BITTRUST - Solução de Prova de Autenticidade Utilizando o Blockchain

Alisson Solitto da Silva
Programa de Pós-graduação em Ciência da Computação, Universidade Estadual Paulista "Júlio de Mesquita Filho"
Presidente Prudente, São Paulo, Brazil
alisson.solitto@unesp.br

***Abstract* —This paper highlights alternative solutions for blockchain technology that address the principles of Information Security and apply these concepts to the registration and validation of digital documents on the Bitcoin network. This way documents can be validated and publicly visible to any user with Internet access. The goal is to develop a solution that aims to abstract all the complexity of cryptographic algorithms and techniques and use them in conjunction with blockchain technology, enhancing the registration and authenticity of a digital document in a decentralized public environment. With the developed solution it is possible to register digital documents in the Bitcoin blockchain, ensuring the authenticity validation of digital files in a chronological and cryptographic manner. In this way the tool can guarantee the authenticity of files without the need for a certifying entity to guarantee its legitimacy.**

***Keywords* —Information Security, Blockchain, Bitcoin, Decentralization, BitTrust, Hash, Encryption**

***Resumo* —O presente artigo destaca soluções alternativas para a tecnologia blockchain visando os princípios da Segurança da Informação e aplicando esses conceitos para o registro e validação de documentos digitais na rede do Bitcoin. Desta forma os documentos podem ter sua integridade validada e visível de maneira pública para qualquer usuário com acesso à Internet. O objetivo é o desenvolvimento de uma solução que visa abstrair toda a complexidade dos algoritmos e técnicas criptográficas e utilizá-las em conjunto com a tecnologia blockchain, potencializando o registro e a autenticidade de um documento digital em um ambiente público e descentralizado. Com a solução desenvolvida é possível o registro de documentos digitais no blockchain do Bitcoin, garantindo a validação da autenticidade dos arquivos digitais de maneira cronológica e criptográfica. Desta forma a ferramenta consegue garantir a autenticidade de arquivos sem a necessidade de uma entidade certificadora para garantir a legitimidade do mesmo.**

***Palavras-chave* —Segurança da Informação, Blockchain, Bitcoin, Descentralização, BitTrust, Hash, Criptografia**

I. Introdução

Com o constante avanço da tecnologia a quantidade de arquivos digitais gerados pelos ambientes corporativos está produzindo uma infinidade de informações, sendo grande parte dessas informações documentos sigilosos e importantes, tais como, contratos, patentes, certificados, artigos acadêmicos e outros diversos documentos digitais que necessitam de procedimentos de Segurança da Informação para garantir sua integridade, confidencialidade e disponibilidade.

Com a ascensão de arquiteturas de software distribuídas e descentralizadas, o blockchain surgiu como uma solução inovadora e segura para a transação de ativos financeiros na Internet, porém o blockchain pode proporcionar inúmeras soluções disruptivas além de transações financeiras que podem agregar segurança e confiabilidade em diferentes outros dados que a rede pode transacionar.

O objetivo do presente trabalho é propor uma solução que garanta a integridade de documentos digitais por meio do protocolo do Bitcoin, abstraindo todo o conhecimento necessário para a integração e comunicação à rede Bitcoin, proporcionando a garantia de integridade e prova temporal da informação registrada na rede.

A solução utiliza conceitos de Segurança da Informação, algoritmos de criptografia, técnicas de armazenamento e recuperação da informação na rede garantindo a disponibilidade e a verificação da informação no momento em que foi registrada na rede, além de testar a integridade do arquivo original enviado pela aplicação.

II. Trabalhos Correlatos

Após a disseminação da tecnologia blockchain no meio acadêmico surgiram alguns trabalhos e aplicações com o objetivo de utilizar o blockchain para além da transação de ativos financeiros. Entre as pesquisas destaca-se o projeto de certificados digitais [1], um projeto incubado pelo *Media Lab Learning Initiative and Learning Machine* no MIT (Massachusetts Institute of Technology) que tem como proposta criar uma solução para compartilhar e verificar certificados educacionais assinados criptograficamente utilizando o protocolo do Bitcoin.

Uma outra proposta desenvolvida no mercado brasileiro é a [2], cujo objetivo é o registro e autenticidade de documentos e a integração com cartórios físicos. A solução proposta utiliza o protocolo do Bitcoin, Ethereum, Ethereum Classic e Decred.

III. Segurança da Informação

A informação pode ser definida por um conjunto de dados e metadados organizados de maneira que apresentem algum significado ou sentido dentro de um determinado contexto. Tradicionalmente a informação está relacionada com documentos impressos e bibliotecas, quando de fato pode estar num diálogo, em uma comunicação informal, numa inovação para indústria, em patentes, numa fotografia ou objeto, em registros magnéticos de uma base de dados ou em documentos digitais [3].

A informação é algo muito importante para as organizações, além de ser utilizada para fornecer determinadas necessidades e a tomada de decisões estratégicas dentro da organização e em diferentes contextos. Em uma organização a informação pode assumir diversas formas entre elas a principal é a forma digital. Com a grande relevância da informação, a necessidade de protegê-la passou a ser fundamental, atualmente com o grande volume de contratos e documentos digitais de várias espécies passou a ser crucial para as organizações uma abordagem da segurança da informação, pois sua falta pode acarretar em altíssimos prejuízos para uma empresa.

De acordo com [4] a área da Segurança da Informação é uma área dedicada à proteção de ativos contra acessos não autorizados, alterações indevidas da informação e sua falta de disponibilidade. Complementando essa definição, de acordo com [5], a Segurança da Informação convém que a informação tenha a preservação da confidencialidade, integridade e disponibilidade, além de outras propriedades que podem constar o não repúdio e confiabilidade da informação.

Consequentemente de acordo com os conceitos expostos acima podemos observar que existem três elementos essenciais para a área da Segurança da Informação visando à proteção de seus ativos das ameaças de confidencialidade, integridade e disponibilidade, a fim de minimizar os riscos da segurança da informação.

- Confidencialidade: é a garantia de acesso restrito à informação, ou seja, apenas os usuários legítimos possuem permissão de acesso à informação [6].
- Integridade: é a preservação da informação na mesma condição em que foi disponibilizada pelo seu proprietário, ou seja, é a garantia de proteção contra adulteração da informação [4].
- Disponibilidade: salvaguarda de que a informação esteja disponível para os legítimos usuários [6].

Uma tecnologia importante para garantir elementos de segurança da informação criada inicialmente por [7], o blockchain utiliza a descentralização para armazenamento e disponibilidade de informações com maior segurança. Inicialmente a proposta do blockchain era realizar transações na Internet de maneira segura e anônima em um sistema descentralizado sem uma autoridade responsável pela validação dos dados, hoje o uso do blockchain pode ir além das transações de valores na rede.

O blockchain pode proporcionar as organizações aplicações altamente seguras, além da sua arquitetura disponibilizar regras confiáveis como prova de tempo, propriedade de direitos, integridade, disponibilidade, confiabilidade e transparência.

IV. Histórico do Bitcoin

No final da década de 90 surgiram as principais contribuições técnicas e científicas para a tecnologia blockchain e que embasaram o artigo intitulado "Bitcoin: a Peer-to-Peer Electronic Cash" [7], publicado por um autor sob o pseudônimo de *Satoshi Nakamoto*. Embora tenha sido um artigo inovador e provido como base de todas as outras criptomoedas, este artigo nunca foi submetido para um periódico tradicional e revisado por acadêmicos da área [8].

Uma das propostas que embasou a versão do Bitcoin foi apresentada em 1998 por Wei Dai, intitulada de "B-Money" [9], este trabalho descreve a criação de um dinheiro digital descentralizado, não sendo necessário uma autoridade centralizadora para a emissão, liquidação e validação de transações desta moeda, porém o dinheiro seria emitido desde que seja resolvido um problema computacional altamente complexo envolvendo um alto esforço computacional com o objetivo de impedir fraudes nas transações. Na proposta a transferência do dinheiro eletrônico é dada por uma troca de mensagens assinadas entre os participantes e um algoritmo de consenso descentralizado que valida o estado das transações.

A contribuição mais próxima do Bitcoin antes de Satoshi Nakamoto foi apresentada por Nick Szabo em 2005 no artigo intitulado "Bit Gold" [10]. O Bit Gold busca a criação de um dinheiro digital com o objetivo de não depender da confiança de terceiros para a emissão, armazenamento e troca de valores entres as pessoas. A proposta é criar uma rede distribuída utilizando como segurança um algoritmo de prova de trabalho e um carimbo de data.

Finalmente em 2008, Satoshi Nakamoto, cuja sua real identidade ainda é um mistério, publica o artigo intitulado "Bitcoin: a Peer-to-Peer Electronic Cash". A proposta de Satoshi Nakamoto resolve todos os outros problemas de projetos anteriores em relação a descentralização, prova de trabalho, carimbo de tempo e gasto duplo. O principal objetivo do artigo é permitir o envio de pagamentos online sem a necessidade de um intermediário para gerar confiança e segurança nas transações.

V. Blockchain

O blockchain é uma cadeia de blocos descentralizada, composta por milhares de computadores, processando centenas de transações por minuto e contendo o histórico de informações de cada transação que ocorrem na rede ponto a ponto (P2P). A estrutura do blockchain pode ser comparada a um banco de dados distribuído em uma rede de vários participantes, onde cada participante possui uma cópia exata da base de dados, não havendo desta forma um servidor central responsável pela confiança e segurança da informação, portanto, dependendo apenas de um consenso descentralizado [11].

Segundo [12] o blockchain é uma tecnologia para se criar um livro razão distribuído (do inglês, ledger) robusto, seguro e transparente. Essa nova tecnologia é disruptiva, além de um protocolo de software baseado em criptografia e fortes algoritmos matemáticos, o blockchain é uma tecnologia para bancos de dados públicos e pode ser melhor entendida como uma tecnologia institucional ou social para coordenar pessoas.

A rede blockchain usa algoritmos de prova de trabalho e mecanismos de consenso para validar a confiança das informações transferidas na rede, não sendo necessário uma instituição ou autoridade centralizadora para garantir a integridade e autenticidade da informação. A solicitação de uma nova informação na rede é feita por meio de uma transação,

a adição dessa informação é imutabilizada por meio de um novo bloco na rede de maneira sequencial, o bloco contém um conjunto de transações validadas pelos participantes, além do identificador do bloco anterior, formando uma autêntica corrente de blocos, o *blockchain*.

O blockchain tem como seu primeiro caso de aplicação a moeda digital Bitcoin (2008), que nada mais é do que o nome do ativo transacionado na rede blockchain. O protocolo do Bitcoin possui algoritmos responsáveis pela função de mineração de ativos através da rede, em média a cada 10 minutos um nó é capaz de validar as transações dos últimos 10 minutos, e criar um bloco contendo todas as transações validadas [11]. Os ativos de Bitcoin são limitados a um máximo de 21 milhões, para cada protocolo diferente do Bitcoin o blockchain e sua aplicação são regidos por algoritmos e técnicas criptográficas diferentes.

O grande benefício do blockhain é que não há um ponto central de falhas e vulnerabilidades. Desta forma para um ataque bem-sucedido com o objetivo de modificar os dados da rede blockchain, o atacante deve refazer todo o poder computacional exigido pelo algoritmo para criar um novo bloco e possuir o maior número de nós atacantes controlando a rede para desta forma gerar um consenso corruptivo.

As principais características de destaque de uma estrutura de dados blockhain são de acordo com [13]:

- Redundância de dados: cada nó tem uma cópia completa do *ledger* do blockchain;
- Verificação dos dados e requisitos da transação antes da validação;
- Inclusão de transações em blocos ordenados sequencialmente, cuja validação para a inclusão na cadeia de blocos é regida por um algoritmo de consenso;
- Transações baseadas em criptografia de chave pública;
- Escrita de transações por meio de algoritmos computacionais.

O blockchain pode ser classificado em dois tipos: público e privado. No blockchain público qualquer usuário pode fazer parte da rede e processar as transações, todos os blocos e dados de transações são públicos e podem ser acessados por qualquer pessoa sem necessitar de uma permissão para isso, no blockchain público há o real proveito da descentralização. No blockchain privado a rede é controlada por uma organização que detêm o controle das políticas de segurança da rede e a autorização de novos participantes, neste caso temos uma falsa impressão de descentralização, pois, a arquitetura dos nós na rede é descentralizado, mas há uma organização controladora [14].

Essa tecnologia disruptiva pode ser utilizada não apenas como ativo monetário, mas também para outras aplicação, tais como: autenticidade e registro de arquivos digitais, processo de votação, cadeia de logística, rastreio de recursos, entre outros. No Brasil uma solução governamental é desenvolvida pela equipe do BNDES (Banco Nacional de Desenvolvimento Econômico e Social), a proposta é a criação de um *token* no blockchain para rastrear os recursos do BNDES, todas as transações serão públicas, visando a transparência e o combate à corrupção dos financiamentos feitos pelo banco [15].

VI. Chaves e endereços

A posse de ativos na rede do Bitcoin é determinada por chaves criptográficas e assinaturas digitais. Assim como nas transações bancarias as transações de valores feitas na rede Bitcoin necessitam de um remetente e de um destinatário, diferente de contas em banco são utilizadas *wallets*, conhecidas como carteiras virtuais. As chaves criptográficas de um usuário são completamente independentes do protocolo Bitcoin e podem ser geradas e gerenciadas por qualquer software que implemente um algoritmo criptográfica para a criação de um par de chaves atendendo as regras do protocolo.

As chaves são parte fundamental da confiança descentralizada e controle do usuário, além da atestação de posse e segurança por prova criptográfica toda transação de um ativo efetuado na rede requer uma assinatura válida para ser incluída no blockchain, apenas o detentor das chaves criptográficas pode gerar assinaturas válidas para uma transação. O protocolo utiliza o conceito de criptografia de chave pública, na qual são necessários duas chaves para o funcionamento do processo, sendo elas:

- Chave privada: neste cenário podemos comparar a chave privada como a senha da sua conta no banco, essa chave é responsável pelo acesso aos fundos de Bitcoin na carteira e por assinar as transações na rede. A chave privada não pode ser perdida, caso contrário nunca mais será possível acessar sua carteira.
- Chave pública: a chave pública é derivada da chave privada e pode ser comparada ao número da sua conta no banco, ela pode ser divulgada a qualquer pessoa para o recebimento de pagamentos, diferente do número da conta no banco a chave pública pode ser gerada diversas vezes a partir da chave privada.

A relação entre a chave privada e pública é 1:N, a partir de "1" chave privada podemos gerar "n" chaves públicas diferentes, desta forma para cada recebimento podemos informar um endereço diferente aumentando ainda mais o anonimato da transação. Uma observação importante é que a partir da chave pública é matematicamente impossível descobrir a chave privada e a relação matemática entre a chave pública e a privada permite que a chave privada seja usada para gerar assinaturas nas transações da rede. Essa assinatura pode ser validada em relação à chave pública, sem a necessidade de se revelar a chave privada.

A figura 1 representa a relação entre a chave privada, chave pública e o endereço na rede Bitcoin. Podemos observar que a partir da chave privada é possível gerar a chave pública e o endereço na rede, mas o contrário é matematicamente impossível.

Outra parte importante em relação as chaves criptográficas do protocolo Bitcoin são os endereços, o endereço é a representação da impressão digital da chave pública, um endereço é gerado a partir de uma chave pública correspon-

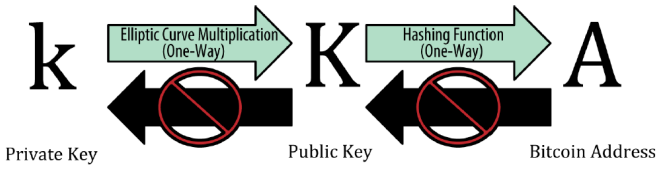

Fig. 1. Chave privada, chave pública e endereço Bitcoin ([16]).

dente. Um dos principais objetivos do endereço é abstrair a representação da chave pública dos usuários na rede.

VII. Transação

A transação é uma das funcionalidades mais importantes no sistema do blockchain, a transação é uma transferência de dados entre usuários da rede que são propagadas para os nós do blockchain, validadas e posteriormente inseridas em um novo bloco da cadeia. Uma vez que as transações são incluídas em um bloco e este tem confirmações suficientes na cadeia, a transação pode ser considerada irreversível.

Todas as transações são transparentes no blockchain, pois não são criptografadas, sendo possível visualizar todos os dados das transações incluídas em um determinado bloco da rede. Para visualizar dados de transações são utilizados softwares de visualização de cadeia de blocos (Block Explorer) sendo possível visualizar os detalhes técnicos das transações e dados de alto nível legíveis por humanos [16].

Fundamentalmente, a transação na rede blockchain informa que o proprietário de algum ativo autorizou a transferência desse ativo para outro usuário da rede, agora este novo proprietário do ativo pode criar uma outra transação, e assim sucessivamente, gerando uma cadeia de propriedade. Essa cadeia de propriedade pode ser observada na figura 2.

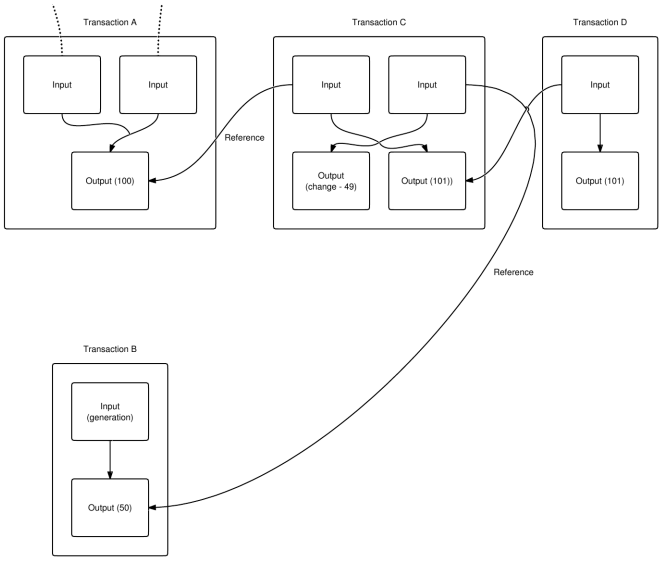

Fig. 2. A envia 100 BTC para C e C gera 50 BTC. C envia 101 BTC para D, e ele precisa enviar alguma alteração para si mesmo. D envia o 101 BTC para outro usuário, mas ainda não a resgatou. Somente a saída de D e a mudança de C podem ser gastas no estado atual ([16]).

Existem quatro formas de estruturação de uma transação no protocolo do Bitcoin:

- (*1:1*): a maneira mais comum é uma transação simples entre dois endereços, que frequentemente inclui uma saída para o endereço de origem com o resíduo do valor original, essa típica forma de transação inclui uma entrada e uma saída.
- (*1:N*): distribuir uma entrada para várias saídas, ou seja, uma saída de um único endereço é enviada para vários endereços diferentes. Esse tipo de transação pode ser utilizado por entidades comerciais para distribuir fundos, como por exemplo no processamento de uma folha de pagamento para vários funcionários [11].
- (*N:1*): agregar várias entradas em uma única saída para o mesmo endereço, ou coletar várias entradas a fim de resultar em um valor total necessário para transferir a outro endereço. Transações como essas são geradas pelas aplicações para limpar muitos valores menores que foram recebidos e unificar em uma única saída válida [11].
- (*N:N*): distribuir várias entradas de um endereço para vários endereços, esse tipo de transação pode ser utilizada para economizar uma transação de agregação (*N:1*) e transmitir para vários endereços.

A. Entradas e Saídas

Uma transação na rede Bitcoin é uma estrutura de dados composta por uma ou mais entrada de dados *input* e uma ou mais saída de dados *output*.

O *input* é uma entrada que faz referência a uma saída (*output*) de outra transação realizada anteriormente. Todos os valores de entrada da nova transação, ou seja, o valor total das saídas anteriores referenciadas pelas entradas da nova transação são somados e o total deduzindo qualquer taxa de transação cobrada pela rede é utilizada pelas saídas da nova transação [16].

O *output* é o bloco de construção fundamental de uma transação na rede bitcoin, apenas as saídas válidas de uma transação registrada no blockchain e não gasto (UTXO) podem ser utilizadas como entrada em novas transações, o *output* de uma transação pode referenciar um endereço de destinatário, ou o próprio endereço do criador da transação. Quando o *output* referência o próprio endereço do criador da transação este *output* é qualificado como uma mudança (*change*). O saldo de um endereço de Bitcon é dado pelos nós completos da rede, estes rastreiam todas as saídas disponíveis não gastas do endereço espalhados pela rede tornando possível calcular o saldo de todos os UTXOs não gastos pertencentes ao endereço [11].

As entradas e saídas são atributos importantes da estrutura de dados de uma transação, além de outros atributos como o script de assinatura, timestamp e hash da transação. O *output* de uma transação também pode ser utilizado para o armazenamento de dados e podem ter usos potenciais muito além dos relacionados ao ativo Bitcoin, esse recurso pode ser alcançado através da utilização da linguagem de script do Bitcoin com a finalidade de criar *outputs* de transação

não gastos contendo outros dados, por exemplo, registro de uma uma impressão digital de um arquivo de uma maneira que qualquer algoritmo consiga estabelecer uma prova de existência daquele arquivo em uma data específica através de uma referência àquela transação.

Isso é possível através do operador *OP_RETURN* disponível a partir da versão 0.9 do cliente Bitcoin, este operador permite que seja adicionado bytes no *output* válidos não gastos. Esse espaço de dados é limitado a 83 bytes (A versão 0.12.0 padronizou essa saída para retransmitir e extrair as saídas de dados nulos com até 83 bytes [17]), desta forma é possível criar aplicações que utilizem um algoritmo SHA256 (32 bytes) para criar uma impressão digital de um arquivo e incluir em uma transação no blockchain, assim essa aplicação pode se favorecer de todos os benefícios do blockchain utilizando sua estrutura para além de aplicações financeiras [11].

B. *Propagação de Transações na Rede Bitcoin*

Após a criação de um script de transação, essa transação deve ser enviada para a rede blockchain. A transação pode ser enviada para qualquer nó conectado a rede, após o nó receber o script de transação, este é validado pelo nó e somente depois de validado será propagado para os outros nós com os quais ele está conectado. As transações são propagadas por cada nó a todos os pares aos quais ele está conectado e assim sucessivamente, este processo é denominado *flooding* (inundação), deste modo uma transação válida será propagada de forma exponencial pela rede até que todos os nós da rede a recebam.

O protocolo do Bitcoin é projetado para propagar transações e blocos para todos os nós participantes da rede de uma maneira eficiente, segura e flexível, a fim de evitar ataques maliciosos na rede Bitcoin cada nó valida independentemente cada transação recebida antes de propagá-la para os próximos nós, consequentemente uma transação mal intencionada ou com alguma falha de script não será recebida por outro nó da rede [11]. Caso a transação seja inválida ou maliciosa o nó rejeitará a transação e propagará uma mensagem de rejeição para o nó que originou a transação na rede.

O fluxo completo de ações está sendo representado na figura 3, para a realização de uma transação no protocolo do Bitcoin são necessárias basicamente 5 etapas [18]:

1) Um usuário da rede que deseja transferir um Bitcoin utilizando sua chave pública ou endereço;
2) O usuário informa a quantidade do ativo a ser transferido, sua chave pública, o endereço de destino e a assinatura da transação;
3) A transação é enviada a rede blockchain por meio do *flooding*;
4) A rede trabalha para incluir a transação valida em um bloco;
5) Após as validações de consenso o bloco é transmitido pela rede e incorporado na cadeia global.

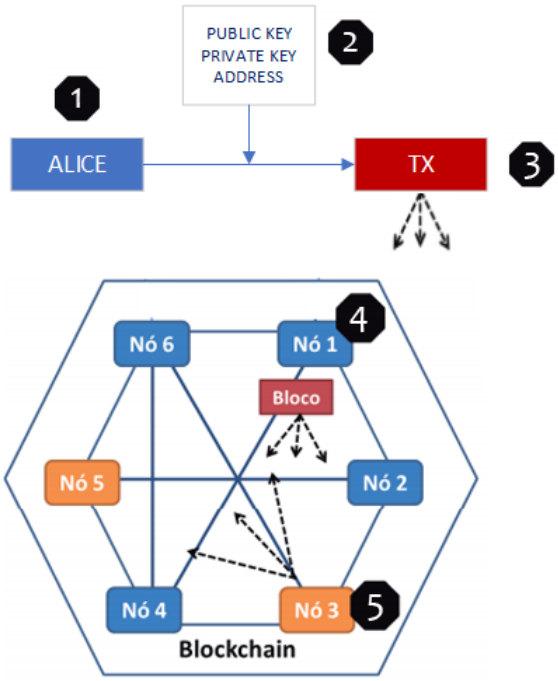

Fig. 3. Etapas do processo da propagação de uma transação na rede blockchain, iniciando pela criação da transação até a inclusão em um bloco na cadeia global (Adaptado de [19])

VIII. Bloco

A principal estrutura de dados do blockchain é a lista encadeada de blocos, cada bloco é referenciado ao bloco anterior, essa estrutura pode ser visualizada como um empilhamento vertical, essa visualização de blocos empilhados como uma estrutura típica de pilha resulta em termos conhecidos como "altura" para se referir à distância em relação ao primeiro bloco, e "topo" para se referir ao bloco mais recentemente do blockchain. O software Bitcoin armazena os metadados do blockchain usando a tecnologia de banco de dados LevelDB do Google.

O bloco é uma estrutura fundamento para o sistema, cada bloco agrega um conjunto de transações válidas recebidas e verificadas pela rede, o bloco é identificado por um hash em seu cabeçalho, o hash é gerado a partir de um algoritmo criptográfico (SHA256) e cada bloco possui sua identificação e a identificação do bloco anterior, ou o bloco pai. Dessa forma, cria-se uma corrente de blocos que pode ser percorrida de forma retrógrada até o bloco inicial, conhecido como bloco gênese [11].

A estrutura de um bloco contém dados que agregam as transações para a inclusão no blockchain. O bloco é composto por um conjunto de dados e metadados, os principais conjuntos dessa estrutura são o cabeçalho que é composto por vários metadados, uma lista de transações e a altura do bloco na cadeia. A estrutura do bloco pode ser visualizada na figura 4.

O cabeçalho do bloco contém metadados importantes para a rede, a sua estrutura é formada por:

- Hash do Bloco Anterior: referência ao hash do bloco anterior (bloco pai) no blockchain. Esse hash também é utilizado para calcular o hash do bloco atual;
- Data e Hora (timestamp): momento aproximado em que este bloco foi criado (em segundos, usando Unix Epoch);
- Dificuldade Alvo: dificuldade do algoritmo de prova de trabalho para o cálculo do hash válido deste bloco;
- Nonce: contador usado para o algoritmo de prova de trabalho da rede blockchain;
- Raiz de Merkle: essa estrutura armazena um hash da raiz da árvore de merkle das transações do bloco, é uma maneira eficiente de resumir as transações contidas no bloco. Segundo [7] essa estrutura fundamental para salvar espaço em disco, dado que as transações gastas anteriormente podem ser descartadas, desta forma os blocos antigos podem então ser compactados ao remover as versões mais antigas da árvore.

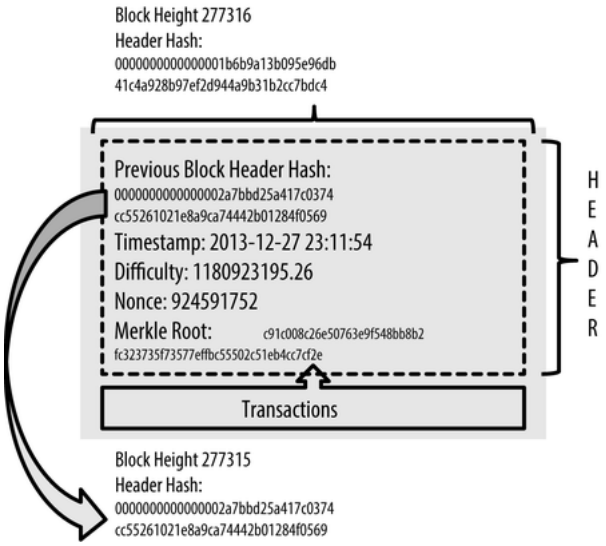

Fig. 4. Representação da estrutura de um bloco na rede Bitcoin ([11]).

IX. Mineração

O grande modelo que sustenta a rede descentralizada e pública do blockchain do Bitcoin é o sistema de incentivo criado por [7], esse sistema é conhecido como mineração. O processo de mineração tem duas funções essenciais, proteger a rede Bitcoin contra possíveis transações fraudulentas ou gastos duplos e gerar novas unidades do ativo Bitcoin como recompensa. Os minerados, como são chamados os nós que fazem o processamento de um algoritmo matemático altamente custoso para a criação de um novo bloco são recompensados com uma quantia do ativo, além do processo de inclusão de um novo bloco na cadeia global estes também são responsáveis por validar as transações que são propagadas na rede [11].

Os mineradores da rede Bitcoin recebem dois tipos de recompensa pelo ardo processamento necessário para a execução dos algoritmos: novas unidades do ativo criadas a partir da geração de um novo bloco e as taxas de todas as transações incluídas no bloco. Para [7] o incentivo da mineração encoraja os nós da rede a permanecerem honestos, se um nó atacante é capaz de possuir mais poder de processamento do que todos os nós honestos da rede, este nó provavelmente precisará escolher entre fraudar as transações da rede, ou usar este amplo poder de processamento para ganhar novas moedas. Para este nó é muito mais lucrativo manter a rede funcionamento de maneira honesta e usar todo este poder de processamento para receber mais unidades do ativo da rede.

Para o nó minerador receber as recompensas da rede, este precisa competir com os outros mineradores da rede para resolver um complexo problema matemático baseado em um algoritmo de hash criptográfico, a solução para esse problema é denominada *proof-of-work* (prova de trabalho). Este processo fornece uma prova de que o nó minerador gastou uma significativa quantidade de esforço computacional para gerar um novo bloco válido na rede.

Fundamentalmente, a mineração é o processo responsável por criar o hash do cabeçalho do bloco de maneira repetida, até que o hash resultante corresponda a um alvo específico. Desta maneira a única forma de produzir um hash que atenda a um alvo específico é através de inúmeras tentativas de processamento até que o hash proposto seja encontrado.

Existem duas maneiras de minerar na rede blockchain do Bitcoin [20]:

1) Mineração solo: nesta modalidade o nó minerador faz todo o processamento de um novo bloco de maneira individual, atualmente é uma maneira muito custosa de processar novos blocos na rede, pois é necessário um poder de processamento computacional muito alto para resolver o problema da proof-of-work.
2) Pool de mineração: a maneira mais comum atualmente de participar como um nó minerador na rede, os nós mineradores se agrupam para compartilhar os recursos computacionais e fazer o processamento de um novo bloco. Desta forma cada nó recebe uma recompensa de acordo com a quantidade de processamento que contribuiu para processar o algoritmo computacional de mineração.

A. Prova de Trabalho

Todo o poder computacional necessário para gerar um novo bloco na rede faz parte do protocolo do Bitcoin, este processo é denominado proof-of-work (prova de trabalho). O algoritmo de prova de trabalho consiste em a partir de um input de dados de comprimento arbitrário e produzir uma saída determinística de comprimento fixo de acordo com o algoritmo de hash utilizado no processo, ou seja, para a rede blockchain o resultado desse processamento é um impressão digital do bloco [11].

O processo de prova de trabalho do Bitcoin utiliza a biblioteca criptográfica Hashcash [21], comumente utilizada como uma técnica de medida para ataques de negação de serviço em vários sistemas. O protocolo Bitcoin utiliza essa biblioteca usando a função criptográfica SHA256, sempre uma determinada entrada resultará em uma saída sempre de 256 bits de comprimento, independente do tamanho do

input. Qualquer mudança na entrada, a adição de uma única letra, uma pontuação ou qualquer outro caractere no input o algoritmo irá produzir uma saída (hash) diferente.

Para que um novo um bloco seja aceito na rede Bitcoin pelos nós participantes da rede, os nós mineradores devem encontrar uma prova de trabalho que atenda todos os dados e metadados do bloco. A prova de trabalho requer encontrar um valor que codificado por um algoritmo como SHA256 comece com um número de zero bits. O trabalho médio necessário é exponencial em número de "zero bits" definidos pela dificuldade da rede e pode ser validado pelos participantes executando uma única codificação [7].

Com o objetivo de compreendermos a complexidade do algortimo de prova de trabalho do protocolo Bitcoin vamos utilizar como exemplo a entrada de dados "I am Satoshi Nakamoto", o objetivo é encontrar uma frase que produza um hash hexadecimal que comece com um zero. Para atingirmos nosso objetivo precisamos processar muitos hashes fazendo a interação com um nonce (número arbitrário incremental), o mesmo conceito utilizado no bloco do Bitcoin, dessa forma é possível alterar a saída do hash modificando a entrada de dados sempre a cada iteração com um novo nonce, até encontrarmos um resultado que satisfaça nosso objetivo. O algoritmo abaixo escrito na linguagem C Sharp (C#), exemplifica o processo de iterações para encontrarmos o hash alvo.

```
string text = "I am Satoshi Nakamoto";

for(int nonce = 0; nonce < 100000; nonce++)
{
  string input = text + nonce;
  string hash = SHA256Hash(input);
  Console.WriteLine($"{input} =>
      {hash.ToUpper()}");
}
```

O algoritmo inicia a variável *text* com o valor que será processado para gerar um hash válido, assim como no algoritmo utilizado no protocolo Bitcoin nesse cenário é utilizada a variável de iteração denominada de *nonce*. O *nonce* é usado para variar a saída da função criptográfica SHA256 com base no valor inicial de *text*. A iteração com o *nonce* no algoritmo é necessário para gerar um hash que atenda as condições, neste caso a condição é que o hash gerado inicie com um zero.

Este desafio é satisfeito quando o *nonce* no valor 13 é iterado, desta forma a entrada "I am Satoshi Nakamoto13" produz o hash "0EBC56D59A34F5082AAEF3D66B37A661696C2B618E..." que preenche o critério de um zero no começo do hash.

No protocolo Bitcoin o nó minerador calcula o hash do novo bloco e verifica se o resultado é menor do que o alvo atual definido na rede. Caso o hash não atinga alvo o nó incrementará nonce processará o hash do bloco novamente. Na dificuldade atual da rede Bitcoin os nós devem fazer quadrilhões de tentativas até encontrar um nonce que resulte em um hash válido para a rede.

Para entendermos o nível de complexidade para a geração de um novo bloco utilizamos como exemplo o bloco na altura 277.316, este bloco contém a dificuldade alvo expressada em 0x1903a30c. Essa notação expressa a dificuldade alvo em um formato coeficiente/expoente, com os primeiros dois dígitos hexadecimais sendo o expoente e os próximos seis dígitos hexadecimais sendo o coeficiente [11].

A fórmula para calcular a dificuldade alvo 0x1903a30c para esse bloco é expressa na figura 5.

```
alvo = coeficiente * 2^(8 * (expoente – 3))
alvo = 0x03a30c * 2^(0x08 * (0x19 - 0x03))^
=> alvo = 0x03a30c * 2^(0x08 * 0x16)^
=> alvo = 0x03a30c * 2^0xB0^
=> alvo = 0x0000000000000003A30C000000000000000000000000000000000000000000
```

Fig. 5. Fórmula para calcular a dificuldade alvo do bloco (Adaptado de [11]).

Em binário o valor alvo é definido em mais de 60 bits zeros iniciais, ou seja, um único minerador precisaria processar 1 trilhão de hashes por segundo (1 TH/seg) para encontrar uma solução em média uma vez a cada 8.496 blocos ou uma vez a cada 59 dias.

A dificuldade alvo do hash é ajustada de modo a limitar a geração de novos blocos na rede para um a cada 10 minutos. De acordo com [7] para compensar o aumento da velocidade do hardware e a variedade de interesse em rodar os nós a medida que o tempo passa, a dificuldade da prova de trabalho é determinada por uma meta variável em número de blocos por hora. Se os blocos estão sendo gerados muito rápido, a dificuldade aumenta. Essa equação pode ser resumida em:

$$ND = DA * (TB/MIN)$$

- ND: Nova Dificuldade;
- DA: Dificuldade Antiga;
- TB: Tempo dos últimos 2.016 blocos;
- MIN: 20.160 minutos.

X. Projeto BitTrust

Este trabalho tem como objetivo o registro de documentos em um blockhain público sem a necessidade de utilizar serviços que utilizem um terceiro confiável para checar a autenticidade do arquivo digital, podendo ser eliminado assim o serviço de autenticidade dos cartórios. Este serviço garante a validação da autenticidade de qualquer arquivo digital, validade e cronologia de registro de arquivos digitais no blockhain do Bitcoin. Com o processo de transação e criação de blocos no protocolo do Bitcoin, após efetuar uma transação registrando um arquivo digital na rede e a mesma é incluída em um bloco o arquivo digital torna-se irrevogável e autentico no tempo em que foi incluído no blockchain.

Com a utilização de um blockchain público o registro possuí grande transparência e qualquer usuário a nível global que possua acesso a Web pode testar a autenticidade do arquivo, se o mesmo estiver de posse do arquivo original, além da verificação de autenticidade qualquer usuário tem acesso a

todos os detalhes da transação em que o arquivo digital foi persistido na rede.

Para a utilização do sistema de registro de arquivos digitais é necessário que o usuário tenha a posse de uma chave privada e de seu respectivo endereço na rede Bitcoin, além de ter saldo disponível que é utilizado apenas para pagar a taxa de mineração na rede, já que a transferência não possuirá um saída de valor para outro endereço, apenas a assinatura digital do arquivo registrado.

A aplicação BitTrust foi desenvolvida utilizando a linguagem de terceira geração C Sharp (C#), o software desenvolvido permite a criação e recuperação de chaves privadas através de uma frase-chave fornecida pelo usuário, ou uma frase-chave aleatória, além da consulta do saldo de qualquer endereço da rede e a visualização das informações detalhadas de qualquer transação, e por fim o registro e o teste de arquivos digitais no protocolo do Bitcoin.

A. Geração de chaves e endereços

As duas primeiras partes da aplicação possuem as funcionalidades de criar e recuperar uma chave privada a partir de uma frase-chave. Na aba ”Generate Key” é possível gerar um endereço na rede Bitcoin informando apenas uma senha, o algoritmo gera e retorna uma frase-chave no idioma português de maneira aleatória além do endereço na rede, a chave pública, a chave privada e a chave privada criptografada com a senha informada. Os dados informados na saída do software são apenas para fins explicativos, os únicos dados públicos são o endereço na rede e a chave pública, os demais dados devem ser guardados de forma segura e são o único meio para garantir acesso ao saldo do endereço. A figura 6 apresenta a tela da aplicação para a geração e recuperação de chaves no protocolo do Bitcoin.

O endereço foi gerado na rede de teste do Bitcoin e pode ser consultado de qualquer ferramenta de visualização de dados do blockchain, exemplo: https://live.blockcypher.com/btc-testnet/address/n17fPRR1dHA79dgs3r6WdLHbUcVrkeYnLx

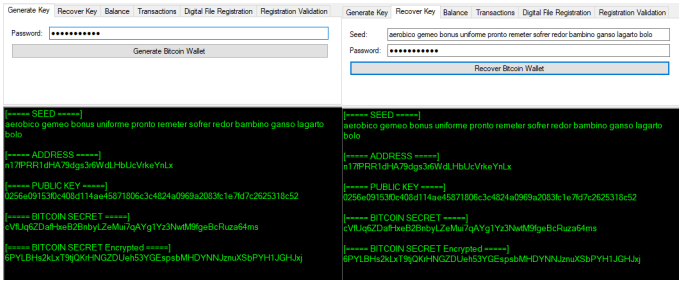

Fig. 6. Geração e recuperação de chaves (Autoria própria).

B. Saldos e Transações do Endereço

Os saldos e as transações são obtidas na rede a partir de qualquer endereço, o processo para obter o saldo de um endereço na aplicação é iniciado fazendo um consulta por todas as transações feitas no endereço e validando as saídas gastas e não gastas de cada transação, desta forma é calculado o saldo final com base na diferença entre os ativos gastas e os ativos recebidos.

A funcionalidade de consulta de transações pode ser feita com base em um endereço da rede, como é demonstrado na figura 7, onde essa consulta retornará todos os detalhes das transações do endereço ou por uma transação específica. O retorno da consulta lista os detalhes do bloco (hash, hash anterior, nonce, confirmações, block time) e os detalhes da transação (fee, entradas, saídas, assinaturas, mensagens), além de detalhes de cada entrada e cada saída que compõem a transação. Todos esses detalhes são públicos e podem ser visualizadas a partir de qualquer ferramenta de visualização de dados do blockchain.

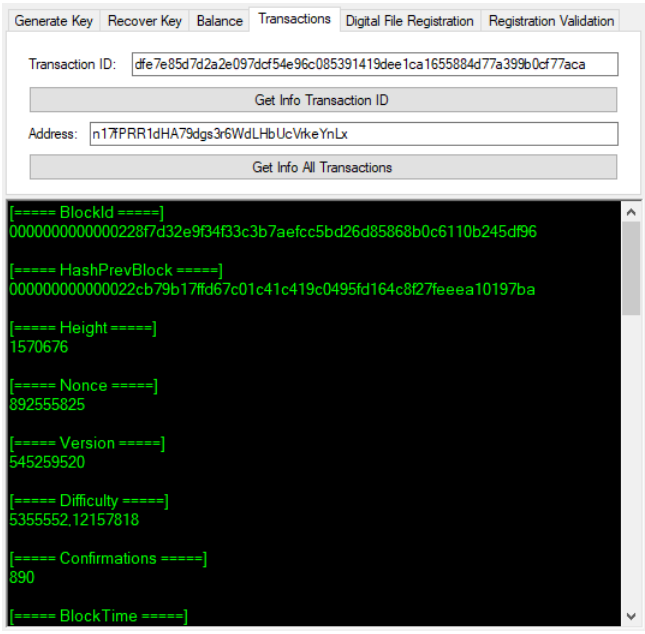

Fig. 7. Consulta de dados de uma transação específica ou de todas as transações de um endereço (Autoria própria).

C. Registro de Arquivos Digitais no Blockchain

O processo de inserir um arquivo digital no protocolo do Bitcoin não é absolutamente fazer a persistência desse arquivo na rede, mas enviar a assinatura digital do arquivo escolhido em uma transação para que futuramente seja possível efetuar uma prova de autenticidade e existência do arquivo na data do registro no blockchain. Para fazer o registro de um documento é necessário possuir um endereço válido no blockchain, estar de posse da chave privada e possuir unidades de Bitcoin para pagar como taxa aos mineradores que propagam e validam a transação e trabalham para a geração do novo bloco.

Para iniciar o processo o BitTrust faz uma varredura por todas as saídas válidas e não gastas que o endereço possui e verifica se as saídas possuem valor maior a zero. Após a consulta de saídas válidas o software desenvolvido solicita a seleção do arquivo que será inserido no blockchain, nessa etapa é iniciado o processo da geração da assinatura do arquivo digital que pode ser visualizado na figura 8. Nesse

processo é feita a extração de todos os bytes do arquivo e aplicada a função de hash SHA256 que retorna uma sequência de 32 bytes representando a assinatura digital do arquivo. Uma das propriedades das funções de hash criptográficas é a sua resistência à colisão, ou seja, é extremamente difícil encontrar duas entradas distintas que resultem no mesmo hash, desta forma a assinatura digital é fortemente confiável para a autenticação de documentos e digitais.

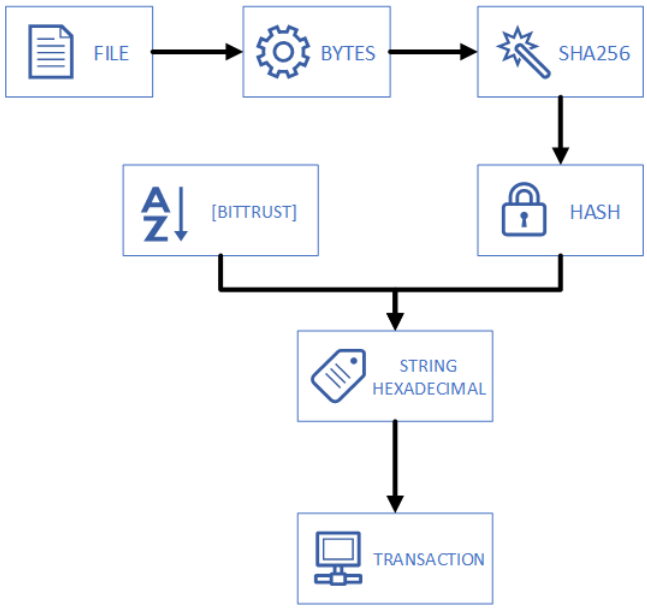

Fig. 8. Etapas do processo de geração da assinatura digital (Autoria própria).

Após a criação do hash do arquivo digital é feita a conversão da assinatura digital para uma *string* hexadecimal e incluído o prefixo *[BITTRUST]* para detectar que aquele registro foi feito através da aplicação desenvolvida. Com a criação da assinatura digital composta pelo prefixo da aplicação é realizada a criação da transação *1:1*, neste processo todas as saídas válidas são incluídas nas entradas da transação, desta forma posteriormente são unificadas em uma única saída válida.

As saídas da transação relacionam o mesmo endereço das entradas, nesta transação especificamente existem duas saídas. A primeira saída está relacionada a atualização do saldo, ou seja, o saldo das entradas atualizado com a taxa de transação. A segunda e mais significativa para esse processo é a saída que armazena a assinatura digital do arquivo, o hash é incluído no script da saída da transação após o opcode *OP_RETURN* usado para transmitir informações adicionais a transação.

Após a composição da transação com as entradas e saídas necessárias é feita a assinatura da transação utilizando o protocolo P2PKH e antes de transmitir pela rede é feita uma validação da estrutura e da assinatura e obtido o tamanho total de bytes da transação, isso é necessário para calcular uma taxa de transação precisa e econômica. A taxa de transação é calcula com base nos valores disponibilizados pela API https://bitcoinfees.earn.com/api, o valor obtido em *hourFee* é multiplicado pelo total de bytes obtidos e atualizado na saída da transação.

Após o processo de cálculo da taxa e a composição da transação é feita a propagação da transação e obtido o hash da mesma para posterior consulta na rede blockchain. O hash da transação é o identificador ou o número de protocolo que pode ser utilizado para validar a autenticidade do arquivo no tempo em que foi incluído no blockchain. A figura 9 demonstra as entradas necessárias e a saída do processo após a propagação da transação na rede.

Fig. 9. Processo de registro de documento digital no blockchain (Autoria própria).

D. Validação de Arquivos Digitais

O processo de validação de autenticidade e existência temporal do arquivo é feito através do hash da transação que gerou o registro da assinatura digital do arquivo na rede blockchain. Para efetuar a autenticação do arquivo o usuário deve estar de posse do arquivo original, além de informar o hash da transação do registro do documento, a aplicação faz uma consulta na rede blockchain e processa as saídas que possuem o opcode *OP_RETURN*.

Com a aquisição dos bytes presentes na saída *OP_RETURN* da transação é feito o cálculo do hash do arquivo importado na aplicação e comparado com a assinatura digital registrada no blockchain. A aplicação calcula e realiza a comparação das duas assinaturas digitais e retorna para o usuário se o arquivo é autentico, ou seja, se a sua integridade está mantida com relação aos dados temporais de registro no blockchain.

XI. Conclusão

Este trabalho teve como objeto o desenvolvimento de uma solução para o registro e autenticidade de documentos utilizando métodos da Segurança da Informação e tecnologias presentes no protocolo Bitcoin. A solução BitTrust visa abstrair toda a complexidade de algoritmos criptográficos e a

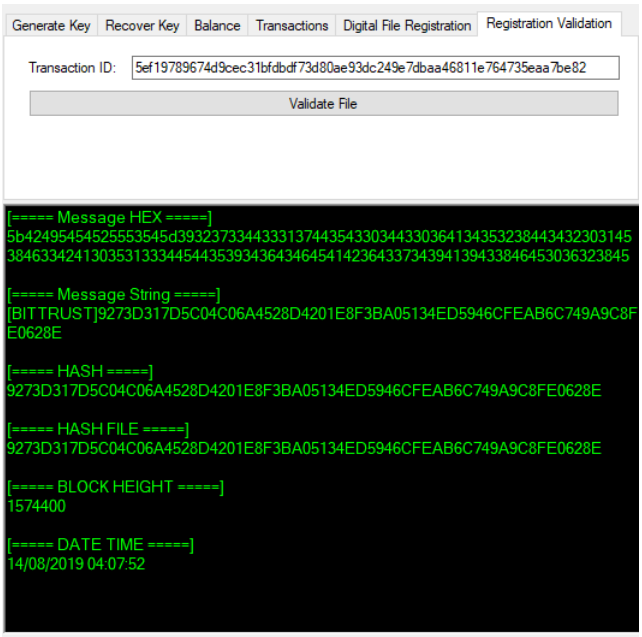

Fig. 10. Processo e retorno após o teste de autenticidade e integridade do documento digital no blockchain (Autoria própria).

comunicação com a rede blockchain, facilitando o registro e a validação de documentos digitais por qualquer usuário.

Com essa solução é possível obter uma validade jurídica do documento digital utilizando uma tecnologia segura e não burocrática, como é o caso dos cartórios atualmente.

De acordo com a Medida Provisória MP 2200/2001 (Artigo 10) o documento digital é valido desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Além de possuir validade jurídica, o documento registrado no protocolo do Bitcoin utiliza todos os benefícios de transparência e descentralização da rede, onde qualquer usuário com acesso a Internet pode consultar o registro do documento na rede.

A. *Trabalhos Futuros*

Para trabalhos futuros, o processo de registro de documentos digitais no blockhain será desenvolvido para outras tecnologias além do Bitcoin, proporcionando dessa forma uma integração maior entre diferentes redes e diminuindo o custo da operação de registro.

Outra melhoria significativa será a disponibilização da aplicação como serviço, sendo possível a criação de aplicativos em diferentes ambientes e tecnologias, proporcionando maior interoperabilidade. Além da utilização da tecnologia de armazenamento distribuído [22], sendo possível o armazenamento do arquivo original em uma rede distribuída.

REFERÊNCIAS

[1] MIT, "Digital certificates project," https://certificates.media.mit.edu, 2015.

[2] OriginalMy, "Pacdigital," https://originalmy.com/pacweb, 2019.

[3] L. V. R. Pinheiro, "Informação: esse obscuro objeto da ciência da informação," *Revista Morpheus-Estudos Interdisciplinares em Memória Social*, vol. 3, no. 4, 2004.

[4] M. Sêmola, "Gestão da segurança da informação: Uma visão executiva. rio de janeiro: Ed," 2003.

[5] P. Representante, B. DO BRASIL, A. Thomé, C. A. Farias Jr, S. EXPERIAN, D. Menoncello, U. G. Ribeiro, I. L. Prícola, G. L. Domingues, T. GLOBO *et al.*, "Tecnologia da informação-técnicas de segurança–código de prática para controles de segurança da informação," 2013.

[6] A. Beal, *Segurança Da Informação: Princípiose Melhores Práticas Para a Proteção Dos Ativos de Informação Nas Organizações*. Editora Atlas SA, 2000.

[7] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] L. Carlozo, "What is blockchain?" *Journal of Accountancy*, vol. 224, no. 1, p. 29, 2017.

[9] W. Dai, "B-money," http://www.weidai.com/bmoney.txt, 1998.

[10] N. Szabo, "Bit gold," https://nakamotoinstitute.org/bit-gold/, 2005, [Online; Acessado em 23-Junho-2019].

[11] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[12] S. Davidson, P. De Filippi, and J. Potts, "Economics of blockchain," *Available at SSRN 2744751*, 2016.

[13] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-oriented software engineering: challenges and new directions," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*. IEEE, 2017, pp. 169–171.

[14] COMPUTERWORLD, "Blockchain privado e público: entenda as principais diferenças," https://computerworld.com.br/2018/03/01/blockchain-privado-e-publico-entenda-principais-diferencas/, 2018, [Online; Acessado em 10-Junho-2019].

[15] G. M. A. Júnior, J. N. D'Almeida Jr, M. T. Onodera, S. M. d. B. M. Moreno, and V. d. R. S. Almeida, "Bndestoken: Uma proposta para rastrear o caminho de recursos do bndes," in *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain-SBRC 2018)*, vol. 1, no. 1/2018. SBC, 2018.

[16] BitcoinWiki, "Transaction," https://en.bitcoin.it/wiki/Transaction, 2019, [Online; Acessado em 25-Junho-2019].

[17] Bitcoin, "Transactions guide," https://bitcoin.org/en/transactions-guide, 2019, [Online; Acessado em 25-Junho-2019].

[18] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127–140.

[19] A. M. BRAGA, "Tecnologia blockchain: Fundamentos, tecnologias de segurança e desenvolvimento de software," 2017.

[20] Bitcoin, "Mining guide," https://bitcoin.org/en/mining-guide, 2019, [Online; Acessado em 21-Junho-2019].

[21] A. Back *et al.*, "Hashcash-a denial of service counter-measure," 2002.

[22] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.