UNIVERSIDADE FEDERAL DE SANTA CATARINA

ESTUDO DA APLICAÇÃO DE ESTRUTURA BLOCKCHAIN COM PROOF OF STAKE PARA ARQUIVAMENTO DE DOCUMENTOS COM REGISTRO NO TEMPO

Otávio Augusto Corrêa

Florianópolis

2017/2

Otávio Augusto Corrêa

ESTUDO DA APLICAÇÃO DE ESTRUTURA BLOCKCHAIN COM PROOF OF STAKE PARA ARQUIVAMENTO DE DOCUMENTOS COM REGISTRO NO TEMPO

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do título de Bacharel, do curso de Sistemas de Informação na Universidade Federal de Santa Catarina.
Orientador: Profª Jean Everson Martina, Dr.

Florianópolis

2017/2

Otávio Augusto Corrêa

ESTUDO DA APLICAÇÃO DE ESTRUTURA BLOCKCHAIN COM PROOF OF STAKE PARA ARQUIVAMENTO DE DOCUMENTOS COM REGISTRO NO TEMPO

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do título de Bacharel, do curso de Sistemas de Informação na Universidade Federal de Santa Catarina.

Profº Frank Augusto Siqueira, Dr.
Coordenador do Curso

Banca Examinadora:

Profª Jean Everson Martina, Dr.
Orientador
Universidade Federal de Santa Catarina

Cristian Thiago Moecke.
Co-Orientador
Universidade Federal de Santa Catarina

Profº Ricardo Felipe Custódio, Dr.
Universidade Federal de Santa Catarina

Florianópolis
2017/2

Dedico este trabalho este trabalho primeiramente a Deus, minha mulher Lais com quem sem eles não teria feito nada, a minha familia, amigos e profissionais os quais passo longas horas do dia conversando e convivendo, ensinando e aprendendo.

Resumo

A transferência de documentos entre entidades existe a muitos anos, desde comprovações de imóveis, decisões jurídicas, até processos dentro das empresas, o alto fluxo de documentos aumentou os gastos com papel, matéria base dos documentos. Com o aumento da tecnologia e utilização de aparelhos eletrônicos, criou-se o que é chamado de documento eletrônico. Porém se com documentos reais fraudes já eram encontradas, com documentos eletrônicos essa insegurança é ainda maior, a modificação dos bytes ou variáveis de um documento poderiam deixar em risco a segurança e confiança do mesmo. Para resolver esta questão foi criado o que é chamado Assinatura Digital, um documento poderia ser assinado por uma chave que somente uma pessoa tivesse posse. Mas outra questão que veio a tona foi o período de validade desta assinatura. Para isso foi criado o carimbo do tempo, que comprova que em determinada data, este documento foi assinado. Toda esta infraestrutura para garantir a validade de um documento tem um custo elevado, com a proposta deste estudo, o autor avaliou a viabilidade de uma estrutura de banco de dados distribuídos baseada em blockchain onde os arquivos possam ser armazenados confiavelmente, sem que tenha problemas com sua segurança, alterações ou fraudes, semelhante ao processo de carimbo do tempo.

Palavras-chave: BlockChain, Criptografia, Assinatura Digital.

Abstract

A transfer of documents between entities has existed for many years, from proof of real estate, legal issues, to cases within companies, the high flow of documents has increased paper expenses, which are the basis of documents. With the increase of technology and the use of electronic devices, we have created what is called an electronic document. But if with real documents already found frauds, with electronic documents this insecurity is even greater, a modification of the bytes or variables of a document in question, leave at risk a security and confidence of itself. To solve this problem with what is called Digital Signature, a document must be signed by a single and single person possession. But all that came at once per period of validity of this signature. For this, the time stamp was created, which proves in certain data, this document was signed. All this infrastructure to ensure the validity of a document has a high cost, with the proposal of this study, the author evaluated the feasibility of a blockchain-based distributed database structure where the files can be stored reliably, without having problems with your security, alterations or frauds, similar to the time stamp process.

Keywords: Digital signature, Blockchain, Cryptography.

Lista de ilustrações

Lista de abreviaturas e siglas

DSA	*Digital Signature Algorithm*
ECDLP	*Elliptic Curve Discrete Logarithm Problem*
TCC	Trabalho de Conclusão de Curso
ITI	Instituto Nacional de Tecnologia da Informação
CA	Autoridade Certificadora
ICP-Brasil	Infraestrutura de Chaves Públicas - Brasil

Sumário

1 Introdução

Vivemos em um século marcado pelo predomínio do conhecimento e da informação, a Internet nos proporciona maior eficiência e rapidez na transmissão de dados e produção. Através do seu acesso, barreiras são desfeitas, permitindo que pessoas se reúnam em lugares virtuais. (GANDINI; SALOMÃO; JACOB, 2001).

Com toda essa informação, é necessário garantir a validade na troca de informações, a assinatura digital é utilizada para agregar confiança e segurança às comunicações e negócios vinculados a um ambiente virtual como a Internet, oferecendo eficiência e rapidez. Além disso, a assinatura digital contribui de forma positiva para o meio ambiente, empresas que armazenam milhares de documentos poderiam digitalizar os mesmos, garantindo a sua validade jurídica através de assinaturas digitais (MENKE, 2003).

A assinatura digital é baseada na criptografia assimétrica ou criptografia de chaves públicas que consiste no uso do par de chaves, pública e privada, uma utilizada pelo remetente e outra pelo receptor da mensagem, e é sobre este conceito que se baseia uma assinatura digital. Este par de chaves é gerado por programas de computador ou hardware e as chaves atuam em conjunto. Tudo que é cifrado pela chave pública, só pode ser decifrado pela chave privada correspondente e vice versa. Uma assinatura digital é feita através do uso da chave privada e a verificação é com o uso da chave pública. Somente a chave pública correspondente aquela chave privada poderá interpretar corretamente a assinatura (STALLINGS, 2008).

Para agregar mais segurança ao processo de assinatura, é necessário garantir que a chave privada utilizada para assinar pertence ao assinante. Um certificado digital é o elemento que garante esta autenticidade, porque um certificado é assinado por uma terceira parte confiável, a qual comprova o vínculo entre o assinante e sua chave pública. Na prática, o certificado digital, que contém a chave pública do assinante, é enviado juntamente com a assinatura, desta forma é possível verificar a assinatura e atestar a autenticidade bem como a validade desta informação.(NAKAMURA; GEUS, 2007)

Hash é uma sequência de bits geradas a partir de uma função, em geral representada em base Hexadecimal. Tem o objetivo de assegurar que determinado documento é único, pois é diferente para cada documento eletrônico. E difundido em diversos softwares onde se deseja

garantir a unicidade de um documento e sua não adulteração. (PFLEEGER, 1997).

Carimbo do Tempo é um documento eletrônico emitido por uma entidade confiável, que serve como evidência de que um documento assinado existia em determinada data e hora no passado, associando-se data de fonte confiável ao hash desse documento assinado. (SILVA; RAMOS; CUSTÓDIO, 2011).

Blockchain é uma estrutura de banco de dados distribuído. Ele foi primariamente desenvolvido para um sistema de criptomoeda chamado de BitCoin, porém é a estrutura de dados por trás do sistema conhecido. Além de distribuído, é descentralizado, não existe uma entidade central para gerir os dados.(LUCENA; HENRIQUES, 2016)

O Blockchain funciona como uma cadeia de blocos, onde estão ligados o bloco anterior ao próximo bloco, formando uma cadeia. Cada bloco contém as transações que serão efetuadas. Estas transações são Peer-to-peer, emissor ligado diretamente ao receptor, ou como no caso do Bitcoin uma wallet envia dados para outra wallet.(RODRIGUES, 2016)

Os blocos após serem gerados são distribuídos para toda a rede que compõem a Blockchain, assim todas as partes contém a informação das transações feitas, a segurança está em que se houver um ataque tentando modificar alguma transação e consequentemente um bloco, o ataque terá que modificar mais da metade da rede. (RODRIGUES, 2016)

O Blockchain funciona da seguinte forma, primeiro seleciona as transações já realizadas, gera o hash de todas essas transações, estrutura em ordem, armazena em um bloco, e valida o bloco, para validação existe um processo de prova o que é chamado proof of work ou prova de trabalho, onde há mineração de hashes para encontrar um que seja válido para a rede e possa efetivar o bloco.(LUCENA; HENRIQUES, 2016)

Um dos problemas encontrados na prova de trabalho (proof of work) é o custo energético, a produção de vários hashes até encontrar um válido, há um alto consumo de energia para os processadores ASIC's (hardware específico para mineração) conseguirem encontrar o próximo hash válido para o bloco. Por conta disto, está se discutindo uma nova forma de mineração, chamada de proof of stake ou prova de participação. Dentre os pontos positivos de utilizar blockchain tem-se o baixo custo, seguro, sem intermediários, imutável, único, público e com facilidade de transações internacionais.(ALIAGA; HENRIQUES, 2017)

Todos estes pontos serão abordados neste trabalho e por meio deste é feito um estudo sobre a arquitetura Blockchain, destrinchando todos seus atributos e feita uma análise

dentre as principais arquiteturas para viabilizar uma que se adeque melhor ao caso proposto de arquivamentos de documentos com registro no tempo.

1.1 Objetivos

Esta seção tratará dos objetivos gerais e específicos a serem alcançados por este Trabalho de Conclusão de Curso.

1.1.1 Geral

O objetivo deste trabalho é desenvolver um estudo sobre o uso de uma arquitetura BlockChain, como ela se comporta, buscando destrinchar todos os atributos necessários para o seu entendimento, e realizar uma análise dentre as arquiteturas já presentes pensando no seu método de consenso com uso de Proof of Stake para armazenamento confiável de documentos eletrônicos, com fim de propor um modelo de confiança, dados os requisitos para a pesquisa.

1.1.2 Específicos

Os objetivos específicos deste trabalho que podem ser listados são:

- Realizar estudo sobre o uso e estrutura de uma BlockChain;
- Elicitar todos os itens referentes a tecnologia;
- Realizar uma análise com arquiteturas de blockchain buscando uma adequada para a confecção de arquivamento no tempo, dadas as limitações do caso específico.
- Encontrar e propor um modelo de uso para arquivamento de assinaturas digitais;

1.2 Justificativa

Hoje em dia o arquivamento de documentos se tornou cada vez mais digital, pela busca de um menor espaço físico a ser utilizado, entretanto a confiança de documentos sempre está em jogo quando se trata do meio digital, onde é possível a manipulação de dados claros por diversas fontes. Para arquivamento de documentos, principalmente aqueles que registram fatos que necessitam de comprovações e garantias, são feitas assinaturas digitais e utilizado carimbos

do tempo, com criptogria e sistemas de segurança que garantam que determinado documento é válido.

Este trabalho buscar encontrar uma forma independente para atestar datação de um documento com segurança. Devido à grande comoção atual para o Bitcoin (criptomoeda) e blockchain, o autor deseja descobrir se é possível utilizar esse modelo para uma nova possibilidade de inovação e utilização de arquivamento de documentos com datação confiável, que possa no futuro ser usada pelas empresas e sistemas jurídicos, garantindo a validade temporal de documentos e assinatuas digitais.

1.3 Metodologia

A obtenção dos resultados finais do trabalho, que consistem na análise de tipos de blockchain para o propósito de arquivamento e datação de documentos no tempo, será realizada por meio de pesquisas exploratórias, buscando em trabalhos correlatos, livros e com auxilio da internet as informações pertinentes a base teorica, os dados da segunda etapa para análise será feito com ponderações, validando as questões cruciais para o desenvolvimento da tecnologia, obtendo produtos já desenvolvidos com proof of stake e outros já consolidados.

2 Fundamentação Teórica

Este capítulo apresenta uma revisão dos conceitos essenciais para o entendimento e desenvolvimento deste trabalho, o autor destacou partes relevantes de cada fundamento, excluindo partes atreladas ao mesmo, porém que não se tornam necessárias para o entendimento geral do trabalho apresentado.

Segundo ISO/IEC 17799 (2005), os atributos básicos da segurança de informação são:

- *Confidencialidade* – Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- *Integridade* - Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente);
- *Autenticidade* - Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;
- *Disponibilidade* - Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- *Não Repúdio* - Propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;
- *Conformidade* - Propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo;
- *Tempestividade* - Possibilidade de comprovar que um evento eletrônico ocorreu em um determinado instante;

2.1 Documento Eletrônico

O termo documento tem origem do latim *documentum*, que deriva de ensinar e indicar. Sendo assim um documento tem a função de indicar e guardar informações de um

individuo para si mesmo ou para outro. Com a evolução da distribuição de artefatos por meio da internet, e multiplicação da informação, criou-se o que chamamos de documento eletrônico, uma forma de tratar os documentos por meio do meio eletrônico. Documentos eletrônicos tem se tornado a principal forma de transferência de informações atualmente. “[...] é uma dada sequência de bits que, captada pelos nossos sentidos com o uso de um computador e um software específico, nos transmite uma informação.” (MARCACINI, 2000)

A característica de um documento é a possibilidade de ser observado futuramente, o documento narra um fato ou pensamento presente. Por isso é definido como uma prova histórica de algo ocorrido. Ações e atos realizados em tempo real se não registrados não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, "é lícito dizer que, na medida em que a técnica evolui permitindo registro permanente dos fatos sem fixá-lo de modo inseparável em alguma coisa corpórea, tal registro também pode ser considerado documento". A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível. Assim, renovando o conceito de documento, documento é o registro de um fato. "Se a técnica atual, mediante o uso da criptografia assimétrica, permite registro inalterável de um fato em meio eletrônico, a isto também podemos chamar de documento". (MARCACINI, 2000)

Figura 1 – Documento Eletrônico

Fonte: L3C (2017)

2.2 Criptografia

Criptografia é a escrita de forma ilegível. Cripto,do grego “kryptos”, significa escondido, oculto, e grafia, também do grego “graphos”, significa escrita.

O aspecto mais importante, segundo (STALLINGS, 2008), na segurança da informação, hoje, é a criptografia, como um componente básico de um computador. A criptografia é uma ciência que tem importância fundamental para a segurança da informação, ao servir de base para diversas tecnologias e protocolos, as propriedades garantidas como sigilo, integridade, autenticação e não-repúdio garantem o armazenamento, comunição e transações seguranas, essenciais no mundo atual.(NAKAMURA; GEUS, 2007)

Criptografia é um tipo de ciência para manter as mensagem seguras, a cifragem é o processo de disfarçar a mensagem original, o texto claro, de tal modo que a sua substância é escondida de uma mensagem com texto cifrado, enquanto a decifragem é o processo de transformar o texto cifrado de volta em texto claro original. A criptografia garante as seguintes propriedades: Integridade, Autenticidade, Não-Repúdio e Sigilo.(NAKAMURA; GEUS, 2007)

- *Texto claro:* Texto original, não cifrado;
- *Texto cifrado:* Texto ilegível, não compreensível;
- *Cifrar:* Transformar texto claro em texto cifrado;
- *Decifrar:* Transformar texto cifrado em texto plano;

"Cryptography is the art and science of encryption"(FERGUSON; SCHNEIER, 2003). Criptografia é usada hoje em dia como forma de autenticação, assinaturas digitais e muitas elementos de funções de segurança, não é apenas um termo utilizado por profissionais da área, mas de interesse de economistas, políticos, fisicos quanticos, entre outors. A criptografia abrange muitas áreas, com muitas direções o que torna algo tão complexo. "There is nobody in the world who knows everything about cryptography".(FERGUSON; SCHNEIER, 2003).

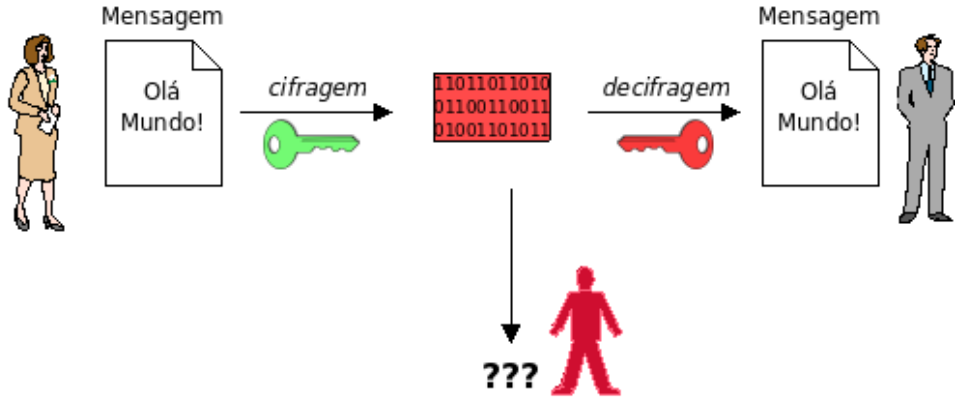
Além dessas propriedades, a assinatura digital e a certificação digital são importantes para proteção das informações. (NAKAMURA; GEUS, 2007).

2.2.1 Criptografia Assimétrica

Para sigilo das informações é utilizada uma chave para a codificação e decodifação dos dados, a chave representa a única forma de utilização dos dados, como em uma fechadura, a chave é única para abrir, no termo criptográfico, chave é a forma de cifrar e decifrar unicamente uma mensagem (BURNETT; PAINE, 2002), existem dois tipos de criptografica: simétrica e assimétrica, para este trabalho será apresentada apenas o conjunto de chaves assimétricas.

O algoritmo de chaves públicas ou assimétrica possibilita a troca de mensagens entre duas entidades, onde cada uma delas contém um par de chaves, público e privado. Uma mensagem por exemplo, pode ser cifrada utilizndo-se uma chave pública e decifrada utilizando somente a chave privada correspondente ou vice-versa. Dessa forma dificulta a ação de uma entidade externa que queira ler a mensagem, sem que tenha a chave privada da chave pública referente. (NAKAMURA; GEUS, 2007).

Figura 2 – Criptograia Assimétrica



Fonte: Cristian Moecke (2017)

Na figura, podemos ver que a entidade da esquerda utiliza a chave pública da entidade a direita para cifrar o texto, esta decifra o texto cifrado com a sua chave privada. Estas chaves são complementares, ou seja, tudo que é cifrado com uma, deve ser decifrado com a outra e vice versa.A chave privada é única e de posse privada da entidade, dessa forma qualquer mensagem cifrada com a chave pública pode ser lida apenas pela pessoa que têm a chave privada, e da mesma forma se a mensagem for cifrada pela chave privada, todos que tem a chave pública podem decifrar com a certeza de quem cifrou foi a pessoa. Estas duas abordagens, garantem respectivamente, a confidencialidade e autenticidade da mensagem. (NAKAMURA; GEUS, 2007).

2.2.2 Funções de resumo (HASH)

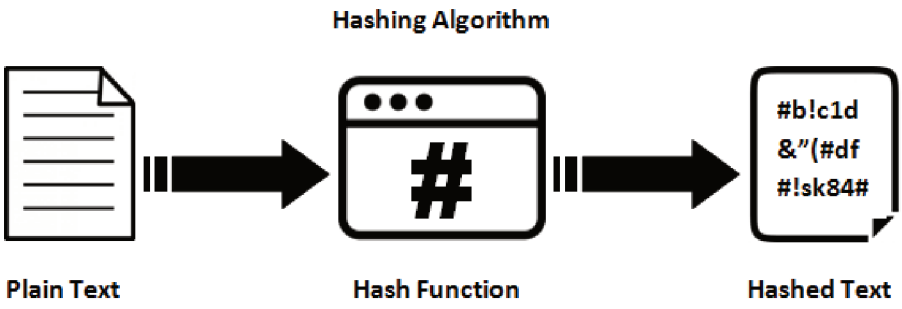
Hash são resumos criptográficos de uma informação e tem um papel fundamental na criptografia. Funções hash recebem uma mensagem como entrada e transformam em uma saída conhecida como hash (ALFRED; PAUL; SCOTT, 1996). "A hash algorithm is a check that protects data against most modification."(PFLEEGER, 1997). Algoritmos hashes tem a função de reduzir o documento em uma certa quantidade de bits, de forma única. (PFLEEGER, 1997).

"The ideal hash function is a random mapping from all possible input values to the set of possivle output values". (FERGUSON; SCHNEIER, 2003)

Algumas funções de hash são bem conhecidas, como o MD5, existem famílias como SHA ou SHA2 para algoritmos seguros de hash, um fator muito importante sobre esses algoritmos é o seu tamanho. Quanto maior o tamanho há mais segurança quanto aos seus hashes de saída. O resumo criptográfico de um dado, se utilizada a mesma função, será sempre o mesmo, ou seja, se um dado for modificado, o seu resumo criptográfico também será, garantindo assim a sua integridade. Como a quantidade de bits definido pelo algoritmo é limitada, podem existir colisões ou colisões parciais, resumos iguais para inputs diferentes. (FERGUSON; SCHNEIER, 2003)

"Hash fuctions produce a reduced form of a body of data such that most changes to the data will also change the reduced form."(PFLEEGER, 1997)

Figura 3 – Função Hash



Fonte: Stack Overflow (2012)

2.3 Assinatura digital

A assinatura digital pode ser obtida com uso de algoritmos de chave pública, O algoritmo de assinatura digital é aplicado sobre o resumo gerado (hash), com o usuário utilizando a chave assimétrica. O resultado, a assinatura digital pode ser adicionada junta a mensagem original. A assinatura digital permite assinar um documento eletrônico de forma mais segura e ágil, garantindo integridade, autenticidade e não repúdio de uma mensagem.(NAKAMURA; GEUS, 2007)

O algoritmo criptografico da assinatura tem origem em problemas matemáticos difíceis, alguns algoritmos que são comummente utilizados, são:

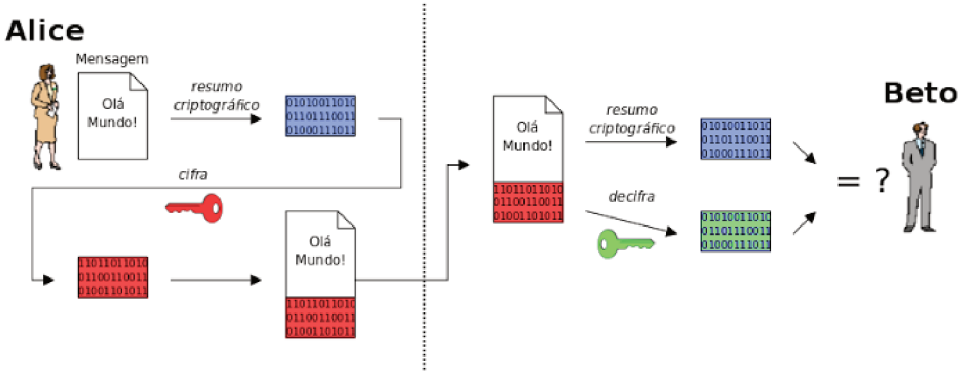
- *DLP:* Discrete Logarithm Problem, como o Diffie-Hellman e o DSA;
- *IFP:* Integer Factorization Problem, como o RSA;
- *ECDLP:* Elliptic Curve Discrete Logarithm Problem;

(NAKAMURA; GEUS, 2007)

Estes algoritmos são utilizados para encriptar um resumo com uma chave privada e produzir uma assinatura digital.(BURNETT; PAINE, 2002)

Cada fragmento de dados tem sua própria assinatura. Cada assinatura é única para os dados assinados e para as chaves utilizadas, Quando uma pessoa assina duas mensagem com a mesma chave, as assinaturas serão diferentes. E quando duas pessoas assinam o mesmo documento, a assinatura também será diferente. (BURNETT; PAINE, 2002)

Figura 4 – Assinatura Digital



Fonte: Cristian Moecke (2012)

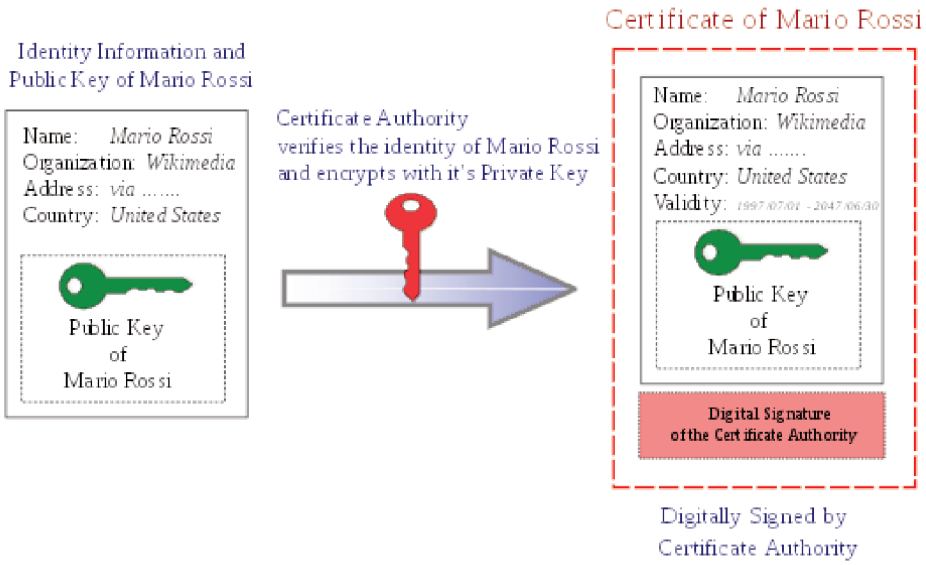
2.4 Certificado digital

"A maneira mais comum de saber se uma chave pública pertence ou não a entidade de destino é por meio de um certificado digital"(BURNETT; PAINE, 2002).

Um certificado Digital associa um nome a uma chave pública. Considerando este nome e chave pública como uma mensagem, é possível assina-la, desta forma o certificado são estes três itens juntos, as informações do proprietário, a chave pública e a assinatura da mesma. Quem deve assinar este certificado é sempre uma autoridade certificado, também chamada de CA.(BURNETT; PAINE, 2002)

Portanto, o certificado contém informações do proprietário do par de chaves e deve ter referência a quem o assinou. No Brasil existe um orgão que controla a infraestrutura de chaves públicas, ICP-Brasil. Todos os certificados possuem propriedades que determinam o nível de confiabilidade, como: Nome do solicitante, Chave pública do solicitante, Período de validade do certificado, Nome da AC, Política de utilização.(NAKAMURA; GEUS, 2007)

Figura 5 – Certificado Digital



Fonte: Wikipedia (2017)

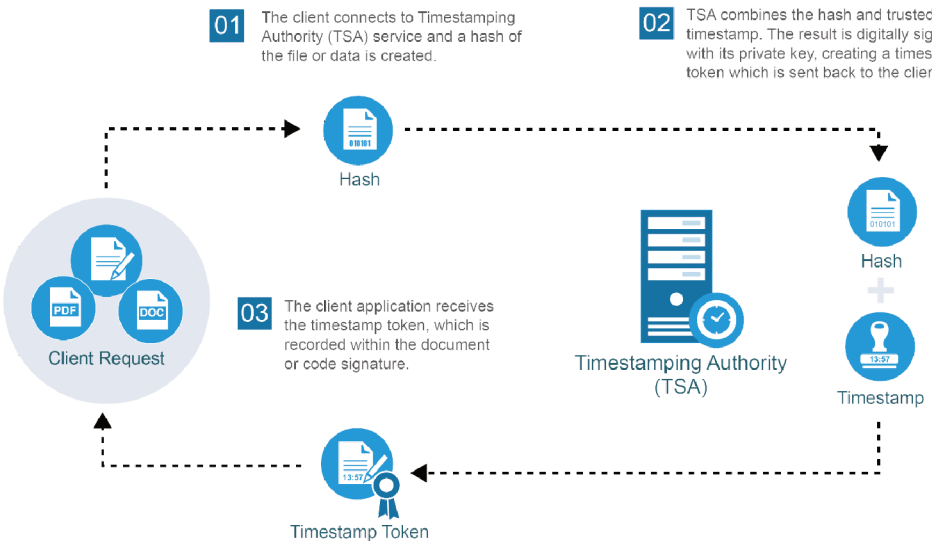
2.5 Carimbo do Tempo

Apesar de amplamente usadas, as assinaturas digitais podem rapidamente perder sua validade, o que constitui um desafio para a preservação daqueles documentos eletronicos que precisam ser guardados por um longo período de tempo. (SILVA; RAMOS; CUSTÓDIO, 2011).

carimbos do tempo, também conhecido como timestamp são documentos eletrônicos assinados por uma terceira parte confiável, denonimada Autoridade de Carimbo do Tempo (ACT), onde constam tanto o resumo criptográfico da informação datada, quanto a data em que o carimbo foi emitido. (SILVA; RAMOS; CUSTÓDIO, 2011).

Para prolongar a vida de uma assinatura digital, é inserida a esta assinatura um carimbo do tempo, com isto garantindo que em determinada data aquela assinatura era válida. (SILVA; RAMOS; CUSTÓDIO, 2011).

Figura 6 – Carimbo do Tempo



Fonte: Global Sign (2017)

2.6 Bitcoin

Bitcoin é uma criptomoeda, um ativo circulante sem controle centralizado, ou seja que não pertence a nenhum governo ou entidade central, que permite transações instantâneas ponto a ponto, e toda sua segurança está baseada em criptografia. (ARAÚJO; SILVA, 2017)

O Bitcoin hoje é uma moeda extremamente difundida, teve seu inicio em 2008, com o artigo de um pseudônimo, Satoshi Nakamoto. O conceito básico consiste em um livro razão

distribuído. (NAKAMOTO, 2008)

Bitcoin tinha por objetivo ser um livro-razão em que todas as transações financeiras ficassem armazenadas. (LUCENA; HENRIQUES, 2016)

O principal problema da economia atual é que a concentração do bem público é feita pela gestão de poucas pessoas e sem concorrência de serviços. O modo de operar o Bitcoin, moeda que alavancou a estrutura da blockchain foi dada a luz das ideias de Mises e Hayek, da escola Austríaca de economia, onde propuseram moedas concorrentes a taxas fixas e constantes, tais ideais são utilizados nas moedas como Bitcoin. (ARAÚJO; SILVA, 2017)

Durante a história dos países, houve muitos períodos de inflação e quedas do valor da moeda, quando isto ocorreu surgiram as primeiras organizações com ideias libertárias, buscando fugir das regras e controle do estado. Até hoje muitas pessoas mantém dinheiro em contas estrangeiras para fugir dos problemas que o estado impõe a sua própria moeda. Com esta tendência, criou-se o que é chamado de moedas livres, primeiro circulando apenas em locais isolados, sem grande repercussão. Nos EUA foi criado a Liberty Dollar, moeda que sofreu perseguição e foi atacada pelo FBI o que ocasionou o fim da moeda, porém nesta mesma época em 2008, uma moeda virtual descentralizada gerada por um algoritmo matemático, teria seu início. Assim surgindo a primeira criptomoeda, o Bitcoin. (ARAÚJO; SILVA, 2017)

"Fica consolidado que a ideia de um sistema livre de moeda, descentralizado e seguro, estaria em discussão como uma possível saída para o atual sistema econômico do país."(ARAÚJO; SILVA, 2017)

o Bitcoin foi considerado como a maior invenção tecnológica desde a criação da Internet. Bitcoin é uma moeda digital ponto a ponto (peer-to-peer), de código aberto e totalmente descentralizada. As transferências das moedas são feitas por meio de carteiras eletrônicas onde dois usuários podem trocar informações diretamente entre si, utilizando de criptografia e segurança digital para estabelecer toda a comunicação e permanência de estado.(RODRIGUES, 2016)

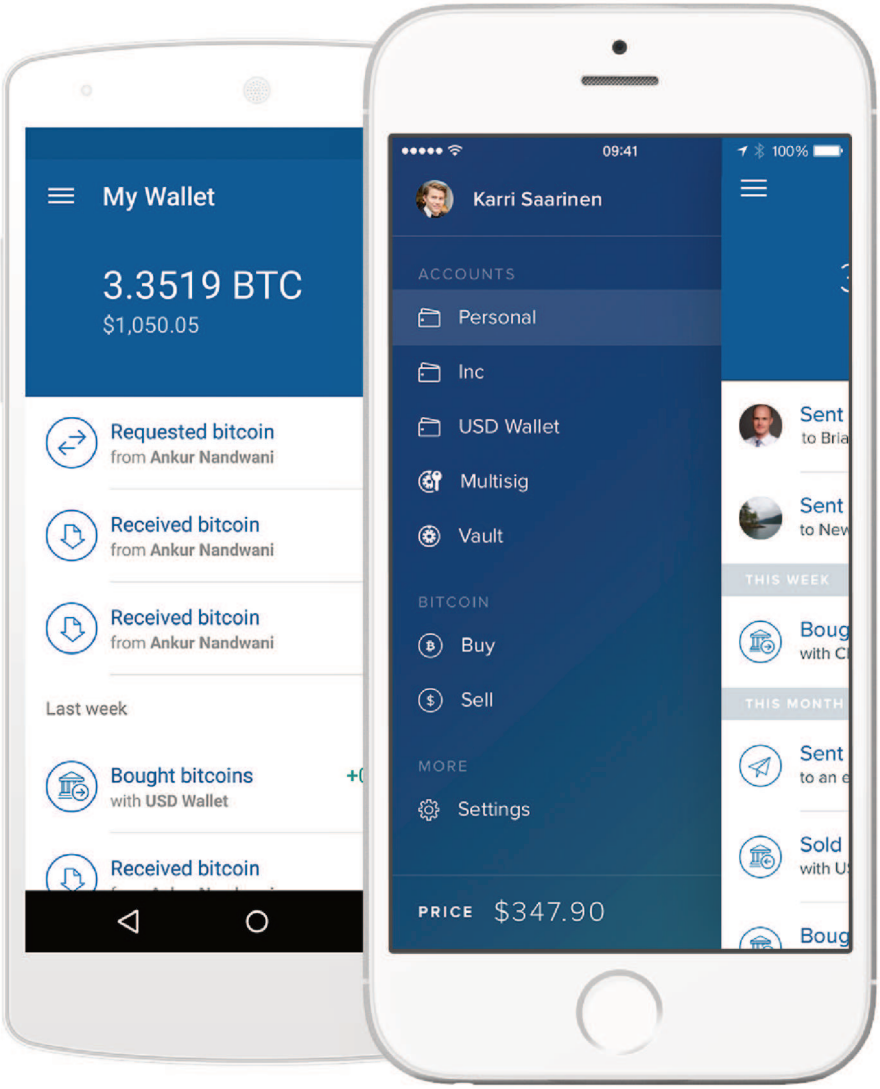
"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."(NAKAMOTO, 2008)

2.6.1 Wallets

As carteiras das criptomoedas baseiam-se no esquema de par de chaves (pública e privada), cada usuário detentor de uma carteira possui uma chave privada e assina uma transação utilizando hash com curvas elípticas. As transações possuem endereços de entrada e saída, e guardam as informações que serão trocadas e os valores da moeda para troca. (RODRIGUES, 2016)

Por ser uma carteira online, a sua wallet pode estar no computador ou no próprio celular, e apenas com a senha pessoal pode-se realizar as transações.

Figura 7 – Wallet



Fonte: CoinBase (2017)

2.7 Blockchain

Por trás do Bitcoin existe uma infraestrutura de banco de dados distribuído, chamado de Blockchain, onde cada bloco está associado ao bloco anterior, por isso, cadeia de blocos. Ele tem este nome pois é uma cadeia de objetos interligados entre si, cada bloco ligado ao bloco anterior, e distribuído entre todos os nós, por isso, block (bloco) chain (cadeia). (LUCENA; HENRIQUES, 2016)

O estudo da blockchain vem aumentando com o tempo, mais e mais conteúdo é lançado na web, documentos, códigos disponíveis para acesso e livros escritos para que a tecnologia seja expandida como um todo, muitas empresas passaram a utilizar o bitcoin como moeda para transações e bancos têm se adequado ao novo sistema. (RODRIGUES, 2016)

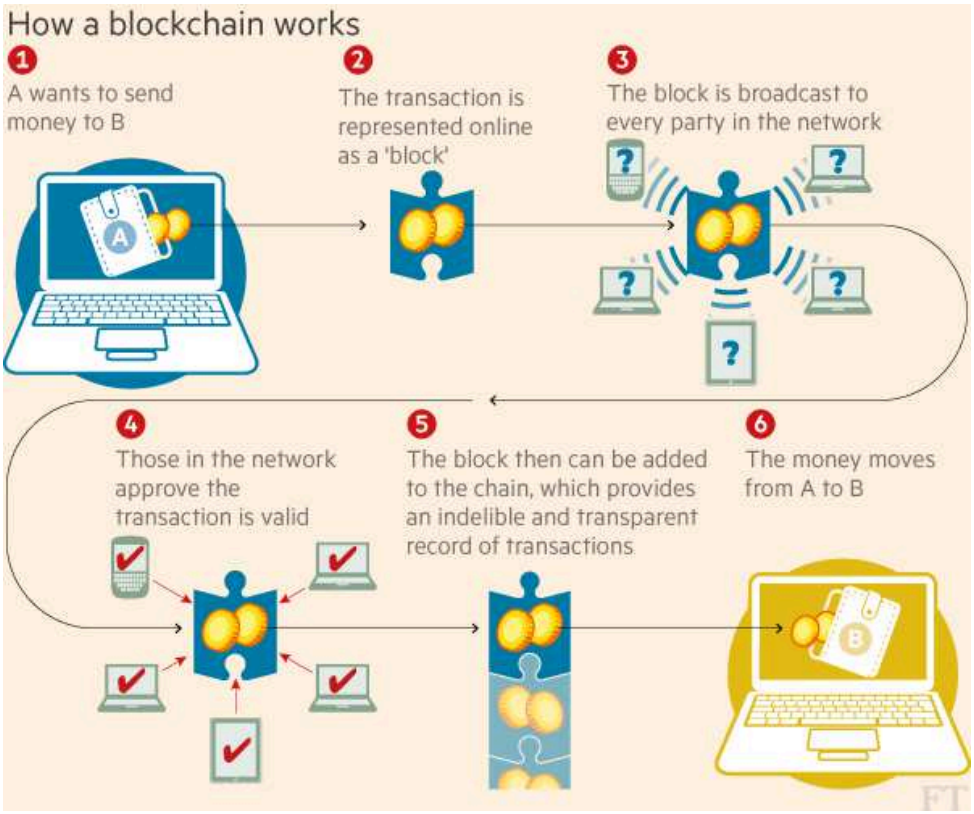
"A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties."(BITCOIN, 2015)

2.7.1 Como funciona?

O funcionamento se baseia nas funções de mão única (hash), registro do tempo (timestamp), assinatura digital, rede descentralizada peer-to-peer e mecanismo de geração de um novo bloco. Uma primeira transação tem seu valor hash calculado, em seguida, a próxima transação em conjunto com o hash da transação anterior também têm seu valor hash calculado e este processo continua até a última transação. Adicionado ao hash das transações é calculado o nonce do novo bloco e do bloco anterior. Desta forma o bloco anterior está ligado ao novo bloco, e assim sucessivamente. (LUCENA; HENRIQUES, 2016)

No blockchain, as transações que são feitas entre duas carteiras são armazenadas e após alcançarem 1mb, é fechado um bloco, selecionando as transações, cada transação é retirado um hash e assim sucessivamente até conter o hash completo do bloco fechado, este bloco contém o cabeçalho do bloco anterior, para ficar ligado a ele, o hash de todas as transações e um nonce (variável), onde é feita a mineração para encontrar uma confirmação de que o bloco é válido e pode ser inserido na cadeia. Após isso é enviado o bloco para toda a rede, assim sendo validado por todos. o tempo médio de criação de um bloco é determinado pelo protocolo, no caso do Bitcoin, 10 minutos para cada bloco.(RODRIGUES, 2016)

Figura 8 – Como Funciona



Fonte: World Economic Forum (2016)

2.7.2 Dificuldades

A escalabilidade do blockchain pode ser um problema, apesar de ter a maior liquidez, e por isso se tornar a mais valiosa, mas ela está estagnada a uma pequena circulação, a rede do Bitcoin suporta apenas 7 transações por segundo, valor muito abaixo do de qualquer sistema tradicional de pagamentos online. A visa por exemplo lida com 56000 transações por segundo. Portanto essa escalabilidade é um problema recorrente. (RODRIGUES, 2016)

Atualmente se propõe alterar os parâmetros do Bitcoin para que seja possível 4000 transações, porém as alterações poderiam levar a uma divisão da moeda, ou como é conhecido, hard fork. (RODRIGUES, 2016)

Outro problema aparente é o gasto duplo, imagina-se uma pessoa que tem apenas 1 bitcoin e faz duas transações enviando esse mesmo valor para duas outras carteiras como as transações ainda não foram confirmadas elas estarão válidas, caso uma transação seja validada primeiro que a outra é possível concluir que a conta de origem não tem mais o dinheiro, invalidando a segunda transação, mas caso as transações sejam efetivadas conjuntas é possível

que não se descubra o gasto duplo,sendo assim uma mesma moeda pode ser utilizada duas vezes se a informação não for distribuída a tempo para toda a rede e a informação da transação. Para resolver o problema de gasto duplo ao se utilizar a criptomoeda Bitcoin deve-se aguardar até 6 blocos para garantir a transferência entre todos os nós da rede e assegurar o uso único da moeda. (LUCENA; HENRIQUES, 2016)

2.7.3 Utilização

O Blockchain foi desenvolvido exclusivamente para aplicações financeiras, porém ele tem aplicações em outra áreas, como sistema financeiro onde é utilizado como mecanismo de armazenamento e processamento de transações. No armazenamento de Dados, onde documentos podem ser arquivados permanentemente e inalteráveis. Na distribuição de mídias, onde músicas e filmes possam ser armazenadas e utilizadas apenas pelo dono de determinado nó, impossibilitando cópia ou distribuição gratuíta. Na votação eletrônica, modelos seguros e distribuídos, onde não fosse possível adulteração de votos, substituindo as urnas eletrônicas. Identificadores pessoais como carteira de motorista, passaporte entre outros. (LUCENA; HENRIQUES, 2016)

2.7.4 Privada ou Pública

O Blockchain pode ser usado de forma privada ou pública, em uma blockchain pública, todos podem ler e enviar transações ou participar do processo de consenso, é o caso do Bitcoin e a maioria das criptomoedas conhecidas, não requer permissão para envio, validação das transações, onde todos permanecem anônimos. As blockchains privadas são comandadas por uma ou mais organizações, no caso de uma organização não haverá concorrência entre a geração de blocos, portanto é pouco viável para ambientes de produção, entretanto, é discutida a forma de consórcio, onde várias organizações de um determinado setor ou linha de produção, entram em consenso e utilizando a mesma arquitetura de blocos em banco de dados para organização. Concorrendo entre si e utilizando da melhor forma a infraestrutura. (BLOCKCHAIN..., 2018)

2.7.5 Método de Mineração

Atualmente existem inúmeros métodos de mineração dos blocos e mais conhecido e utilizado pelo Bitcoin é o Proof of Work (Prova de trabalho), onde cada minerador ou nó da rede busca encontrar uma colisão de hash estipulado pela rede. O segundo método mais conhecido é proof of stake, utilizado em uma altcoin (moeda alternativa) a Ethereum.

A natureza do Proof of Work significa que a criptografia depende do consumo de energia, apresentando custos indiretos significativos na operação de tais redes, que são suportadas pelos usuários através de uma combinação de taxas de inflação e transação. À medida que a taxa de mineração diminui na rede Bitcoin, eventualmente poderá exercer pressão sobre a elevação taxas de transação para manter um nível de segurança preferido.(KING; NADAL, 2012)

Um conceito denominado Proof of Stake foi discutido entre os círculos de Bitcoin já em 2011. Em termos aproximados, Proof of Stake significa uma forma de prova de propriedade da moeda. A idade da moeda consumida por uma transação pode ser considerada uma forma de prova de participação. (KING; NADAL, 2012)

Método de Mineração também é chamado de método de consenso. Um mecanismo de consenso é um algoritmo que serve para criar um novo bloco num ambiente descentralizado de forma consensual entre os nós da rede P2P.É uma nova solução para o dilema de atingir um consenso entre os usuários com um objetivo comum. (ALIAGA; HENRIQUES, 2017)

2.7.6 Proof of Work

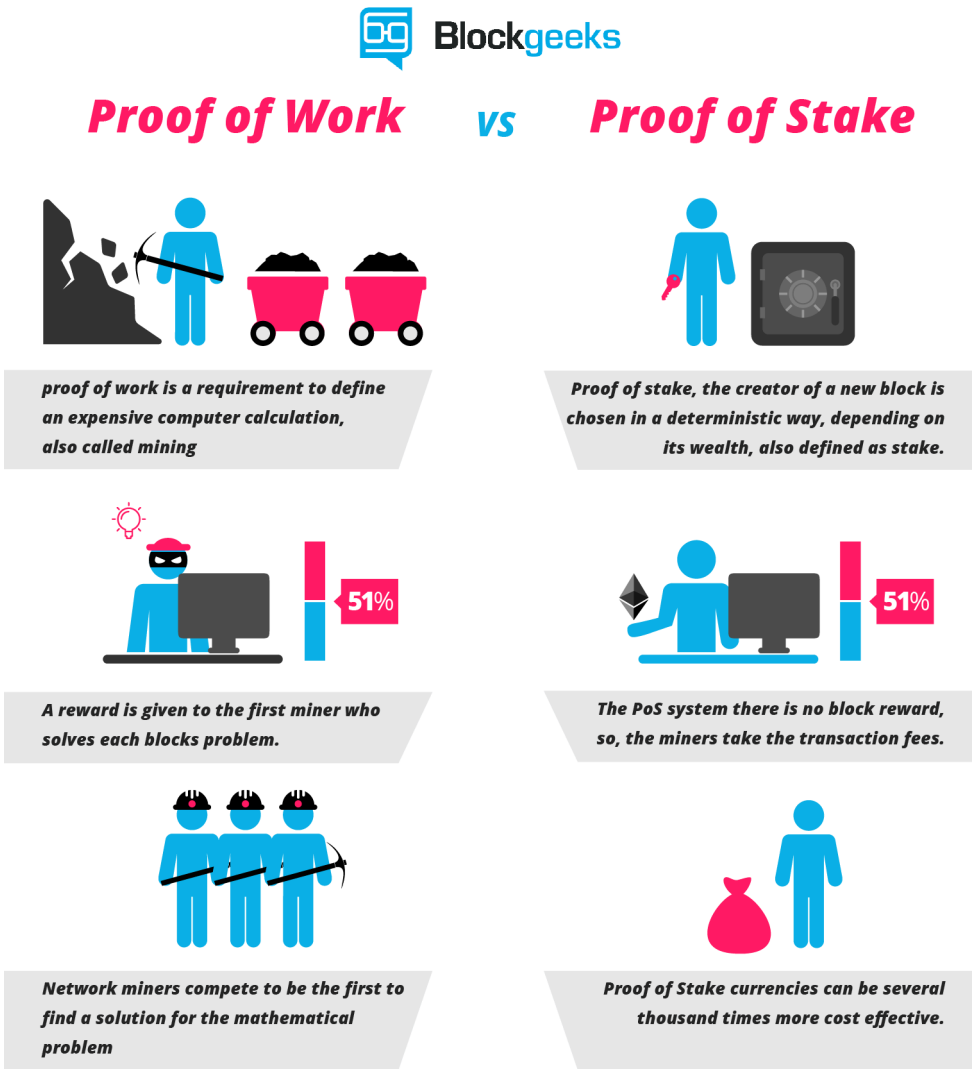
Quando a taxa de mineração do Proof of Work aproxima-se de zero, há cada vez menos incentivo para blocos serem minerados. Sob este cenário, o consumo de energia na rede pode cair para níveis muito baixos, já que os mineiros desinteressados param de extrair a prova de trabalho dos blocos. (KING, 2013)

Entre os pontos negativos destaca-se a necessidade de um grande poder computacional, o que resulta na concentração do poder de mineração entre aqueles que detém controle de uma grande quantidade de hardware capaz de trabalhar em paralelo.(ALIAGA; HENRIQUES, 2017)

Hoje já existem computadores especializados chamados Application Specific Integrated Circuits (ASICs), projetados para resolver a Prova de trabalho(POW) com a maior eficiência possível.(DASH, 2017)

Outros problemas, são o consumo excessivo de energia elétrica para fazer a mineração e o fato de dois nós mineradores poderem achar dois blocos válidos desde um mesmo bloco pai de forma quase simultânea. Tal ramificação é resolvida e não se mantém, pois há regras claras que determinam que a cadeia de blocos mais longa é a que será aceita pelos demais nós, sendo a outra totalmente abandonada. Isso acaba resultando em outro problema que é o desperdício de

Figura 9 – Proof of Work vs Proof of Stake



Fonte: BlockGeeks (2017)

energia e tempo, uma vez que todo o trabalho que vários nós estejam fazendo ao mesmo tempo para criar um novo bloco pode ser perdido a qualquer momento que um dos nós chegar primeiro à solução do hash desafio. (ALIAGA; HENRIQUES, 2017)

2.7.7 Proof of Stake

Proof of Stake não se trata sobre mineração, mas sobre validação. Em efeito os blocos ainda precisam ser criados da mesma forma, mas o processo de seleção tem certa aleatoriedade. A participação significa que você deposita algum dinheiro na rede e em certo sentido usa isso como garantia para adquirir um bloco. Em Proof of Stake é necessário confiar na cadeia com maior garantia.

É um mecanismo de consenso em que o sistema faz uma escolha do nó minerador que poderá criar um novo bloco. A forma usual da escolha é um sorteio cuja chance de ganhar é proporcional à quantidade de moedas que o nó já possui. É como se um nó rico em moedas (ou em qualquer outro parâmetro) tivesse mais bilhetes da loteria para concorrer com mais chances de ganhar. Seu gasto de energia é menor em comparação com Proof of Work e não depende de tanto poder computacional; (ALIAGA; HENRIQUES, 2017)

A estrutura da transação de Proof of Stake consiste na geração de um bloco para a rede, a operação de hashing é feita sobre um espaço de pesquisa limitado ao invés de um espaço de busca ilimitado como no Proof of Work, portanto, nenhum consumo significativo de energia está envolvida. O alvo de hash que o kernel de participação deve atender é um alvo por unidade de moeda. Assim, quanto mais a idade da moeda consumida na semente, mais fácil encontrar o protocolo de destino hash. Por exemplo, se Bob tiver uma carteira com moedas durante 10 dias que leve dois dias para geração, Alice com 20 dias levará 1 dia para encontrar o bloco.(KING; NADAL, 2012)

2.7.8 Outros Protocolos

Practical Byzantine Fault Tolerance (PBFT) Método onde um novo bloco é gerado em uma rodada e, em cada rodada, um nó primário é escolhido. Porém para funcionamento algum nó precisa conhecer toda a rede, este protocolo não pode ser utilizado em blockchains públicos. (ALIAGA; HENRIQUES, 2017)

Delegate Proof-of-Stake (DPOS) É semelhante ao Proof of Stake, porém existem stakeholders delegados para definir qual bloco será minerado. Pode ser alterado o tamanho do bloco e quantidade de transações. (ALIAGA; HENRIQUES, 2017)

Ripple O servidor tem uma lista de nós únicos (LNU) para realizar consultas, a qual é importante para o servidor, já que ajuda a determinar se uma transação está no livro razão. Este método é aplicável para blockchains privadas. (ALIAGA; HENRIQUES, 2017)

3 Proposta

Há proposta deste trabalho busca entender como funciona toda a arquitetura do blockchain e como o meio se comporta em relação a utilização de assinaturas digitais com validade temporal, garantida pela cadeia de blocos, pensando não somente na utilização de uma tecnologia inovadora, mas também no seu método de consenso, por ser um critério muito importante para a escolha de um tecnologia que seja sustentável.

A hipótese abordada foi a inclusão de documentos no Blockchain e obtenção da datação relativa. Como visto é possível a inclusão de dados e documentos nas arquiteturas e modelos de Blockchain, porém a questão mais importante é a precisão quanto a validade de um documento. A possibilidade da cadeia de blocos garantir com certo nível de precisão o momento em que uma assinatura digital foi gerada, e que um documento foi assinado.

A partir desta hipótese serão analisados algumas tecnologias apresentadas a seguir que utilizam Blockchain como sua estrutura e permitem o arquivamento de documentos por meio das transações e geração dos blocos.

3.1 Bitcoin

A primeira análise a ser feita é com a tecnologia mais conhecida e utilizada hoje pela grande parte do mundo, o Bitcoin vem tomando espaço a cada nova notícia gerada pela mídia, como explicado na fundamentação teórica o blockchain foi criado a partir da necessidade e confecção do Bitcoin, uma criptomoeda ou moeda digital.

Hoje é possível o arquivamento de documentos no Bitcoin, apesar de ser especificamente uma criptomoeda, com teor financeiro em sua origem, há diversos casos de transações contendo conteúdos de documentos e hash's de arquivos, para que possam estar guardados e seguros, garantindo a sua idade na história.

Entretanto, existem alguns pontos que inviabilizam e prejudicam a utilização do Bitcoin como forma de arquivamento de documentos, o primeiro ponto é o tempo de geração dos blocos, a forma de garantir que determinado documento está seguro e não será mais alterado é quando o documento faz parte de um bloco e começa a participar da cadeia imutável do

blockchain, porém como pode ser visto na figura 10, a média de geração de blocos definidas pelo protocolo é de cerca de 7 minutos, portanto teriamos um atraso de pelo menos 7 minutos na datação exata do documento, caso a transação seja efetivada no bloco seguinte a sua criação.

Figura 10 – Exploração de Blocos - Bitcoin

ÚLTIMOS BLOCOS MAIS... →

Altura	Era	Transações	Total Enviado	Transmitido Por	Tamanho (em kB)	Peso (kWU)
526961	13 minutes	1947	16,790.25 BTC	BTC.com	1,138.59	3,992.78
526960	27 minutes	153	641.85 BTC	AntPool	59.56	218.38
526959	28 minutes	1852	15,246.63 BTC	BTC.com	1,116.1	3,992.38
526958	47 minutes	1634	18,394.94 BTC	BTC.com	767.32	2,648.25

Fonte: Blockchain Info (2018a)

Outro ponto que reduz o uso do Bitcoin para o arquivamento de documentos, diz respeito também ao seu protocolo de geração de blocos, por conta na demora da geração dos blocos, há mais transações esperando para serem consolidadas em blocos que blocos efetivamente sendo criados, como pode ser visto na imagem, existem muitas transações pendentes, e hoje é discutido que existem transações que nunca serão efetivadas, o que pode garantir a efetivação de uma transação é a taxa que será fornecida ao minerador para que ele dê prioridade a transação colocando no bloco que será gerado. Porém o preço atualmente gira em torno de 40 dólares.

Figura 11 – Transações Não Confirmadas - Bitcoin

3538 Transações Não Confirmadas Lista atualizada em tempo real com as novas transações bitcoin

Resumo	Status: Conectado
Total das Taxas	87.55348847 BTC
Tamanho total	545449.578 (KB)
Transações por segundo	7.29

Fonte: Blockchain Info (2018b)

E por fim, o método de consenso utilizado pelo Bitcoin, conhecido como prova de

trabalho, utiliza uma quantidade enorme de energia o que confrontaria a idea de sustentabilidade advinda dos documentos eletrônicos para os antigos documentos físicos. Na figura 10 também é possível perceber quanto de energia foi consumida para a geração do bloco, atualmente o Bitcoin consome a mesma quantidade de energia que a Dinamarca produz. (CUSTO. . . , 2017)

3.2 Ethereum

Outra arquitetura que será analisada, sendo o segundo maior blockchain público, é o Ethereum. O Ethereum não é essencialmente uma criptomoeda, mas uma ide ou plataforma de desenvolvimento onde é possível definir contratos inteligentes com regras de negócios e diretrizes, sendo possível por exemplo em uma venda de produto a cobrança de juros automática quando os valores não forem pagos devidamente no prazo, estes contratos inteligentes, também conhecidos como smart contracts e é a peça preciosa do Ethereum.

Assim como no Bitcoin, é possível o arquivamento de documentos. Como o interesse principal é a imutabilidade de um documento, provando a sua integridade, não será tratado mais especificamente sobre os smart contracts. O Ethereum foi arquitetado por um jovem russo de 19 que planejou a maior parte da estrutura que seria aplicada ao Ethereum, publicando tudo em um white paper. Diferente do Bitcoin, no Ethereum o tempo de criação dos blocos foi reduzido para 17 segundos, processando cerca de 30 vezes mais transações que o Bitcoin e garantindo com certa precisão a questão principal que é a datação do documento e sequênciamento em blocos, assim que este fosse enviado para a rede. No entanto, Ethereum ainda utiliza proof of work como seu algoritmo de consenso, apesar do algoritmo do Ethereum (Ethash) ser menos custoso, ainda assim o gasto com energia para mineração dos blocos é expressivo. Há mudanças previstas para a transição de um algoritmo hibrido entre Proof of Work e Proof of Stake para a arquitetura, com o Ethereum Casper.

3.2.1 Ethereum Alarm Clock

Uma funcionalidade desenvolvida para o Ethereum é a Ethereum Alarm Clock, onde é possível fazer agendamentos de transações mediante a execução de smart contracts, é uma funcionalidade que pode garantir o processamento de um novo registro em bloco assim que uma assinatura for adicionada a um documento, ou um comando executado. (CUSTO. . . , 2017)

Entretanto, como no Bitcoin o preço do Eter (moeda virtual do Ethereum), vem

subindo e as transações podem se tornar custosas para quem deseja arquivar documentos com garantia e tempestividade.

3.3 Cronologic

A Arquitetura mais nova a ser analisada foi lançada no final do ano de 2017, contando com um brasileiro na sua equipe. É uma arquitetura que busca mudar a forma de consenso, ela utiliza a funcionalidade do Ethereum Alarm Clock e é baseada na primeira arquitetura Ethereum, entretanto a prova de consenso que se busca instalar é Proof of Time, onde a criação de tokens é dada pela passagem do tempo. Token's são instâncias de objetos reais em smart contracts.

Ainda em processo de desenvolvimento este pode ser um recurso utilizado, caso a geração de blocos seja parte do consenso, seria possível garantir que qualquer documento transacionado para este tipo de arquitetura, está seguro de modificações.

3.4 Hyperledger Fabric

O Hyperledger Fabric é uma implementação de estrutura blockchain e um dos projetos Hyperledger hospedados pela The Linux Foundation. Destinado como uma base para o desenvolvimento de aplicativos ou soluções com uma arquitetura modular. O Hyperledger Fabric aproveita a tecnologia de contêiner para hospedar contratos inteligentes chamados "chaincode", que compõem a lógica de aplicação do sistema.

Hyperledger concentra informações onde as transações são geradas e validadas sem tempo de espera, garantindo o momento exato da validação de uma transação, outro fator importante é o gasto que é cobrado pelas transações em blockchains públicas, onde é necessário o gasto de eter (Ethereum) ou Bitcoin para consolidação das transações. No caso de blockchains privadas este gasto se torna desnecessário. (HYPERLEDGER. . . , 2018a)

Hyperledger trabalha com duas formas de consenso Proof of Stake e Proof of Elapsed Time(PoET), que fornece uma escalabilidade parecida com a blockchain do bitcoin, mas sem o alto consumo de energia. (HYPERLEDGER. . . , 2018b)

3.5 Análise Geral

É necessário lembrar que a principal questão de funcionamento de um blockchain trata-se da não confiança entre as partes e a utilização do blockchain tras a confiança da tecnologia por meio da disputa pelas gerações de blocos.

Há diversos tipos de blockchains operando hoje, cada uma com suas características, é possível a utilização da maioria delas, porém algumas limitações podem não garantir o suporte ideal para a tempestividade, como visto a blockchain do Bitcoin leva cerca de 7 minutos em média, definido pelo protocolo, para a geração do bloco, onde também é possível que uma transação nunca seja efetivada, para tal, este modelo de blockchain não é viável, pois, é possível que seja feita uma assinatura digital com um certificado ICP Brasil, a assinatura é enviada para a nuvem de transações e deve esperar o tempo para ser anexada ao bloco, supondo que o certificado seja revogado entre o tempo de transação e geração de bloco, a assinatura digital passa a não ter mais validade, mesmo estando no bloco, pois o certificado utilizado na assinatura não pode garantir a tempestividade da assinatura. Portanto não podemos esperar o tempo de validação do bloco, assim deve ser utilizada uma tecnologia onde a transação seja transformada em bloco no momento preciso em que ela for criada.

Da mesma forma Ethereum pode sofrer das mesmas causas do Bitcoin, por ser uma plataforma pública. Quanto ao Cronologic é possível que a nova forma de conceito possa garantir tanto a validade temporal das transações quanto a utilização para arquivamento seguro de documentos;

A tecnologia que vem tomando mercado e em expansão, principalmente pela sua utilização com a IBM, é a Hyperledger Fabric, não só uma arquitetura blockchain, ele é um framework para implementação de blockchain onde é possível definir da melhor forma como se deseja utilizar a infraestrutura, sendo uma blockchain privada ela pode garantir tanto segurança dos dados, como privacidade, sem necessidade de custos para as transações.

3.6 Protótipos

Esta seção apresenta uma descrição de como pode ser desenvolvido o protótipo funcional de uma blockchain utilizando Hyperledger Fabric.

O primeiro protótipo e prova de conceito se concentrou na utilização e criação de

um blockchain peer-to-peer para comunicação entre as partes, como em um modelo funcional, viabilizando a utilização nas transações.

O segundo protótipo se preocupou com as questões legais e teóricas, criando por meio de uma ferramenta um conjunto de informações para a blockchain e criação dos blocos com suas transações, garantindo a datação das transações.

3.6.1 Peer-To-Peer

Antes de atentarmos para os protótipos é necessário entender outro conceito sobre Blockchain, Peer-to-Peer significa ponto a ponto, o que quer dizer que a conexão estabelecida entre dois pontos é direta, não há interlocução nem desvios.

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

A base do projeto Hyperledger Fabric pode ser encontrada sobre container's, principalmente distribuida pela IBM, com utilização do docker é possível subir uma instância do projeto e conectar nodos peer-to-peer para acesso. Sendo assim foi desenvolvida uma aplicação rápida para baixar os dados de container e subir instâncias para o carregamento de uma rede blockchain peer-to-peer e conseguir se comunicar.

Abaixo é possível encontrar o arquivo compose-yml utilizado para executar comandos dentro do docker.

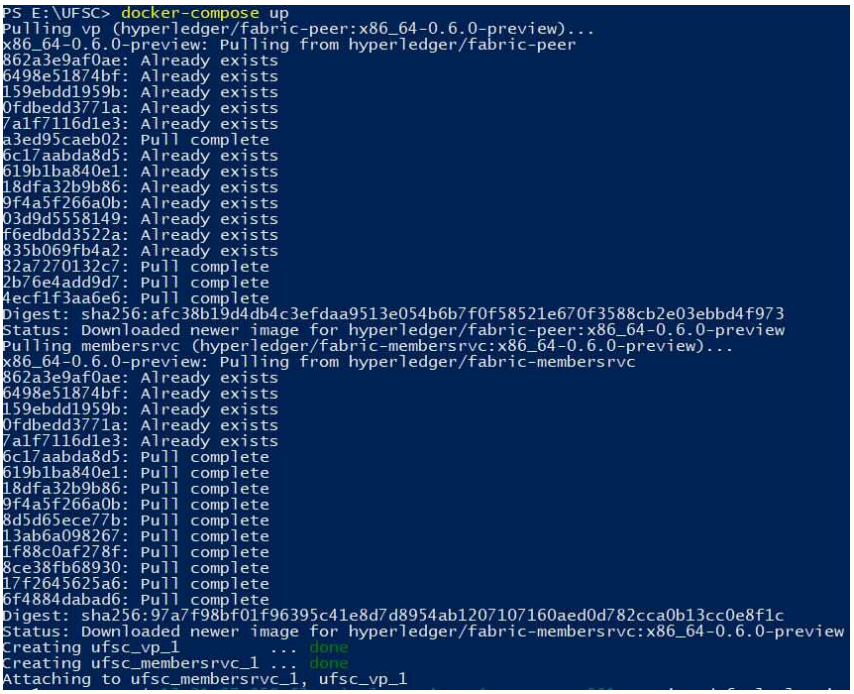
Antes de executar os comandos acima foi necessário utilização de uma máquina virtual com Linux, com o virtualizador VirtualBox, a execução passa a ser na VM linux, embora seja possível utilizar o PowerShell do Windows para visualizar suas interações.

Ao executar os comandos acima o docker se compromete com o trabalho de baixar os arquivos necessários e subir a instância do Hyperledger. Após carregar todas as imagens do Hyperledger ele passa a executar e aguardar as conexões peer to peer, criando a chaincode. Como pode ser visto nas imagens abaixo. (GUIA. . . , 2018)

Figura 12 – Docker Compose

Fonte: IBM Developer Workers (2016)

Figura 13 – Carregando Docker

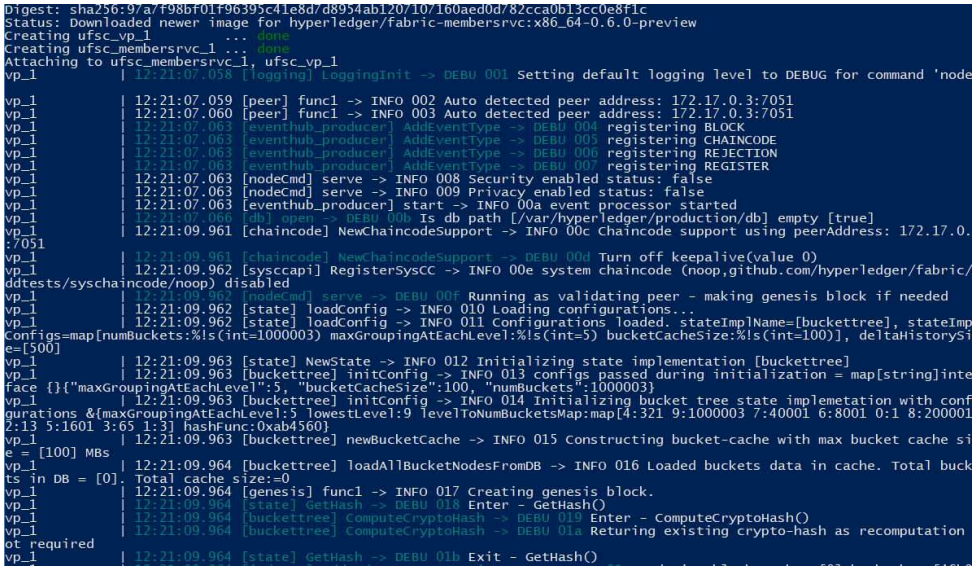


Fonte: Elaborado pelo Autor (2018)

3.6.2 Hyperledger Composer

o Hyperledger Composer tem o objetivo de tornar simples e rápida a construção de redes (chamadas Business Network) com contratos inteligentes e aplicativos que utilizem Blockchain. Oferece abstrações centradas no negócio, o que torna mais amigável o alinhamento entre os requisitos comerciais com o desenvolvimento técnico, tornando-se uma boa opção para criação de provas de conceito.

Figura 14 – Executando Hyperledger Fabric P2P



Fonte: Elaborado pelo Autor (2018)

Hyperledger Composer Playground é uma ferramenta desenvolvida pela IBM para orquestração de toda a arquiteura de uma blockchain, com ela é possível criar uma blockchain funcional, com parâmetros e atributos que a blockchain necessita e como ela irá se comportar, visualizando os testes com uma interface convidativa.

Configurando um sistema para gerênciamento de transações de documentos é possível obter o timestamp exato de uma transação que será assegurada pela sequência de blocos. Além de outras, é possível criar e extrair o código que irá gerir a blockchain. Utilizando a criação de testes para simulação de transações é possível a obtenção do timestamp da criação da transação no bloco.

Abaixo são demonstrados os testes realizados, criando uma arquitetura onde a transação se configura em uma criação de blocos em sequência e pode ser visto o momento exato em que esta foi realizada.

Figura 15 – Sequência de Blocos

Date, Time	Entry Type	Participant	
2018-06-01, 22:05:19	PublishBond	admin (NetworkAdmin)	view record
2018-06-01, 22:05:15	PublishBond	admin (NetworkAdmin)	view record
2018-06-01, 22:05:11	PublishBond	admin (NetworkAdmin)	view record

Fonte: Elaborado pelo Autor (2018)

Figura 16 – Informações da Transação


```
17      "periodMultiplier": 56060,
18      "period": "DAY"
19     },
20     "dayCountFraction": "Fugiat.",
21     "issuer": "resource:org.acme.bond.Issuer#0397"
22    },
23    "transactionId": "024924cf-787f-439f-a96a-a981d39ff721",
24    "timestamp": "2018-06-02T01:05:19.419Z"
25   }
```


Fonte: Elaborado pelo Autor (2018)

4 Conclusão

Os objetivos do presente trabalho foram alcançados, com os esforços foi possível entender toda a estrutura e tecnologia envolvida no conceito de Blockchain, esta estrutura de banco de dados distribuido que dá razão para muitas criptomoedas, garantindo segurança eletrônica, sendo um marco para as novas ações de tecnologia, foram discutidas algumas diretrizes do Blockchain, como a utilização privada e pública, os algoritmos e métodos de trabalho para validação dos blocos.

O intuito de validar a tecnologia como uma nova fonte segura de datação para documentos digitais foi alcançado, sendo demonstrado por meio de simulações o uso para tais fins.

A utilização de Hyperledger Fabric cumpre a maior parte dos requisitos, datação confiável, sem custo de transação e a utilização de Proof of Stake, o uso de blockchains privadas como concessionárias, onde grupos definidos detêm parte da tarefa de validação dos blocos também pode ser aplicado para o Hyperledger. Por outro lado foi possível confirmar que a utilização de blockchains de serviço público possam garantir todos os requisitos deste caso de uso proposto específico, o autor entende que para determinadas situaçãoes é possível a utilização mesmo com as arquiteturas aqui analisadas.

A pesquisa se concentrou no entendimento da estrutura blockchain e sua utilização com validação no tempo, as implementações utilizadas apenas foram para prova de conceito.

É possível então determinar que a utilização de blockchain pode garantir com determinada acurácia a tempestividade de documentos adicionados a ele. Entretando não foi encontrado nenhum produto que satisfaça todos os requisitos do caso de uso proposto, o que ainda se torna necessária a utilização de Carimbos do Tempo para segurança e datação confiável de assinaturas digitais.

5 Trabalhos futuros

O autor deixa como trabalhos futuros a utilização desta pesquisa para viabilizar um projeto de criação utilizando Hyperledger Fabric com consórcios para uma estrutura de blockchain no ITI, onde empresas privadas ou mesmo algumas instituições públicas possam fazer parte da rede de validação, garantindo a competitividade e funcionamento da estrutura.

O Autor ainda salienta que hoje no curto período de desenvolvimento do trabalho, foram encontradas e adaptadas novas formas de consenso para o blockchain, é importante avaliar a tolerância a falha bizantina que vem tomando bastante mercado e chamando a atenção no lançamento de novos papers.

6 Apêndice A

Estudo da Aplicação de Estrutura Blockchain com Proof of Stake para arquivamento de Documentos com Registro no Tempo

Otávio Augusto Corrêa[1]

[1]Sistemas de informação – Departamento de informática e estatística – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil

otavio.ssnt@gmail.com

Abstract. *A transfer of documents between entities has existed for many years, from proof of real estate, legal issues, to cases within companies, the high flow of documents has increased paper expenses, which are the basis of documents. With the increase of technology and the use of electronic devices, we have created what is called an electronic document. But if with real documents already found frauds, with electronic documents this insecurity is even greater, a modification of the bytes or variables of a document in question, leave at risk a security and confidence of itself. To solve this problem with what is called Digital Signature, a document must be signed by a single and single person possession. But all that came at once per period of validity of this signature. For this, the time stamp was created, which proves in certain data, this document was signed. All this infrastructure to ensure the validity of a document has a high cost, with the proposal of this study, the author evaluated the feasibility of a blockchain-based distributed database structure where the files can be stored reliably, without having problems with your security, alterations or frauds, similar to the time stamp process.*

Resumo. *A transferência de documentos entre entidades existe a muitos anos, desde comprovações de imóveis, decisões jurídicas, até processos dentro das empresas, o alto fluxo de documentos aumentou os gastos com papel, matéria base dos documentos. Com o aumento da tecnologia e utilização de aparelhos eletrônicos, criou-se o que é chamado de documento eletrônico. Porém se com documentos reais fraudes já eram encontradas, com documentos eletrônicos essa insegurança é ainda maior, a modificação dos bytes ou variáveis de um documento poderiam deixar em risco a segurança e confiança do mesmo. Para resolver esta questão foi criado o que é chamado Assinatura Digital, um documento poderia ser assinado por uma chave que somente uma pessoa tivesse posse. Mas outra questão que veio a tona foi o período de validade desta assinatura. Para isso foi criado o carimbo do tempo, que comprova que em determinada data, este documento foi assinado. Toda esta infraestrutura para garantir a validade de um documento tem um custo elevado, com a proposta deste estudo, o autor avaliou a viabilidade de uma estrutura de banco de dados distribuídos baseada em blockchain onde os arquivos possam ser armazenados confiavelmente, sem que tenha problemas com sua segurança, alterações ou fraudes, semelhante ao processo de carimbo do tempo.*

1. Introdução

Vivemos em um século marcado pelo predomínio do conhecimento e da informação, a Internet nos proporciona maior eficiência e rapidez na transmissão de dados e produção. Através do seu acesso, barreiras são desfeitas, permitindo que pessoas se reúnam em lugares virtuais. (GANDINI; SALOMÃO; JACOB, 2001).

Com toda essa informação, é necessário garantir a validade na troca de informações, a assinatura digital é utilizada para agregar confiança e segurança às comunicações e negócios vinculados a um ambiente virtual como a Internet, oferecendo eficiência e rapidez. Além disso, a assinatura digital contribui de forma positiva para o meio ambiente, empresas que armazenam milhares de documentos poderiam digitalizar os mesmos, garantindo a sua validade jurídica através de assinaturas digitais (MENKE, 2003).

Carimbo do Tempo é um documento eletrônico emitido por uma entidade confiável, que serve como evidência de que um documento assinado existia em determinada data e hora no passado, associando-se data de fonte confiável ao hash desse documento assinado. (SILVA; RAMOS; CUSTÓDIO, 2011).

Blockchain é uma estrutura de banco de dados distribuído. Ele foi primariamente desenvolvido para um sistema de criptomoeda chamado de BitCoin, porém é a estrutura de dados por trás do sistema conhecido. Além de distribuído, é descentralizado, não existe uma entidade central para gerir os dados.(LUCENA; HENRIQUES, 2016).

O Blockchain funciona como uma cadeia de blocos, onde estão ligados o bloco anterior ao próximo bloco, formando uma cadeia. Cada bloco contém as transações que serão efetuadas. Estas transações são Peer-to-peer, emissor ligado diretamente ao receptor, ou como no caso do Bitcoin uma wallet envia dados para outra wallet.(RODRIGUES, 2016). Os blocos após serem gerados são distribuídos para toda a rede que compõem a Blockchain, assim todas as partes contém a informação das transações feitas, a segurança está em que se houver um ataque tentando modificar alguma transação e consequentemente um bloco, o ataque terá que modificar mais da metade da rede. (RODRIGUES, 2016)

Todos estes pontos serão abordados neste trabalho e por meio deste é feito um estudo sobre a arquitetura Blockchain, destrinchando todos seus atributos e feita uma análise dentre as principais arquiteturas para viabilizar uma que se adeque melhor ao caso proposto de arquivamentos de documentos com registro no tempo.

2. Fundamentação

2.1. Documento Eletrônico

O termo documento tem origem do latim documentum, que deriva de ensinar e indicar. Sendo assim um documento tem a função de indicar e guardar informações de um indivíduo para si mesmo ou para outro. Com a evolução da distribuição de artefatos por meio da internet, e multiplicação da informação, criou-se o que chamamos de documento eletrônico, uma forma de tratar os documentos por meio do meio eletrônico. Documentos eletrônicos tem se tornado a principal forma de transferência de informações atualmente. “[...] é uma dada sequência de bits que, captada pelos nossos sentidos com o uso de um

computador e um software específico, nos transmite uma informação.” (MARCACINI, 2000).

2.2. Criptografia

Criptografia é a escrita de forma ilegível. Cripto, do grego “kryptos”, significa escondido, oculto, e grafia, também do grego “graphos”, significa escrita. Criptografia é um tipo de ciência para manter as mensagem seguras, a cifragem é o processo de disfarçar a mensagem original, o texto claro, de tal modo que a sua substância é escondida de uma mensagem com texto cifrado, enquanto a decifragem é o processo de transformar o texto cifrado de volta em texto claro original. A criptografia garante as seguintes propriedades: Integridade, Autenticidade, Não-Repúdio e Sigilo.(NAKAMURA; GEUS, 2007).

2.3. Criptografia assimétrica

Para sigilo das informações é utilizada uma chave para a codificação e decodificação dos dados, a chave representa a única forma de utilização dos dados, como em uma fechadura, a chave é única para abrir, no termo criptográfico, chave é a forma de cifrar e decifrar unicamente uma mensagem (BURNETT; PAINE, 2002), existem dois tipos de criptografia: simétrica e assimétrica, para este trabalho será apresentada apenas o conjunto de chaves assimétricas.

O algoritmo de chaves públicas ou assimétrica possibilita a troca de mensagens entre duas entidades, onde cada uma delas contém um par de chaves, público e privado. Uma mensagem por exemplo, pode ser cifrada utilizando-se uma chave pública e decifrada utilizando somente a chave privada correspondente ou vice-versa. Dessa forma dificulta a ação de uma entidade externa que queira ler a mensagem, sem que tenha a chave privada da chave pública referente. (NAKAMURA; GEUS, 2007).

2.4. Funções de resumo criptográfico

Funções hash de resumo criptográfico tem um papel fundamental na criptografia. Funções hash recebem uma mensagem como entrada e transformam em uma saída conhecida como hash [ALFRED; PAUL; SCOTT 1996].

Algumas funções de hash são bem conhecidas, como o MD5, existem famílias como SHA ou SHA2 para algoritmos seguros de hash, um fator muito importante sobre esses algoritmos é o seu tamanho. Quanto maior o tamanho há mais segurança quanto aos seus hashes de saída. O resumo criptográfico de um dado, se utilizada a mesma função, será sempre o mesmo, ou seja, se um dado for modificado, o seu resumo criptográfico também será, garantindo assim a sua integridade. Como a quantidade de bits definido pelo algoritmo é limitada, podem existir colisões ou colisões parciais, resumos iguais para inputs diferentes. (FERGUSON; SCHNEIER, 2003).

2.5. Assinatura digital

A assinatura digital pode ser obtida com uso de algoritmos de chave pública, O algoritmo de assinatura digital é aplicado sobre o resumo gerado (hash), com o usuário utilizando a chave assimétrica. O resultado, a assinatura digital pode ser adicionada junta a mensagem original. A assinatura digital permite assinar um documento eletrônico de forma mais segura e ágil, garantindo integridade, autenticidade e não repúdio de uma mensagem.(NAKAMURA; GEUS, 2007).

2.6. Certificado digital

Um certificado Digital associa um nome a uma chave pública. Considerando este nome e chave pública como uma mensagem, é possível assiná-la, desta forma o certificado são estes três itens juntos, as informações do proprietário, a chave pública e a assinatura da mesma. Quem deve assinar este certificado é sempre uma autoridade certificado, também chamada de CA.(BURNETT; PAINE, 2002).

Portanto, o certificado contém informações do proprietário do par de chaves e deve ter referência a quem o assinou. No Brasil existe um órgão que controla a infraestrutura de chaves públicas, ICP-Brasil. Todos os certificados possuem propriedades que determinam o nível de confiabilidade, como: Nome do solicitante, Chave pública do solicitante, Período de validade do certificado, Nome da AC, Política de utilização.(NAKAMURA; GEUS, 2007).

2.7. Carimbo do Tempo

Apesar de amplamente usadas, as assinaturas digitais podem rapidamente perder sua validade, o que constitui um desafio para a preservação daqueles documentos eletrônicos que precisam ser guardados por um longo período de tempo. (SILVA; RAMOS; CUSTÓDIO, 2011). Carimbos do tempo, também conhecido como timestamp são documentos eletrônicos assinados por uma terceira parte confiável, denominada Autoridade de Carimbo do Tempo (ACT), onde constam tanto o resumo criptográfico da informação datada, quanto a data em que o carimbo foi emitido. (SILVA; RAMOS; CUSTÓDIO, 2011).

2.8. Bitcoin

Bitcoin é uma criptomoeda, um ativo circulante sem controle centralizado, ou seja que não pertence a nenhum governo ou entidade central, que permite transações instantâneas ponto a ponto, e toda sua segurança está baseada em criptografia. (ARAÚJO; SILVA, 2017).

Bitcoin tinha por objetivo ser um livro-razão em que todas as transações financeiras ficassem armazenadas. (LUCENA; HENRIQUES, 2016)

"Fica consolidado que a ideia de um sistema livre de moeda, descentralizado e seguro, estaria em discussão como uma possível saída para o atual sistema econômico do país."(ARAÚJO; SILVA, 2017) .

2.9. Blockchain

Por trás do Bitcoin existe uma infraestrutura de banco de dados distribuído, chamado de Blockchain, onde cada bloco está associado ao bloco anterior, por isso, cadeia de blocos. Ele tem este nome pois é uma cadeia de objetos interligados entre si, cada bloco ligado ao bloco anterior, e distribuído entre todos os nós, por isso, block (bloco) chain (cadeia). (LUCENA; HENRIQUES, 2016).

2.9.1. Como Funciona

O funcionamento se baseia nas funções de mão única (hash), registro do tempo (timestamp), assinatura digital, rede descentralizada peer-to-peer e mecanismo de geração de um novo bloco. Uma primeira transação tem seu valor hash calculado, em seguida, a próxima transação em conjunto com o hash da transação anterior também têm seu valor

hash calculado e este processo continua até a última transação. Adicionado ao hash das transações é calculado o nonce do novo bloco e do bloco anterior. Desta forma o bloco anterior está ligado ao novo bloco, e assim sucessivamente. (LUCENA; HENRIQUES, 2016).

No blockchain, as transações que são feitas entre duas carteiras são armazenadas e após alcançarem 1mb, é fechado um bloco, selecionando as transações, cada transação é retirado um hash e assim sucessivamente até conter o hash completo do bloco fechado, este bloco contém o cabeçalho do bloco anterior, para ficar ligado a ele, o hash de todas as transações e um nonce (variável), onde é feita a mineração para encontrar uma confirmação de que o bloco é válido e pode ser inserido na cadeia. Após isso é enviado o bloco para toda a rede, assim sendo validado por todos. o tempo médio de criação de um bloco é determinado pelo protocolo, no caso do Bitcoin, 10 minutos para cada bloco.(RODRIGUES, 2016).

2.9.2 Método de Mineração

Método de Mineração também é chamado de consenso. Atualmente existem inúmeros métodos de mineração dos blocos e mais conhecido e utilizado pelo Bitcoin é o Proof of Work (Prova de trabalho), onde cada minerador ou nó da rede busca encontrar uma colisão de hash estipulado pela rede. O segundo método mais conhecido é proof of stake, utilizado em uma altcoin (moeda alternativa) a Ethereum.

A natureza do Proof of Work significa que a criptografia depende do consumo de energia, apresentando custos indiretos significativos na operação de tais redes, que são suportadas pelos usuários através de uma combinação de taxas de inflação e transação. À medida que a taxa de mineração diminui na rede Bitcoin, eventualmente poderá exercer pressão sobre a elevação taxas de transação para manter um nível de segurança preferido.(KING; NADAL, 2012).

Um conceito denominado Proof of Stake foi discutido entre os círculos de Bitcoin já em 2011. Em termos aproximados, Proof of Stake significa uma forma de prova de propriedade da moeda. A idade da moeda consumida por uma transação pode ser considerada uma forma de prova de participação. (KING; NADAL, 2012).

3. Proposta

Há proposta deste trabalho busca entender como funciona toda a arquitetura do blockchain e como o meio se comporta em relação a utilização de assinaturas digitais com validade temporal, garantida pela cadeia de blocos, pensando não somente na utilização de uma tecnologia inovadora, mas também no seu método de consenso, por ser um critério muito importante para a escolha de um tecnologia que seja sustentável.

A hipótese abordada foi a inclusão de documentos no Blockchain e obtenção da datação relativa. Como visto é possível a inclusão de dados e documentos nas arquiteturas e modelos de Blockchain, porém a questão mais importante é a precisão quanto a validade de um documento. A possibilidade da cadeia de blocos garantir com certo nível de precisão o momento em que uma assinatura digital foi gerada, e que um documento foi assinado.

A partir desta hipótese serão analisados algumas tecnologias apresentadas a seguir que utilizam Blockchain como sua estrutura e permitem o arquivamento de documentos por meio das transações e geração dos blocos.

3.1. Bitcoin

Hoje é possível o arquivamento de documentos no Bitcoin, apesar de ser especificamente uma criptomoeda, com teor financeiro em sua origem, há diversos casos de transações contendo conteúdos de documentos e hashes de arquivos, para que possam estar guardados e seguros, garantindo a sua idade na história. Entretanto, existem alguns pontos que inviabilizam e prejudicam a utilização do Bitcoin como forma de arquivamento de documentos, o primeiro ponto é o tempo de geração dos blocos, a forma de garantir que determinado documento está seguro e não será mais alterado é quando o documento faz parte de um bloco e começa a participar da cadeia imutável do blockchain, porém a média de geração de blocos definidas pelo protocolo é de cerca de 7 minutos, portanto teríamos um atraso de pelo menos 7 minutos na datação exata do documento, caso a transação seja efetivada no bloco seguinte a sua criação.

Outro ponto que reduz o uso do Bitcoin para o arquivamento de documentos, diz respeito também ao seu protocolo de geração de blocos, por conta na demora da geração dos blocos, há mais transações esperando para serem consolidadas em blocos que blocos efetivamente sendo criados, como pode ser visto na imagem, existem muitas transações pendentes, e hoje é discutido que existem transações que nunca serão efetivadas, o que pode garantir a efetivação de uma transação é a taxa que será fornecida ao minerador para que ele dê prioridade a transação colocando no bloco que será gerado. Porém o preço atualmente gira em torno de 40 dólares.

E por fim, o método de consenso utilizado pelo Bitcoin, conhecido como prova de trabalho, utiliza uma quantidade enorme de energia o que confrontaria a ideia de sustentabilidade advinda dos documentos eletrônicos para os antigos documentos físicos. Atualmente o Bitcoin consome a mesma quantidade de energia que a Dinamarca produz. (CUSTO. . . , 2017).

3.2. Ethereum

Outra arquitetura que será analisada, sendo o segundo maior blockchain público, é o Ethereum. O Ethereum não é essencialmente uma criptomoeda, mas uma ide ou plataforma de desenvolvimento onde é possível definir contratos inteligentes com regras de negócios e diretrizes, sendo possível por exemplo em uma venda de produto a cobrança de juros automática quando os valores não forem pagos devidamente no prazo, estes contratos inteligentes, também conhecidos como smart contracts e é a peça preciosa do Ethereum.

Assim como no Bitcoin, é possível o arquivamento de documentos. Como o interesse principal é a imutabilidade de um documento, provando a sua integridade, não será tratado mais especificamente sobre os smart contracts. O Ethereum foi arquitetado por um jovem russo de 19 que planejou a maior parte da estrutura que seria aplicada ao Ethereum, publicando tudo em um white paper. Diferente do Bitcoin, no Ethereum o tempo de criação dos blocos foi reduzido para 17 segundos, processando cerca de 30 vezes mais transações que o Bitcoin e garantindo com certa precisão a questão principal que é a datação do documento e sequenciamento em blocos, assim que este fosse enviado para a rede. No entanto, Ethereum ainda utiliza proof of work como seu algoritmo de consenso, apesar do algoritmo do Ethereum (Ethash) ser menos custoso, ainda assim o gasto com energia para mineração dos blocos é expressivo. Há mudanças previstas para a transição de um algoritmo híbrido entre Proof of Work e Proof of Stake para a arquitetura, com o Ethereum Casper.

3.3. Hyperledger Fabric

O Hyperledger Fabric é uma implementação de estrutura blockchain e um dos projetos Hyperledger hospedados pela The Linux Foundation. Destinado como uma base para o desenvolvimento de aplicativos ou soluções com uma arquitetura modular. O Hyperledger Fabric aproveita a tecnologia de contêiner para hospedar contratos inteligentes chamados "chain code", que compõem a lógica de aplicação do sistema.

Hyperledger concentra informações onde as transações são geradas e validadas sem tempo de espera, garantindo o momento exato da validação de uma transação, outro fator importante é o gasto que é cobrado pelas transações em blockchains públicas, onde é necessário o gasto de éter (Ethereum) ou Bitcoin para consolidação das transações. No caso de blockchains privadas este gasto se torna desnecessário. (HYPERLEDGER. . . , 2018a)

4. Análise Geral

É necessário lembrar que a principal questão de funcionamento de um blockchain trata-se da não confiança entre as partes e a utilização do blockchain traz a confiança da tecnologia por meio da disputa pelas gerações de blocos.

Há diversos tipos de blockchains operando hoje, cada uma com suas características, é possível a utilização da maioria delas, porém algumas limitações podem não garantir o suporte ideal para a tempestividade, como visto a blockchain do Bitcoin leva cerca de 7 minutos em média, definido pelo protocolo, para a geração do bloco, onde também é possível que uma transação nunca seja efetivada, para tal, este modelo de blockchain não é viável, pois, é possível que seja feita uma assinatura digital com um certificado ICP Brasil, a assinatura é enviada para a nuvem de transações e deve esperar o tempo para ser anexada ao bloco, supondo que o certificado seja revogado entre o tempo de transação e geração de bloco, a assinatura digital passa a não ter mais validade, mesmo estando no bloco, pois o certificado utilizado na assinatura não pode garantir a tempestividade da assinatura. Portanto não podemos esperar o tempo de validação do bloco, assim deve ser utilizada uma tecnologia onde a transação seja transformada em bloco no momento preciso em que ela for criada.

A tecnologia que vem tomando mercado e em expansão, principalmente pela sua utilização com a IBM, é a Hyperledger Fabric, não só uma arquitetura blockchain, ele é um framework para implementação de blockchain onde é possível definir da melhor forma como se deseja utilizar a infraestrutura, sendo uma blockchain privada ela pode garantir tanto segurança dos dados, como privacidade, sem necessidade de custos para as transações.

5. Prova de Conceito

Hyperledger Composer Playground é uma ferramenta desenvolvida pela IBM para orquestração de toda a arquitetura de uma blockchain, com ela é possível criar uma blockchain funcional, com parâmetros e atributos que a blockchain necessita e como ela irá se comportar, visualizando os testes com uma interface convidativa.

Configurando um sistema para gerenciamento de transações de documentos é possível obter o timestamp exato de uma transação que será assegurada pela sequência de blocos. Além de outras, é possível criar e extrair o código que irá gerir a blockchain. Utilizando a

criação de testes para simulação de transações é possível a obtenção do timestamp da criação da transação no bloco. viável, pois, é possível que seja feita uma assinatura digital com um certificado ICP Brasil, a assinatura é enviada para a nuvem de transações e deve esperar o tempo para ser anexada ao bloco, supondo que o certificado seja revogado entre o tempo de transação e geração de bloco, a assinatura digital passa a não ter mais validade, mesmo estando no bloco, pois o certificado utilizado na assinatura não pode garantir a tempestividade da assinatura. Portanto não podemos esperar o tempo de validação do bloco, assim deve ser utilizada uma tecnologia onde a transação seja transformada em bloco no momento preciso em que ela for criada.

6 Considerações finais

Os objetivos do presente trabalho foram alcançados, com os esforços foi possível entender toda a estrutura e tecnologia envolvida no conceito de Blockchain, esta estrutura de banco de dados distribuido que dá razão para muitas criptomoedas, garantindo segurança eletrônica, sendo um marco para as novas ações de tecnologia, foram discutidas algumas diretrizes do Blockchain, como a utilização privada e pública, os algoritmos e métodos de trabalho para validação dos blocos.

O intuito de validar a tecnologia como uma nova fonte segura de datação para documentos digitais foi alcançado, sendo demonstrado por meio de simulações o uso para tais fins.

7 Conclusão

A utilização de Hyperledger Fabric cumpre a maior parte dos requisitos, datação confiável, sem custo de transação e a utilização de Proof of Stake, o uso de blockchains privadas como concessionárias, onde grupos definidos detêm parte da tarefa de validação dos blocos também pode ser aplicado para o Hyperledger. Por outro lado foi possível confirmar que a utilização de blockchains de serviço público possam garantir todos os requisitos deste caso de uso proposto específico, o autor entende que para determinadas situações é possível a utilização mesmo com as arquiteturas aqui analisadas.

A pesquisa se concentrou no entendimento da estrutura blockchain e sua utilização com validação no tempo, as implementações utilizadas apenas foram para prova de conceito.

É possível então determinar que a utilização de blockchain pode garantir com determinada acurácia a tempestividade de documentos adicionados a ele. Entretanto não foi encontrado nenhum produto que satisfaça todos os requisitos do caso de uso proposto, o que ainda se torna necessária a utilização de Carimbos do Tempo para segurança e datação confiável de assinaturas digitais.

8. References

ARAÚJO, H. P. de; SILVA, R. B. A. R. da. A tecnologia digital blockchain: análise evolutiva e pragmática. Refas-Revista Fatec Zona Sul, v. 3, n. 4, p. 23–39, 2017.

BURNETT, S.; PAINE, S. Criptografia e Segurança: O Guia Oficial RSA. [S.l.]: Elsevier Editora LTDA, 2002.

FERGUSON, N.; SCHNEIER, B. Practical Cryptography. [S.l.]: Wiley Publishing, Inc., 2003.

ALFRED, J. M.; PAUL, C. v. O.; SCOTT, A. V. Handbook of applied cryptography. Massachusetts Institute of Technology, p. 560, 1996.

KING, S. Primecoin: Cryptocurrency with prime number proof-of-work. July 7th, 2013.

MENKE, F. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a icp alemã. Revista de Direito do Consumidor, v. 12, n. 48, 2003.

SILVA, N. da; RAMOS, T. A.; CUSTÓDIO, R. F. Carimbos do tempo autenticados para a preservaçao por longo prazo de assinaturas digitais. 2011.

STALLINGS, W. Criptografia e segurança de redes: principios e práticas. [S.l.]: Pearson Prentice Hall, 2008.

Referências

ALFRED, J. M.; PAUL, C. v. O.; SCOTT, A. V. Handbook of applied cryptography. *Massachusetts Institute of Technology*, p. 560, 1996. Citado na página 25.

ALIAGA, Y. E. M.; HENRIQUES, M. A. A. *Uma comparaçãoo de mecanismos de consenso em blockchains*. 2017. Disponível em: <https://www-.fee.unicamp.br/sites/default/files/departamentos/dca/eadca/eadcax/trabalhos-/artigo_20_Mecanismos_Consenso_Blockchains_Yoshitomi_Maehara_Prof_Marco_Aurelio.pdf>. Acesso em: 21 out. 2017. Citado 4 vezes nas páginas 18, 34, 35 e 36.

ARAÚJO, H. P. de; SILVA, R. B. A. R. da. A tecnologia digital blockchain: análise evolutiva e pragmática. *Refas-Revista Fatec Zona Sul*, v. 3, n. 4, p. 23–39, 2017. Citado 2 vezes nas páginas 28 e 29.

BITCOIN, B. *BlockChain Technology*. 2015. Disponível em: <http://scet.berkeley.edu-/wp-content/uploads/BlockchainPaper.pdf>. Acesso em: 19 out. 2017. Citado na página 31.

Blockchain Info. *Explorador de Blocos Bitcoin*. 2018. Disponível em: <https://blockchain.info-/pt>. Acesso em: 10 jun. 2018. Citado na página 38.

Blockchain Info. *Transações Não Confirmadas Bitcoin*. 2018. Disponível em: <https:/-/blockchain.info/pt/unconfirmed-transactions>. Acesso em: 10 jun. 2018. Citado na página 38.

BLOCKCHAIN privado e público: entenda as principais diferenças. 2018. Disponível em: <http://computerworld.com.br/blockchain-privado-e-publico-entenda-principais-diferencas>. Acesso em: 28 mai. 2018. Citado na página 33.

BlockGeeks. *Proof of Stake vs Proof of Work*. 2017. Disponível em: <https://blockgeeks.com-/wp-content/uploads/2017/03/infographics2017-01.png>. Acesso em: 15 ago. 2017. Citado na página 35.

BURNETT, S.; PAINE, S. *Criptografia e Segurança: O Guia Oficial RSA*. [S.l.]: Elsevier Editora LTDA, 2002. Citado 3 vezes nas páginas 24, 26 e 27.

CoinBase. *Bitcoin Wallet*. 2017. Disponível em: <https://www.coinbase.com/assets/mobile-/mobile-app-dcc08ce0469484f95e8c5f282aa741f3059afb115a953d0e025ea5243f7bbe05-.png>. Acesso em: 20 nov. 2017. Citado na página 30.

Cristian Moecke. *Assinatura Digital*. 2012. Disponível em: <http://www.cristiantm.com.br-/artigos/criptografia/criptografia-para-leigos/parte-iii—assinatura-digital/assinatura_digital-.png?attredirects=0>. Acesso em: 20 nov. 2017. Citado na página 26.

Cristian Moecke. *Criptografia Assimétrica*. 2017. Disponível em: <https://cristiantm.files-.wordpress.com/2008/10/cifragem-ass.png>. Acesso em: 19 nov. 2017. Citado na página 24.

CUSTO Elétrico de Mineração. 2017. Disponível em: <https://g1.globo.com/economia-/tecnologia/noticia/mineracao-de-bitcoin-e-verdade-que-producao-da-moeda-gasta-mais-energia-que-paises-inteiros.ghtml>. Acesso em: 11 jun. 2018. Citado na página 39.

DASH. *Hardware Miner*. 2017. Disponível em: <https://www.dash.org/pt/mining/>. Acesso em: 21 out. 2017. Citado na página 34.

Elaborado pelo Autor. *carregandoDocker*. 2018. Acesso em: 2018. Citado 3 vezes nas páginas 43, 44 e 45.

FERGUSON, N.; SCHNEIER, B. *Practical Cryptography*. [S.l.]: Wiley Publishing, Inc., 2003. Citado 2 vezes nas páginas 23 e 25.

GANDINI, J. A. D.; SALOMÃO, D. P. d. S.; JACOB, C. A segurança dos documentos digitais. *Disponıvel em< http://www. jus. com. br>. Acesso em: 17 out. 2017*, v. 11, 2001. Citado na página 17.

Global Sign. *What is a Timestamping*. 2017. Disponível em: <https://www.globalsign.com-/files/4714/8637/9180/timestamping_image.png>. Acesso em: 20 nov. 2017. Citado na página 28.

GUIA Iniciação Hyperledger. 2018. Disponível em: <https://www.ibm.com/developerworks-/br/cloud/library/cl-ibm-blockchain-101-quick-start-guide-for-developers-bluemix-trs/index-.html>. Acesso em: 28 mai. 2018. Citado na página 42.

HYPERLEDGER Fabric. 2018. Disponível em: <https://www.hyperledger.org/projects/fabric>. Acesso em: 24 mai. 2018. Citado na página 40.

HYPERLEDGER Fabric - InfoChain. 2018. Disponível em: <https://infochain.com.br-/blockchain-para-desenvolvedores-conceitos-de-hyperledger/>. Acesso em: 11 jun. 2018. Citado na página 40.

IBM Developer Workers. *docker-compose.yml*. 2016. Disponível em: <https://developer.ibm-.com/opentech/2016/07/21/running-hyperledger-fabric-natively-on-windows/>. Acesso em: 20 mai. 2018. Citado na página 43.

ISO/IEC 17799. *Código de Prática para a Gestão da Segurança da Informação*. 2005. Disponível em: <http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09-/215545813-ABNT-NBR-177991.pdf>. Acesso em: 17 out. 2017. Citado na página 21.

KING, S. Primecoin: Cryptocurrency with prime number proof-of-work. *July 7th*, 2013. Citado na página 34.

KING, S.; NADAL, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, v. 19, 2012. Citado 2 vezes nas páginas 34 e 36.

L3C. *GED*. 2017. Disponível em: <http://www.l3c.com.br/img/ged.png>. Acesso em: 20 out. 2017. Citado na página 22.

LUCENA, A. U. de; HENRIQUES, M. A. A. *Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum*. 2016. Disponível em: <https://pdfs.semanticscholar.org/eb41-/c8ea5c5d191c909d3e107ec84d5e441794c0.pdf>. Acesso em: 20 out. 2017. Citado 4 vezes nas páginas 18, 29, 31 e 33.

MARCACINI, A. T. R. O documento eletrônico como meio de prova. *Diponível em:< http://augustomarcacini. cjb. net/textos/docelet2. html>. Acesso em*, v. 15, 2000. Citado na página 22.

MENKE, F. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a icp alemã. *Revista de Direito do Consumidor*, v. 12, n. 48, 2003. Citado na página 17.

NAKAMOTO, S. *Bitcoin: A peer-to-peer electronic cash system*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 20 out. 2017. Citado na página 29.

NAKAMURA, E. T.; GEUS, P. L. d. *Segurança em Redes: Em ambientes cooperativos*. [S.l.]: Novatec Editora Ltda., 2007. Citado 5 vezes nas páginas 17, 23, 24, 26 e 27.

PFLEEGER, C. P. *Security in Computing*. [S.l.]: Prentice Hall PTR, 1997. Citado 2 vezes nas páginas 18 e 25.

RODRIGUES, E. I. *Estudo sobre Bitcoin: escalabilidade da blockchain*. 2016. Disponível em: <http://elias19r.com/files/cv/tcc1-monografia_7987251.pdf>. Acesso em: 20 out. 2017. Citado 5 vezes nas páginas 18, 29, 30, 31 e 32.

SILVA, N. da; RAMOS, T. A.; CUSTÓDIO, R. F. Carimbos do tempo autenticados para a preservaç ao por longo prazo de assinaturas digitais. 2011. Citado 2 vezes nas páginas 18 e 28.

Stack Overflow. *Fundamental different between Hash and Encryption*. 2012. Disponível em: <https://i.stack.imgur.com/WEKK4.png>. Acesso em: 20 nov. 2017. Citado na página 25.

STALLINGS, W. *Criptografia e segurança de redes: principios e práticas*. [S.l.]: Pearson Prentice Hall, 2008. Citado 2 vezes nas páginas 17 e 23.

Wikipedia. *Public key certificate*. 2017. Disponível em: <https://upload.wikimedia-.org/wikipedia/commons/thumb/6/65/PublicKeyCertificateDiagram_It.svg/550px-PublicKeyCertificateDiagram_It.svg.png>. Acesso em: 20 nov. 2017. Citado na página 27.

World Economic Forum. *Beyond Bitcoin*. 2016. Disponível em: <https://assets.weforum.org-/editor/4sGoxDfpGJXm-t51JPPNqz2G5PXYFPCD1ZN13yWGoVU.png>. Acesso em: 20 nov. 2017. Citado na página 32.