **Mastering Bitcoin.** O'Reilly, 2010.

WATTENHOFFER, Roger. **The Science of the Blockchain**. CreateSpace Independent Publishing Platform, 2016.

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

PÉREZ-MARCO, Ricardo. **Bitcoin and Decentralized Trust Protocols**. Univ. Paris, France, 2016.

PEARSON, Jordan. Former Bitcoin Developer Shares Early Satoshi Nakamoto Emails. Motherboard, 2017.

POINTCHEVAL, David. **Practical Security in Public-Key Cryptography**. Springer-Verlag, 2002.

STALLINGS, William. **Criptografia e Segurança de Redes**. 6. ed. São Paulo: Pearson, 2014.

BURNETT, S. 2001. **RSA Security's Official Guide to Criptography**. Berkley: McGraw-Hill.

CARTS, David A. **A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols**. SANS Institute, 2001.

OKUPSKI, Krzysztof. **Bitcoin Developer Reference**. Technische Universiteit Eindhoven, The Netherlands, 2016.

JANSMA, Nicholas; ARRENDONDO, Brandon. **Performance Comparison of Elliptic Curve and RSA Digital Signatures**. University of Michigan, 2004.

MORENO, Edward; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005.

BURNETT, Steve; PAINE, Stephen. **RSA Security's Official Guide to Cryptography**. McGraw-Hill, 2001.

BURR, Bill. **NIST Hash Competition**. NIST, 2008.

FORBELLONE, André Luiz; EBERSPÄCHER, Henri Frederico. **Lógica de programação**. 3. ed. São Paulo: Pearson, 2005.

LAUREANO, Marcos. **Estrutura de Dados com Algoritmos e C**. Rio de Janeiro: Brasport, 2008.

NARAYANAN, Arvind et al; **Bitcoin and Cryptocurrency Technologies**. Princeton, 2015.

CURRY, Ian. **An Introduction to Cryptography and Digital Signatures**. Entrust, 2001.

TANENBAUM, Andrew S; Maarten Van STEEN. **Distributed Systems** - Principles and paradigms. Upper Saddle River: Pearson, 2007.

TANENBAUM, Andrew S. **Computer Networks** - 4th Edition. Prentice Hall, 2002.

DONET, Joan Antoni Donet; PEREZ-SOLA, Cristina; HERRERA-JOANCOMART, Jordi. **The Bitcoin P2P network**. Universitat Autònoma de Barcelona, 2014.

GUEGAN, Dominique. **Public Blockchain versus Private blockhain**. Sorbonne, 2017.

GARZIK, Jeff. **Public versus Private Blockchains**. Bitfury, 2015.

UK Government, Her Majesty's Treasury. **Digital currencies**: response to the call for information. Crown, 2015.

THOMAS, Ryan. **Attacks on PGP: A User's Perspective**. SANS Institute, 2003.

KROMBHOLZ, Katharina; JUDMAYER, Aljosha; GUSENBAUER, Matthias. and Edgar Weippl. **The Other Side of the Coin**: User Experiences with Bitcoin Security and Privacy. SBA Research, 2016.

DESHPANDE, Advait et al. **Distributed Ledger Technologies/Blockchain**: Challenges, opportunities and the prospects for standards. BSI, 2017.

GUADAMUZ, Andres; MARSDEN, Chris. **Blockchains and Bitcoin**: regulatory responses to cryptocurrencies. Sussex, 2015.

The Primary Challenge To Blockchain Technology. Disponível em <https://www.forbes.com/sites/peterbendorsamuel/2017/05/23/the-primary-challenge-to-blockchain-technology>. Acesso em 16 de maio de 2018.

Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain. Disponível em: <http://www.marketwired.com/press-release/holberton-school-authenticate-its-academic-certificates-with-bitcoin-blockchain-2065768.htm>. Acesso em 14 de maio de 2018.

Blockchain Certificates. Disponível em: <http://www.blockcerts.org/guide/>. Acesso em 14 de maio de 2018.

Sony Global - Sony Global - Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records. Disponível em: <https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html>. Acesso em 14 de maio de 2018.

Gamification in Education. Disponível em: <https://www.learning-theories.com/gamification-in-education.html>. Acesso em 14 de maio de 2018.

AI, Gamification and Blockchain at DBS Hong Kong Accelerator. Disponível em: <http://www.finews.asia/finance/23329-fintech-dbs-nest-innovation-blockchain-gamification-incubator-accelerator-lawrence-morgan-sebastian-paredes>. Acesso em 14 de maio de 2018.

Blockchains. Disponível em <https://tokenmarket.net/blockchain/>. Acesso em 19 de maio de 2018.

Academic Certificates on the Blockchain. Disponível em: <https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/>. Acesso em 14 de maio de 2018.

Joint Research Center Science for Policy Report – Blockchain in Education. Disponível em: <http://blockchain.open.ac.uk/>. Acesso em 14 de maio de 2018.

College Cryptocurrency Network Rebrands to Blockchain Education Network, Expands Worldwide. Disponível em: <https://bitcoinmagazine.com/articles/college-cryptocurrency-network-rebrands-to-blockchain-education-network-expands-worldwide-1455904096/>. Acesso em 14 de maio de 2018.

Blockchain – What is Permissioned vs Permissionless? Disponível em <https://bornonjuly4.me/2017/01/10/blockchain-what-is-permissioned-vs-permissionless/>. Acesso em 19 de maio de 2018.

PECK, Morgen. **Reinforcing the links of the Blockchain**. IEEE, 2017.

MUZAMMAL, Muhammad. **Renovating blockchain with distributed databases**: An open source system. Elsevier, 2018.

BHARDWAJ S., KAUSHIK M. (2018) **Blockchain** - Technology to Drive the Future. In: Satapathy S., Bhateja V., Das S. (eds) Smart Computing and Informatics. Smart Innovation, Systems and Technologies, vol 78. Springer, Singapore.

HALABURDA, Hanna. **Blockchain Revolution Without the Blockchain**. Communications of the ACM, July 2018, Vol. 61 No. 7, Pages 27-29.

MOUGAYAR, William; SBRAVATTI, Vivian. **Blockchain para negócios**. Alta Books, 2017.

DRESCHER, Daniel; KINOSHITA, Lúcia A. **Blockchain Básico**. Novatec, 2018.

CAMPOS, Emília Malgueiro. **Criptomoedas e Blockchain**. Lumen Juris, 2018.

HOLLINS, Steve. **Bitcoin Para Iniciantes** - O Guia Definitivo para Aprender a Usar Bitcoin e Criptomoedas. Createspace Independent Publishing Platform, 2018.

MARTINS, Pedro. **Introdução à Blockchain**. FCA, 2018.

BARBOSA, Tatiana Casseb. **A Revolução das Moedas Digitais**. Revoar, 2015.

ULRICH, Fernando. **Bitcoin** - A Moeda na Era Digital. Mises, 2014.

TAPSCOTT, Dan; TAPSCOTT, Alex. **Blockchain Revolution**. SENAI-SP, 2017.

SILVA, Luiz Gustavo Doles. **Bitcoins e Outras Criptomoedas**. Juruá, 2018.

MOUGAYAR, William. **Blockchain Para Negócios**. Alta Books, 2017.

CONG, Lin William. **Blockchain, Disruption and Smart Contracts**. National Bureau of Economic Research, Cambridge, MA, 2018.

BONEH, Dan; SHOUP, Victor. **A Graduate Course in Applied Cryptography**. Stanford, 2017.

MENEZES, Alfred J; OORSCHOT, Paul C; VANSTONE, Scott A. **Handbook of applied cryptography**. CRC Press, 1996.

DENIS, Tom St; JOHNSON, Simon. **Cryptography for Developers**. O'Reilly, 2007.

SHARMA, Toshendra Kumar. **List of best open source blockchain platforms**. Blockchain-council, 2017.

BASTIAAN, Martijn. **Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin**. University of Twente, 2016.

ROSIC, Ameer. **What is Blockchain Technology?** A Step-by-Step Guide For Beginners. Blockgeeks, 2016.

GERARD, David. **Attack of the 50 Foot Blockchain**. Google Books, 2017.

DRESCHER, Daniel. **Blockchain Basics**: A Non-Technical Introduction in 25 Steps. Appress, 2017.

GATES, Mark. **Blockchain**: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. CreateSpace Independent Publishing Platform, 2017.

LAURENCE, Tiana. **Blockchain For Dummies**. John Wiley & Sons, 2017.

SWAN, Melanie. **Blockchain**: Blueprint for a New Economy. O'Reilly, 2015.

FERREIRA, Juliandson Estanislau; PINTO, Filipe Gutemberg Costa; SANTOS, Simone Cristiane dos. Estudo de Mapeamento Sistemático sobre as Tendências e Desafios do Blockchain. **Revista Gestão.Org**, v. 15, Edição Especial, 2017. p. 108-117.

SANTANA, Caio Vinicius; SANTOS, Davi Bispo dos; SANTOS, Paulo Rogério dos. Introdução ao estudo do Bitcoin e uma análise empírica das tentativas de regulação. **Revista Científica Integrada da UNAERP**, Vol. 3. Edição 3.

DINIZ, Eduardo Henrique. Emerge uma nota tecnologia disruptiva. **FGV. GVExecutivo**. V 16. N 2. MAR/ABR 2017.

ARAÚJO, Henrique Pereira; SILVA, Rebecca Bignardi. A tecnologia digital Blockchain: análise evolutiva e pragmática. **Revista FATEC Zona Sul**. 1a Edição. OUT/2014.

PIRES, H. F. Bitcoin: a moeda do ciberespaço. **Geousp** - Espaço e Tempo (Online), v. 21, n. 2, p. 407-424, agosto. 2017. ISSN 2179-0892.

BENÍCIO, Alberto Ayres. Bitcoin, a moeda digital que se tornou realidade. **Revista Científica da UNESC** v. 12, n. 15 (2014).

BRANCÓS i NÚÑEZ, Enric. “Blockchain, función notarial y registro”. **El notario del siglo XXI**: revista del Colegio Notarial de Madrid, ISSN 1885-009X, Nº. 71, 2017, p. 50-53.

CERVERA RUIZ, Pedro. “Smart contracts: la eficacia autónoma”. **Estrategia financiera**, ISSN 1130-8753, Nº 343, 2016, p. 26-31.

ESPAÑA ALBA, Víctor Manuel. “Bitcoin: un antes y un después en el blanqueo de capitales”. **Diario La Ley**, ISSN 1989-6913, N. 8740, 2016.

FERNÁNDEZ BURGUEÑO, Pablo. “Retos legales del bitcoin, ethereum y los smart contracts”. **Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática**: [Salamanca, 19-21 de octubre 2016]. Coord. por Erika Yamel Munive Cortés, Irene González Pulido, Lorena Muñoz Sánchez; Federico Bueno de Mata (dir. congr.). Salamanca: Ratio Legis, 2016. Vol. 2, 2016, ISBN 9788416324422, p. 259-271.

NAVAS NAVARRO, Susana; CAMACHO CLAVIJO, Sandra. **Mercado digital**: principios y reglas jurídicas. Valencia: Tirant lo Blanch, 2016. (Derecho y tic's). ISBN 9788491195269.

NAVAS NAVARRO, Susana. “Un mercado financiero floreciente: el del dinero virtual no regulado (especial atención a los Bitcoins)”. **Revista CESCO de Derecho de Consumo**. ISSN-e 2254-2582, N. 13, 2015, p. 79-115.

PACHECHO JIMÉNEZ, María Nieves. “Criptodivisas: del bitcoin al MUFG. El potencial de la tecnología blockchain”. **Revista CESCO de Derecho de Consumo**, ISSN-e 2254-2582, Nº. 19, 2016, p. 6-15.

PÉREZ GAIPO, Julio. “Monedas virtuales: el embargo de bitcoins y sus problemas”. En: **Fodertics 4.0**: Estudios sobre Nuevas tecnologías y Justicia. Federico Bueno de Mata (coord.). Madrid: Comares, 2015. ISBN 9788490452745, p. 271-282.

PRENAFETA RODRÍGUEZ, Javier. “Smart contracts: aproximación al concepto y problemática legal bàsica”. En: **Diario La Ley**, ISSN 1989-6913, Nº 8824, 2016.

ROSEMBUJ, Tulio. **Bitcoin**. Barcelona: el Fisco, 2015. ISBN 9788494409806.

SÁNCHEZ MONJO, Miguel. “FinTech: panorama actual y tendencias regulatorias”. En: **Revista de derecho del mercado de valores**, ISSN 1888-4113, Nº. 19, 2016.

VEGA VEGA, José Antonio. **Derecho mercantil electrónico**. Madrid: Reus, 2015. (Derecho mercantil). ISBN 9788429018608.

ZÚÑIGA, Ángeles. “Bitcoin: mucho más que una moneda”. En: **Escritura pública**. ISSN 1695-6508. N. 92 (2015), p. 57.

What is Blockchain Technology. Disponível em: <https://www.coindesk.com/information/what-is-blockchain-technology/>. Acesso em 12 de maio de 2018.

Satoshi Nakamoto. Disponível em: <https://en.bitcoin.it/wiki/Satoshi_Nakamoto>. Acesso em 12 de maio de 2018.

Bitcoin P2P e-cash paper. Disponível em: <http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>. Acesso em 12 de maio de 2018.

Who is Satoshi Nakamoto. Disponível em: <http://www.coindesk.com/information/who-is-satoshi-nakamoto/>. Acesso em 13 de maio de 2018.

Security by Design Principles. Disponível em: <https://www.owasp.org/index.php/Security_by_Design_Principles>. Acesso em 13 de maio de 2018.

Fault tolerance. Disponível em: <https://www.computerhope.com/jargon/f/faulttol.htm>. Acesso em 13 de maio de 2018.

How blockchains could change the world. Disponível em: <http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world>. Acesso em 14 de maio de 2018.

What we learned from designing an academic certificates system on the blockchain. Disponível em: <https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196>. Acesso em 14 de maio de 2018.

Blockchain certificates. Disponível em: <https://www.media.mit.edu/projects/media-lab-digital-certificates/overview/>. Acesso em 14 de maio de 2018.

SHA-256. Disponível em <https://en.bitcoin.it/wiki/SHA-256>. Acesso em 15 de maio de 2018.

MILLER, Jaime Núñez."ECDSA". Disponível em <http://libroblockchain.com/ecdsa/>. Acesso em 15/05/2018.

Standards for Efficient Cryptography. Disponível em <www.secg.org>. Acesso em 16 de maio de 2018.

Secp256k1. Disponível em <https://en.bitcoin.it/wiki/Secp256k1>. Acesso em 16 de maio de 2018.

Krypton Recovers from a new type of 51% network attack. Disponível em: <https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack>. Acesso em 16 de maio de 2018.

Op-ed: China Ranked [51% Attack] Verge and Bitcoin at #13 in Blockchain List. Disponível em: <https://www.ccn.com/op-ed-china-ranked-51-attack-verge-and-bitcoin-at-13-in-blockchain-list/>. Acesso em 16 de maio de 2018.

Bitcoin Gold loses over $18 million to 51% attack. Disponível em <https://mybroadband.co.za/news/cryptocurrency/261805-bitcoin-gold-loses-over-18-million-to-51-attack.html>. Acesso em 16 de maio de 2018.

Open platform for building blockchains. Disponível em <https://www.multichain.com/>. Acesso em 17 de maio de 2018.

What Vim Can Do. Disponível em <https://www.vim.org/about.php>. Acesso em 18 de maio de 2018.

Multichain data streams. Disponível em <https://www.multichain.com/developers/data-streams/>. Acesso em 18 de maio de 2018.

This is what happens when bitcoin miners take over your town. Disponível em <https://www.politico.eu/article/this-is-what-happens-when-bitcoin-miners-take-over-your-town/>. Acesso em 18 de maio de 2018.