FACULDADE DE TECNOLOGIA, CIÊNCIAS E EDUCAÇÃO

Graduação

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Uso da Blockchain como medida de segurança para o processo eleitoral Brasileiro

Willian Candido Malachias
Lucas Custódio Recco (Orientador)

RESUMO

A tecnologia blockchain emergiu juntamente com a criptomoeda bitcoin, é o mecanismo que registra e valida as transações desta e de outras moedas digitais. Ela rompeu o paradigma de confiabilidade em transações financeiras, trouxe uma abordagem completa- mente diferente da utilizada por bancos e instituições financeiras para realizar operações de valores. Seu principal objetivo é consentir que informações digitais sejam gravadas de maneira distribuída em um grande livro-razão, porém, não editadas. O objetivo desse estudo foi apresentar argumentos, por meio de uma revisão bibliográfica, demonstrando como essa tecnologia emergente pode ser incorporada no processo brasileiro de votação. O sistema brasileiro de votação há anos sofre duras críticas em relação a segurança dos votos, posto que, a urna eletrônica (sistema de contagem de votos), já pôde comprovada- mente ser acessada em testes de segurança. Esse artigo expôs a arquitetura utilizada pela blockchain e o funcionamentos dos protocolos bitcoin como solução para viabilizar uma eleição mais segura e transparante.

Palavras-chaves: Blockchain. Bitcoin. Eleição. Votação. Chave Pública e Privada.

ABSTRACT

The blockchain technology emerged along with the bitcoin criptomoeda, it's the mecha- nism that registers and validates the transactions of this and other digital coins. It broke the paradigm of reliability in financial transactions, brought a completely different appro- ach to that used by banks and financial institutions to carry out financial operations. Its main objective is to allow digital information to be recorded in a distributed manner in a large ledger, but, not edited. The purpose of this study is to present arguments, through the a bibliographic review, showing

how this emerging technology can be incorporated into the Brazilian voting process. The Brazilian voting system has been criticized for years in terms of vote safety, since the electronic ballot box (wishes counting system) already gone accessed in security tests. This article exposes the architecture used by blockchain and the workings of the bitcoin protocols as a solution to make safer and more transparent election.

Keywords: Blockchain. Bitcoin. Election. Voting. Public and Private Key.

Introdução

O surgimento da Blockchain está intimamente ligado ao projeto original do Bit- coin, criado por Nakamoto (2008). Ela foi definida originalmente dentro do código fonte desta criptomoeda, servindo como base de funcionamento. É uma tecnologia baseada em protocolos de confiança que oferece uma estrutura compartilhada entre os participantes, estes que não possuem ligação entre si, apenas estão conectados de forma distribuída den- tro de uma larga rede peer-to-peer, sendo está uma das composições da tecnologia, como também, banco de dados descentralizado. A blockchain possui potencial de transforma- ção para substituir processos burocráticos em rotinas onde existe a necessidade de uma terceira parte de segurança, como processos realizados por bancos, cartórios, unidades certificadoras, entre outras (ULRICH, 2017).

Desde sua criação a tecnologia passou por evoluções, destacadas em 3 projetos: Blockchain 1.0, relacionada com o lançamento do bitcoin em 2008, envolve as imple- mentações iniciais da criptomoeda e sistema de pagamentos; Blockchain 2.0, teve sua idealização em 2013, baseada em contratos inteligentes e, qualquer esfera de operações financeiras; Blockchain 3.0, caracterizada por aplicações em áreas não financeiras, como saúde, governo, ciência e indústrias (BASHIR, 2017).

A alta confiabilidade da blockchain pode ser entendida como resultado da com- binação entre (i) computação distribuída: grande rede de computadores compartilhando poder computacional para determinada finalidade, sistema peer-to-peer; (ii) criptografia de chaves: chaves pública e privada, funções hash e algoritmo de consenso com medidas de segurança; e (iii) teoria dos jogos: incentivos para descoberta de problemas matemá- ticos. A tecnologia também possui forte resistência a ataque de duplo-gasto, impedindo que usuários

dupliquem as informações digitais na rede e, livro-razão distribuído, os da- dos e informações são auditáveis por qualquer usuário de forma pública (GREVE et al., 2018).

O sucesso do bitcoin só se fez possível devido a tecnologia oferecida pela block- chain, um sistema de registro compartilhado que tem como principal característica a des- centralização dos dados e informações como medida de segurança (YLI-HUUMO et al., 2016). O Bitcoin é um modelo de moeda virtual que não carece de um órgão ou ins- tituição centralizada para emitir a moeda, efetivar transações e confirma-las (IANSITI; LAKHANI, 2017). Os autores Pacheco, Araújo e Tavares (2018) definem Bitcoin como: "[...] Neste sistema, os utilizadores têm direitos iguais e não existe uma terceira parte ou autoridade de controle, sendo possível realizar transações entre utilizadores sem a neces- sidade de intermediários [...]".

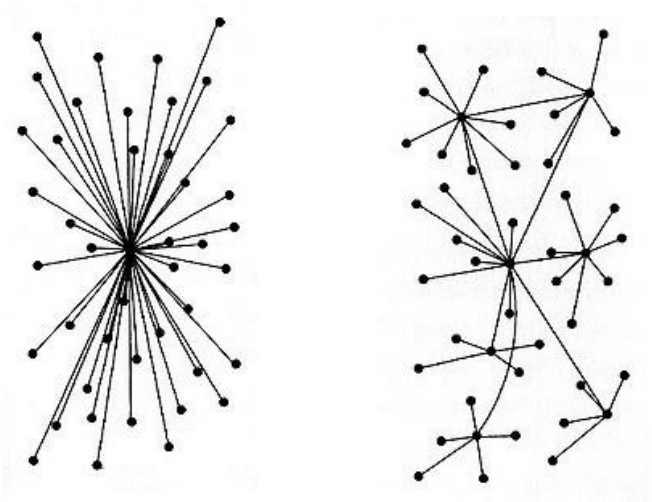
O potencial oferecido pela tecnologia blockchain vêm sendo utilizado amplamente no setor financeiro, mais especificamente com o bitcoin. Os autores Ferreira, Pinto e San- tos (2017) afirmam que 80% do uso da blockchain está relacionado ao bitcoin, e apenas 20% a outras aplicações, como por exemplo, smart contract. Figueiredo (2018) aponta que apesar dos benefícios advindos da blockchain, sua utilização no meio empresarial é muito pequena, motivo associado ao desconhecimento da tecnologia. Uma pesquisa rea- lizada pela empresa "The 451 Group"[1] indica que apenas 28% do setor corporativo global visam usar blockchain em alguma fase de seus processos, e apenas 3% já fazem uso.

1 Estrutura e funcionamento da Blockchain

O conceito acerca do funcionamento da blockchain é dado por "informações arma- zenadas em blocos", onde a descentralização das informações é considerado uma medida de segurança, todos os usuários da rede têm poder sobre os dados, esse conceito pode ser observado na Figura 1 (b). Cada bloco possui uma identificação única chamada de hash, está é uma chave identificadora que garante que as informações daquele bloco não foram

[1] https://451research.com/

alteradas. Quando um novo bloco é formado, este irá possuir uma nova hash exclusiva, além de portar a hash do bloco anterior. Tornando, dessa forma, as transações e infor- mações nos blocos altamente seguras, visto que, para invadir o sistema seria necessário romper a criptografia do bloco atual e anterior de maneira progressiva, esse esforço re- sultaria em um poder computacional incalculável. Logo que uma transação é confirmada pela rede, esse registro jamais poderá ser alterado ou excluído, pois todas as informações registradas tornaram-se públicas (LIMA; HITOMI; OLIVEIRA, 2018).



(a) Rede Centralizada (b) Rede Descentralizada

Figura 1. Tipos de Estruturas de Rede
Fonte: Adaptado de Recuero (2009)

Estende-se ao conceito de blockchain elementos como: (i) rede peer-to-peer: rede de computadores que compartilham informações, trabalho ou dados entre pares. Todos os pares, chamados de nós, possuem o mesmo privilégio. Na rede blockchain cada compu- tador atua como um nó, quando uma nova informação é inserida na rede, essa é compar- tilhada entre todos os nós; (ii) dados distribuídos: a informação fica disponível a todos os nós, dessa forma, se um nó abandonar a rede todos os outros terão uma cópia de toda a informação; (iii) bloco: o bloco gênesis possui as normas e rotinas do estado inicial do sistema, à partir dele outros blocos serão inseridos na cadeia, respeitando a regra básica de que ao final de cada bloco uma assinatura hash é

inserida, essa assinatura é conectada ao bloco anterior, criando uma cadeia de blocos até chegar no bloco gênesis; (iv) algoritmo de consenso: utilizado para resolver um problema matemático extremamente complexo, nenhuma informação pode ser inserida na rede antes da resolução do algoritmo. O nó que primeiro encontrar a solução deverá passar o resultado aos outros nós da rede, estes irão validar o resultado. Um novo bloco só é considerado aberto (minerado) quando as normas estabelecidas pelo algoritmo de consenso forem satisfeitas, alcançando a confiabilidade total da rede (AITZHAN; SVETINOVIC, 2018).

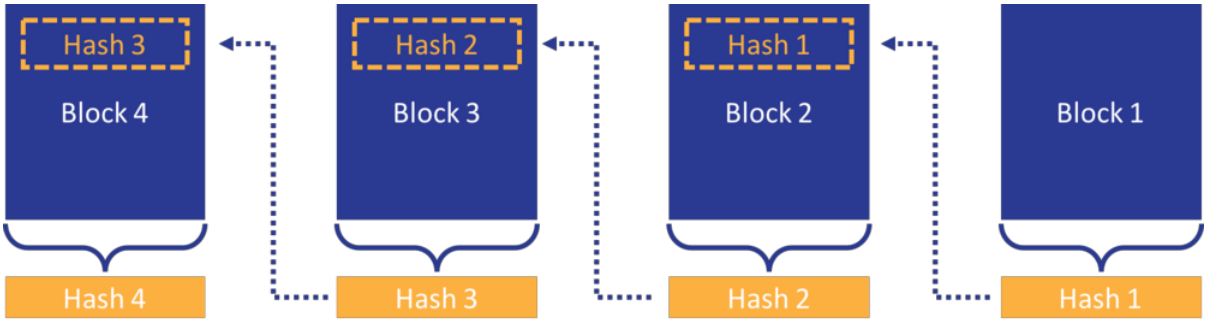


Figura 2. Diagrama Blockchain
Fonte: (NARAYANAN, 2016)

Além dos elementos presentes na Figura 2, também compõe a estrutura da blockchain um Nonce e um Data. O autor Chicarino et al. (2017) define esses elementos como:

• Block: número de identificação de cada bloco, número que não se repete;

• Nonce: número único e arbitrário; gerado de forma aleatória ou pseudo-aleatória à fim de garantir um protocolo de autenticação;

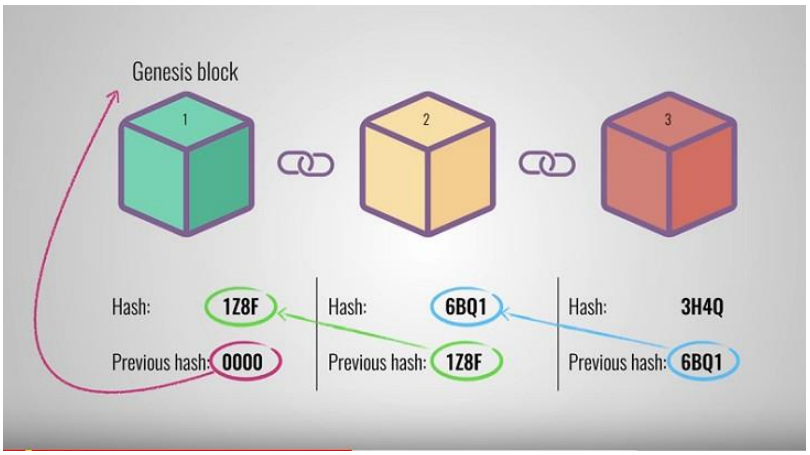
• Data: conjunto de entrada; são todos os dados, informações e transações presentes

no bloco. No Data são armazenados todos os registros de entrada (endereço de origem) e saída (endereço de destino) das informações. A informação gerada por um nó é passada a todos os nós vizinhos, estes por sua repassam essa informação para todos seus vizinhos, fazendo com que toda a rede tenha acesso a informação;

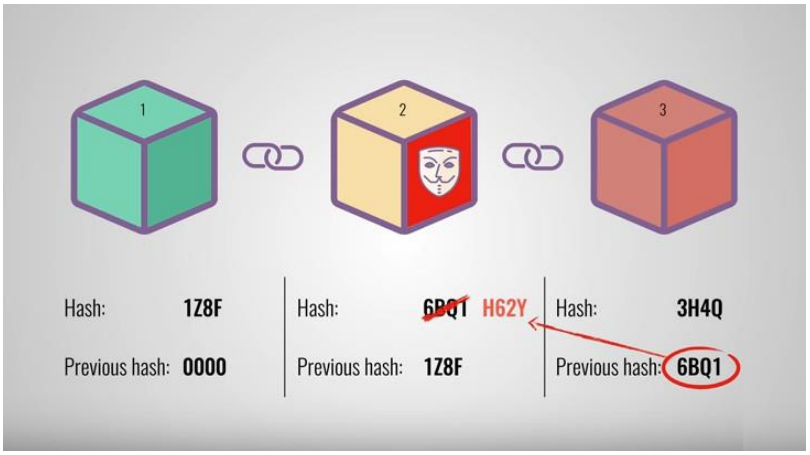
• Prev Hash: valor que permite que um bloco seja conectado ao anterior; como demonstrado na Figura 2, o Block 2 possui a hash do Block 1, dessa forma, todos

os nós da rede vão possuir a hash e informação do Block 1, criando assim, uma "cadeia de blocos" (tradução de blockchain);

• Hash: identificação principal do bloco; número criptografado criado à partir do conteúdo inserido no data, sempre que uma nova operação é criada, altera-se o valor da hash, assim, quando um bloco é fechado e auditado pela rede, as infor- mações contidas nele não podem mais ser alteradas. A tentativa em alterar alguma informação resultaria em uma não-validação do bloco atual e seguinte, dado que, uma hash fora alterada, quebrando assim, a conexão entre os blocos da cadeia. A Figura 3 ilustra esse conceito:



(a) Cadeia de blocos original



(b) Cadeia com tentativa de fraude

Figura 3. Resistência de um bloco a ataques
Fonte: Adaptado de Amoyal (2018)

No exemplo acima, Figura 3 (b), a tentativa em alterar o conteúdo do data provo- cou a mudança do valor da hash, esse comportamento não seria validado pela rede, dessa forma, os dados seriam preservados.

1.1 Propriedades da Blockchain

Os autores Greve et al. (2018) apontam 7 propriedades que contribuem para o desenvolvimento inovador da tecnologia blockchain, permitindo sua utilização em dife- rentes sistemas e aplicações. São dados como: (i) Descentralização: principal motivador da tecnologia, as aplicações são executadas de forma distribuída, sem a necessidade de uma instituição de confiança; (ii) Disponibilidade e Integridade: todas as informações es- tão disponíveis a todos nós da rede e, todos mantém uma cópia de todas as informações; (iii) Transparência e Auditabilidade: todas as operações registradas no livro-razão podem ser auditadas e verificadas por qualquer usuário da rede; (iv) Imutabilidade e Irrefutabi- lidade: uma vez registradas no livro-razão, as operações jamais poderão ser alteradas, atualizações ocorrem apenas com a geração e validação de novos blocos; (v) Privacidade e Anonimidade: a identidade dos usuários permanecem anonimas, cada usuário possui controle sobre suas chaves; (vi) Desintermediação: a blockchain possui a característica de alcançar sistemas (clientes) sem a necessidade de intermediários; (vii) Cooperação e Incentivos: os nós que validam as operações cedendo poder computacional a rede, rece- bem como incentivo uma taxa sobre as transações realizadas.

1.2 Tipos de Blockchain

Os autores Lin e Liao (2017) definem que a tecnologia blockchain é subdividada em 3 tipos básicos:

1. Blockchain Pública: todas as transações são públicas a rede, qualquer pessoa pode ter acesso. Nesse modelo ninguém é possuidor da rede, toda adição de dados necessita ser validada pelos participantes;

2. Blockchain de Consórcio: os nós tem autoridade em escolher que os dados sejam públicos ou privados, esse modelo de blockchain é controlado por um número restrito de nós, normalmente utilizado como modelo de negócio, onde mantém-se a privacidade das transações. Esse tipo de blockchain é considerado parcialmente descentralizada, nem toda a rede faz parte do processo de revisão das transações;
3. Blockchain Privada: acesso restrito as transações, são moderados por uma única organização, está determina quem poderá enviar e receber transações. Muito uti- lizada em ambientes restritos, ondem os dados são sigilosos, normalmente por empresas que não querem que seus dados fiquem documentados em cadeias de blocos sem um mediador.

2 Problemática

O sistema atual de votação brasileiro é realizado através de "urnas eletrônicas". A primeira eleição eletrônica ocorreu em 1996, onde parte população votará com essa nova tecnologia[2].

A urna eletrônica é composta por dois terminais, (i): o terminal do mesário, onde verifica-se se o eleitor faz parte daquela sessão de votação, se sim, autoriza-se o voto; (ii): a própria urna eletrônica, onde são armazenados de forma aleatória e criptografada os votos. Durante a votação a urna não possui acesso à internet, os votos contabilizados são armazenados em um pendrive. Após o termino das eleições, a transmissão dos votos ao TRE (Tribunal Regional Eleitoral) é realizado através de uma rede privada[3].

Desde então, a integridade e segurança dos votos vem sendo questionada, visto que, a transmissão é realizada através de uma de rede de internet, expondo os dados a ataques e alterações durante o envio.

Os autores Aranha et al. (2012), realizaram um relatório técnico sobre as vulne- rabilidades no software da urna eletrônica, do qual, registraram um grave problema de segurança no sistema. Em testes públicos supervisionados pelo TSE (Tribunal Superior Eleitoral) foi possível acessar o RDV (registro digital do

[2] http://www.tse.jus.br/imprensa/noticias-tse/2014/Junho/conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos
[3]https://epocanegocios.globo.com/Brasil/noticia/2018/10/entenda-como-funciona-urna-letronica-utilizada-no-brasil.html

voto). O RDV é uma especie de log da votação, com a falha da urna foi possível visualizar os votos em ordem cronológica, não possível associar o voto ao eleitor nem altera-lo, porém, o acesso ao RDV não deixou nenhuma indicação de que fora visto, a auditoria da urna eletrônica jamais saberia que o log de votação havia sido visualizado.

O mesmo problema foi registrado no ano de 2017, quando novamente em testes públicos supervisionados pelo TSE, especialistas em segurança da informação mais uma vez obtiveram exito em acessar o RDV[4].

3 Justificativa

O sistema brasileiro de votação vêm a cada eleição sofrendo duras críticas pelos eleitores, em toda eleição fortes questionamentos são feitos sobre a segurança e inviola- bilidade dos votos (ARRUDA, 2017). A própria NASA (National Aeronautics and Space Administration), agência espacial americana, afirma que em 2011 sofreu 13 ataques de onde credenciais de funcionários e projetos foram roubados[5], evidenciando a fragilidade na transmissão dos votos em eleições brasileiras.

Considerando a importância da democracia para o sistema público brasileiro e para o próprio brasileiro, é fundamental que esse direito seja integralmente preservado, não permitindo que velhas práticas de segurança coloquem em dúvida a integridade do sistema brasileiro de votação. Pensando nisso, este estudo através de uma revisão teórica, propôs o uso de blockchain em eleições eleitorais brasileiras, onde a votação e apuração teriam maior transparência e credibilidade ao eleitor. A blockchain é uma tecnologia baseada em protocolos de confiança, os registros da eleição não ficariam subordinados a uma instituição centralizadora, todas as informações ficariam distribuídas pela rede, que é baseada em validações de múltiplos usuários como medida de segurança.

Recentemente tal tema vêm sendo estudado e discutido como forma de viabilizar uma eleição mais segura. Nos Estados Unidos a tecnologia blockchain

[4]https://epocanegocios.globo.com/Brasil/noticia/2018/10/entenda-como-funciona-urna-eletronica-utilizada-no-brasil.html

[5] http://g1.globo.com/tecnologia/noticia/2012/03/nasa-diz-que-sofreu-13-ataques-de-hackers-em-2011.html

será utilizada em carácter experimental para uma eleição restrita a militares no estado da Virgínia Ocidental[6]. Na Suiça, uma votação municipal piloto foi criada para testar a eficiência e integridade do sistema[7].

4 Trabalhos Relacionados

Para Silva (2018), o uso de blockchain no processo eleitoral seria a forma mais viável de garantir uma eleição transparante e sem fraudes. O autor defende a viabilidade da tecnologia em eleições fundamentado na imutabilidade dos dados, onde as informações e registros dos votos ficariam em uma rede descentralizada, os dados não estariam sob o poder de uma única instituição ou pessoa. Outro ponto abordado é um sistema de votação baseado em blockchain do tipo privada, onde somente membros autorizados por uma entidade mediadora poderiam participar da rede.

Lima, Hitomi e Oliveira (2018) propuseram o uso da tecnologia blockchain como solução em ambientes corporativos, objetivando redução de custos, maior segurança, au- tenticidade e privacidade nas rotinas internas das empresas. Os autores argumentam que a tecnologia já vem sendo utilizada por grandes empresas como IBM, Oracle, Porshe e Go- ogle em forma de "contratos inteligentes", onde não existe interferência de outras partes. Também argumentam que, segundo um estudo realizado pela revista online de The Economist[8], os bancos poderiam economizar em seus caixas cerca de US% 20 bilhões anuais com a sincronização de seus livros-razões entre corporações de mesmo seguimento. A sincronização tradicional exige muito tempo e recurso financeiro, a blockchain reduziria gastos em tempo, riscos e custos desse processo.

Arruda (2017) propõe a criação de uma infraestrutura baseada na descentralização para auditar e validar votos em uma eleição utilizando blockchain. Cada eleitor poderia votar anonimamente utilizando sua chave pública, transferindo seu voto para a carteira de seu candidato. A blockchain registraria as operações de votos, as chaves públicas com maior quantidade

[6] https://portaldobitcoin.com/blockchain-testada-eleicao-estados-unidos/
[7] https://www.btcsoul.com/noticias/votacao-baseada-blockchain-considerada-sucesso-zug/
[8] https://www.economist.com/

de votos por cargo disputado venceria a votação. O autor ainda argumenta que, uma eleição utilizando blockchain como forma de auditar os votos seria uma maneira transparente de realizar tal processo, uma vez que, o número de votos por candidato poderia ser acompanhado em tempo real em qualquer parte do mundo.

Lavina (2018) defende o uso de blockchain para solucionar um grave problema existente no setor público e privado de saúde, compartilhar as informações de pacientes entre as inúmeras organizações de saúde existentes. O blockchain tem potencial para armazenar de forma segura e inviolável todas as informações pertinentes ao quadro do paciente, como medicamentos utilizados, dieta, tratamentos e genética. Permitindo, dessa forma, que profissionais da saúde tenham o registro médico do paciente sempre atualizado e, possam tomar decisões baseadas em um histórico.

Chicarino et al. (2017) apresentaram o uso de blockchain para aumentar a segu- rança e privacidade em IOT - Internet da Coisas. O conceito de IOT é dado por dispositi- vos conectados a internet coletando e compartilhando dados, como exemplo destacam-se, cidades inteligentes, saúde supervisionada, casas online, carros autônomos, entre outras. Com o crescimento de IOT, cada vez mais dispositivos estão conectados a internet. Junto a expansão dessa tecnologia surge o problema de segurança das informações comparti- lhada pelos dispositivos. Os autores propuseram o emprego de blockchain em IOT com a finalidade de oferecer uma estrutura padronizada para os dispositivos conectados, ob- jetivando agilizar a troca de informações entre eles, dispensando a necessidade de um servidor centralizado.

5 Objetivos

5.1 Geral

Demonstrar como a tecnologia blockchain pode ser utilizada como solução para garantir eleições mais seguras e transparantes. Apresentando argumentos que comprovem a alta confiabilidade e robustez do sistema para uma eleição eleitoral.

5.2 Específico

• teorizar a estrutura e elementos para funcionamento da blockchain;

• categorizar os conceitos de bloco, hash, blockchain pública e privada, chaves pú- blicas e privada;

• compreender o movimento de transações com bitcoin para clareza da metodologia proposta.

6 Metodologia

Para poder compreender a metodologia proposta por esse estudo será necessário estender o conhecimento ao funcionamento de transações utilizando a criptomoeda bit- coin.

6.1 Funcionamento da criptomoeda

6.1.1 Chaves Pública e Privada

Inicialmente é necessário que o usuário que deseja transacionar bitcoins tenha uma carteira digital para isso; essa carteira servirá como forma de armazenar a moeda e endereço público (ROCHA; RODRIGUES, 2016). A Figura 4 exemplifica os elementos básicos de uma carteira bitcoin.

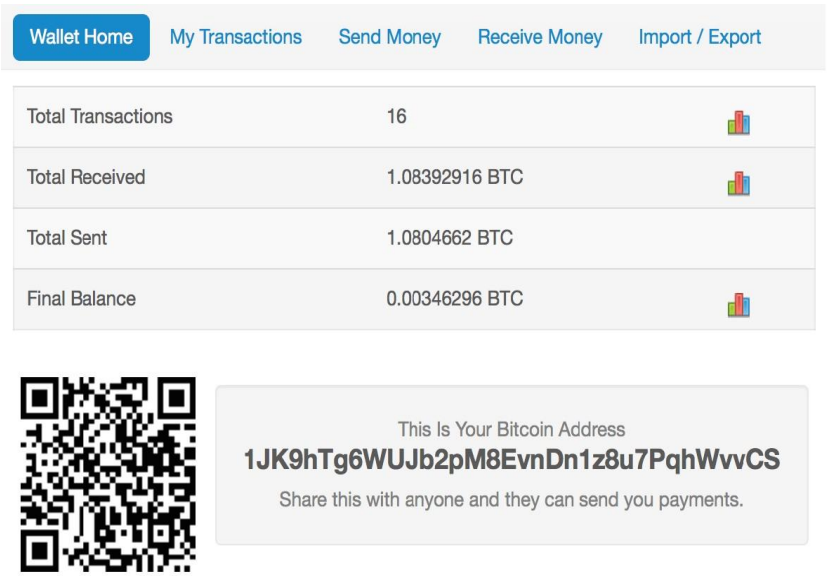


Figura 4. Carteira Bitcoin
Fonte: Adaptado de Betbybitcoin (2016)

A própria carteira criará para o usuário um par de endereços constituídos de letras e números, denominados chaves publica e privada. Na Figura 4 é apresentada a chave pública do usuário, essa chave é pública e de livre conhecimento da rede blockchain. Sempre que o usuário for receber saldo em bitcoins, ele deverá informar essa cadeia de números ou QR Code ao outro utilizador que lhe deseja enviar "moedas" (PREVIDI, 2014).

A chave privada, também criada pela carteira, é um arranjo de letras e números que autorizam o proprietário da carteira a gastar os bitcoins de um endereço público, é a assinatura digital do usuário. A chave pública é derivada da chave privada, está que cria endereços públicos para receber saldo em bitcoins (GREVE et al., 2018). A Figura 5 apresenta um exemplo de chave pública e privada e funcionamento prático.

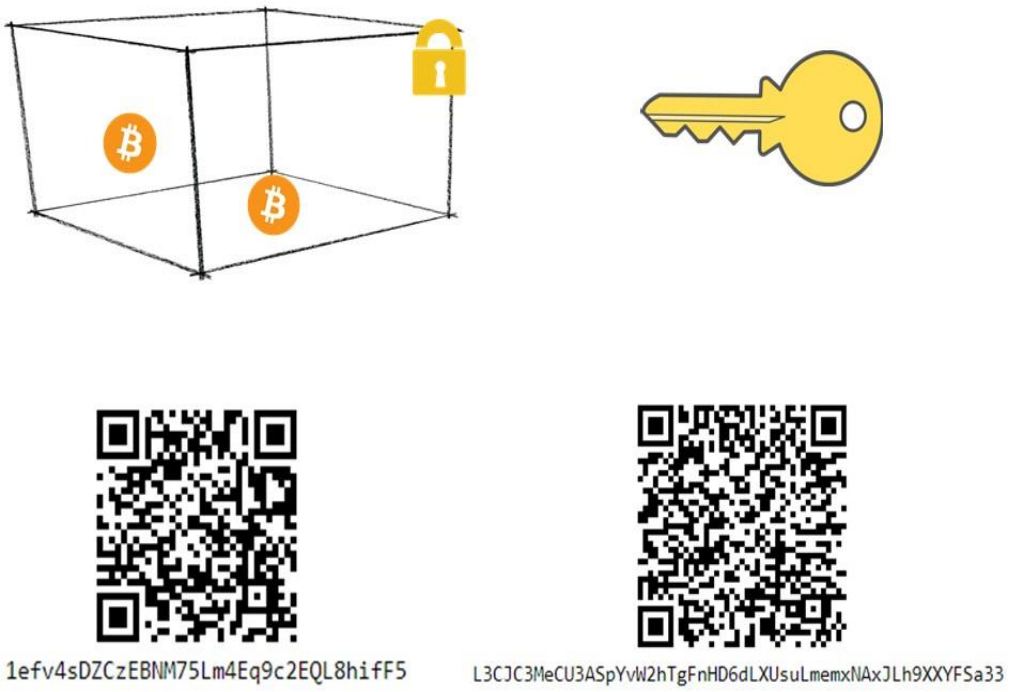


Figura 5. Tipos de Chave
Fonte: (BONDER, 2017)

A Figura 5 elucida o funcionamento das chaves pública e privada definido por Bonder (2017). O autor compara a chave pública a uma caixa de vidro onde se pode conhecer o conteúdo (no exemplo duas moedas) e, uma chave de cadeado a chave privada. O endereço da caixa de vidro (chave pública) fica público a rede, porém, a caixa só poderá ser aberta com a posse da chave do

cadeado (chave privada). A caixa de vidro também não traz nenhuma informação de seu proprietário, mantendo o sigilo das informações de seu possuidor.

Existem dois tipos de carteiras para armazenar bitcoins, carteiras online e cartei- ras físicas (propriamente instaladas em computadores ou celulares). Como exemplo de carteira online pode-se citar a BitCointrade[9], e carteira física a Exodus[10]. A grande diferença entre ambas está no poder da chave privada, na carteira online, a chave privada (assinatura digital do usuário), fica em poder da carteira, salvo é claro, que para confir- mar transações o usuário utiliza uma senha eletrônica criada por si próprio. Nas carteiras físicas, essa sequência de letras e números é totalmente restrita ao possuidor da carteira, não tem conexão com a internet e, é umas das formas de recuperar acesso a carteira caso o usuário esqueça seu login ou senha (NIELSEN, 2013).

6.1.2 Mineradores

O processo de validar as transações existente na rede, criação de novos blocos e fechamento de blocos é realizado pelos mineradores. A mineração de criptomoedas pode ser entendida, portanto, como registro de operações em blocos (livro-razão). Essa atividade é remunerada em forma de moedas para os que tiveram êxito em efetuar as ope- rações em menor tempo. Em média, um bloco de bitcoin é minerado a cada 10 minutos, tempo necessário para auditar as informações, validar o bloco e fecha-lo para criação de um novo (EYAL, 2015).

A função fundamental dos mineradores é assegurar que as transações que estão ocorrendo sejam validas, verificando o saldo do endereço de origem e validando como existente o endereço de destino, impossibilitando, assim, operações ilegítimas. Para isso, eles cedem poder computacional a rede com o objetivo de resolver cálculos complexos, cuja finalidade é registrar as operações decorrerentes na rede (SIRER; EYAL, 2018).

[9] https://bitcointrade.com.br/
[10] https://www.exodus.io/

6.2 Blockchain nas Eleições

Após compreensão das transações com bitcoins, a percepção da metodologia ado- tada torna-se simples.

Em conjunto com órgãos eleitorais, seria criada uma carteira física de votação, dado que, nas carteiras físicas a chave privada ficaria em posse do usuário, aumentado a segurança da eleição. Nessa carteira, os eleitores aptos ao voto já estariam previamente cadastrados.

Em uma plataforma digital ficariam registrados as chaves públicas de todos os candidatos, permitindo aos eleitores encontrar as carteiras para qual iriam transferir seus votos. A plataforma de votação só poderia ser acessada no dia da eleição, respeitando os mesmos horários de votação já estipulados pelo TSE, dás 08h00 às 17h00[11], horário local de cada estado.

Cada eleitor, previamente cadastrado na plataforma, receberia uma quantidade de tokens de acordo com o tipo de eleição, por exemplo, em uma eleição presidencial cada usuário receberia 6 tokens. O eleitor enviaria seu token (voto) para a carteira de seu candidato, essa por sua vez só deve aceitar 1 token por chave pública, impedindo que o mesmo eleitor vote no mesmo candidato repetida vezes.

Como forma de aumentar a segurança durante a votação, cada voto enviado, além da confirmação da chave privada, também seria autenticado por uma ferramenta de "Con- firmação em 2 Passos" oferecido pelo Google[12]. Essa autenticação consiste em confirma- ções de senhas aleatórias para determinados acessos, tais confirmações são geradas com auxílio de um smartphone. Empresas como Facebook, Gmail, Microsoft, entre outras, já permitem esse tipo de autenticação. Dessa forma, se o eleitor tivesse sua chave pri- vada roubada, a pessoa que a roubou não conseguiria votar em seu lugar, pois a segunda validação falharia.

Todo o processo de transferência dos votos seria realizado e auditado pela block- chain utilizando seus protocolos de confiabilidade e informações descentralizadas, a vali- dação e integridade dos votos ficaria a cargo da rede.

[11] http://www.tse.jus.br/imprensa/noticias-tse/2018/Agosto/tse-mantem-horario-de-votacao-nas-eleicoes-2018
[12] https://www.google.com/landing/2step/

Dado que, as eleições são um tipo de ambiente restrito, o tipo de blockchain utili- zada seria a privada, onde as informações seriam moderadas por uma única organização e, o acesso a rede seria limitado. As informações ainda ficariam auditáveis pelos eleitores, porém, somente com o consentimento do responsável pela rede; visto que o objetivo de se utilizar blockchain em eleições é aumentar a transparência da votação, esse privilégio seria automaticamente fornecido a todos os eleitores participantes da rede ao final da elei- ção. A blockchain do tipo pública causaria um problema de "antecipação da apuração dos votos", posto que, as chaves públicas dos candidatos estariam públicas a rede, podendo influenciar o resultado das eleições. Todas as informações individuais dos eleitores per- maneceriam seguras, no final, os candidatos com maior número de tokens por ocupação venceriam a eleição.

Trabalhos Futuros

O levantamento teórico foi uma difícil etapa durante a produção desta obra, visto que, a tecnologia blockchain é uma inteligência em estágio embrionário, muitas pesquisas ainda estão sendo realizadas acerca desse tema, autores ainda buscam possibilidades de aplicação e melhor aproveitamento dessa recente inovação. Diante disso, esse estudo propõe como possíveis trabalhos futuros:

- forte aprofundamento na tecnologia blockchain e conceitos;
- levantamento bibliográfico para aplicação de blockchain em outros campos da sociedade;
- aprimoramento do conteúdo apresentado neste artigo e;
- esse estudo teve apenas carácter de explanação teórica, apresentado argumentos que comprovem o potencial da blockchain para auditar eleições.

Uma das suges- tões para trabalhos futuros seria a implementação de um sistema demo, este que contemplaria as características descritas nesta obra. Dessa forma, testes experi- mentais poderiam ser realizados em eleições modelos juntamente com a supervi- são de um órgão governamental.

Considerações Finais

Este estudo apresentou uma proposta de integração da tecnologia blockchain como medida de maximizar a segurança, confiabilidade dos dados e transparência em eleições brasileiras, onde a validação e filtragem dos votos seria realizado pelos protocolos de confiança oferecidos pela blockchain, sem a necessidade de uma terceira organização. Esses atributos são características da rede descentralizada presente na tecnologia, permi- tindo uma eleição mais democrática para o estado, especialmente em sistemas eleitorais diretos, como do Brasil.

Umas das grandes vantagens desse sistema seria a enorme e inquestionável trans- parência oferecida ao eleitor, diferente do sistema atual. Todas as informações de votos e candidatos presentes na blockchain seriam facilmente auditáveis por qualquer usuário, preservando ainda, todas as informações pessoais dos eleitores.

A agilidade na apuração seria outro ponto importante, em eleições tradicionais o resultado dos votos costumam ser divulgados à partir das 21h00, visto que as eleições terminam às 17h00. Com a blockchain, o prazo máximo para divlgação dos resultados seriam de 10 minutos, tempo necessário para abertura e fechamento de um bloco.

Redução de gastos nos cofres públicos, uma eleição com blockchain diminuiria de maneira considerável despesas com urnas eletrônicas, segurança, organização de uma eleição, remuneração de mesários convocados para fiscalizar os locais de votação. To- davia, ainda seria necessário uma infraestrutura pequena para atender aqueles que não possuem acesso a internet, garantido-lhe o direito de voto previsto em Lei nº 4.737[13].

Um ponto desfavorável seria o desconhecimento do uso da tecnologia por parte da população, uma vez que a proposta necessita de um conhecimento prévio acerca de chave pública, chave privada, tokens e confirmação em 2 passos. Isso forçaria o eleitor a procurar auxílio de um usuário mais experiente, este que poderia persuadir seu voto. Esse inconveniente poderia ser contornado

[13]http://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965

com a "reeducação dos eleitores" para adaptação ao novo sistema, da mesma forma como fora feito com as urnas eletrônicas; e também, postos de votação prontos para atender eleitores com eventuais dúvidas e sem acesso a internet.

A blockchain possui grande potencial para receber uma eleição, talvez num período não tão próximo, devido sua baixa popularização entre pessoas e empresas, porém, com incentivos de órgãos públicos e privados, a tecnologia poderá ser adotada não so- mente em eleições, mas em qualquer atividade que sua versatilidade possa satisfazer.

Referências

AITZHAN, N. Z.; SVETINOVIC, D. Security and privacy in decentralized energy tra- ding through multi-signatures, blockchain and anonymous messaging streams. **IEEE Transactions on Dependable and Secure Computing**, v. 15, n. 5, p. 840-852, 2018.

AMOYAL, D. What is blockchain technology. **Chainbits**, oct. 2018. Disponível em: <https://www.chainbits.com/blockchain-101/ what-is-blockchain-technology/>. Acesso em: 19 dez. 2018.

ARANHA, D. F. et al. Vulnerabilidades no software da urna eletrônica brasileira. **Relatório Técnico**, v. 18, p. 19, 2012.

ARRUDA, G. O. de. A tecnologia a serviço da democracia: O processo eleitoral na era da informação. **Revista da Advocacia Pública Federal**, v. 1, n. 1, 2017.

BASHIR, I. **Mastering Blockchain:** Distributed ledgers, decentralization and smart contracts explained, Book Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained. [S.l.]: Packt Publishing, 2017.

BETBYBITCOIN. **Blockchain.info wallet:** Be your own bank. may 2016. Disponível em:<http://betbybitcoin.com>. Acesso em: 14 dez. 2018.

BONDER, O. **O que são chaves pública e privada. 2**017. Disponível em: <https://medium.com/@otaviobonder/o-que-s\%C3\%A3o-chaves-p\ %C3\%BAblica-e-privada-f5897e0a8395>. Acesso em: 14 dez. 2018.

CHICARINO, V. et al. **Uso de blockchain para privacidade e segurança em internet das coisas.** Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, 2017.

EYAL, I. The miner's dilemma. In: IEEE. **Security and Privacy** (SP), 2015 IEEE Symposium on. [S.l.], 2015. p. 89-103.

FERREIRA, J. E.; PINTO, F. G. C.; SANTOS, S. C. dos. Estudo de mapeamento sistemático sobre as tendências e desafios do blockchain. **Gestão.org: Revista Eletrônica de Gestão Organizacional**, 2017.

FIGUEIREDO, A. Blockchain: Tecnologia pode ser grande aliada para aumentar compe- tividade nas empresas. **Revista Fenacon**, v. 187, 2018.

GREVE, F. et al. Blockchain e a revolução do consenso sob demanda. SBRC, Ufscar, 2018.

IANSITI, M.; LAKHANI, K. R. The truth about blockchain. **Harvard Business Review**, v. 95, n. 1, p. 118-127, 2017.

LAVINA, M. E. Validação do uso da tecnologia blockchain para o tráfego seguro de dados na área da saúde. **Gestão da Segurança da Informação-Unisul Virtual**, 2018.

LIMA, B. H. N.; HITOMI, F. A. C.; OLIVEIRA, G. S. de. Aplicação da tecnologia block- chain em ambientes corporativos. **FaSCi-Tech**, v. 1, n. 13, 2018.

LIN, I.-C.; LIAO, T.-C. A survey of blockchain security issues and challenges. **IJ Network Security**, v. 19, n. 5, p. 653-659, 2017.

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. Working Paper, 2008. NARAYANAN, V. How blockchain works. mar 2016. Disponível em: <https://medium.com/@venkinarayanan/how-blockchain-works-b0a62ca2fca1>. Acesso em: 12 dez. 2018.

NIELSEN, M. **How the bitcoin protocol actually works.** 2013. Disponível em: <http://www.michaelnielsen.org/ddi/ how-the-bitcoin-protocol-actually-works/>. Acesso em: 14 dez. 2018.

PACHECO, L. M.; ARAÚJO, B.; TAVARES, F. O. A bitcoin e o seu desenvolvimento: estudo aplicado a uma amostra representativa. **Revista Espacios**, v. 39, n. 17, 2018.

PREVIDI, G. D. S. **Descentralização monetária:** um estudo sobre o bitcoin. 2014.

RECUERO, R. **Redes sociais como estruturas de poder.** 2009. Disponível em: <http://www.raquelrecuero.com/arquivos/redes_sociais\ _como_estruturas_de_poder.html>. Acesso em: 15 dez. 2018.

ROCHA, J. G. da; RODRIGUES, C. K. da S. O processo de negócio do sistema de transações financeiras bitcoin. **Universitas: Gestão e TI**, v. 6, n. 1, 2016.

SILVA, M. P. A segurança da democracia e a blockchain. **Projeção, direito e sociedade**, v. 9, n. 1, p. 119-138, 2018.

SIRER, E. G.; EYAL, I. Majority is not enough: Bitcoin mining is vulnerable. **Communications of the ACM**, v. 61, n. 7, p. 95-102, 2018.

ULRICH, F. **Bitcoin**: a moeda na era digital. [S.l.]: LVM Editora, 2017.

YLI-HUUMO, J. et al. Where is current research on blockchain technology? A systematic review. **PloSone, Public Library of Science**, v. 11, n. 10, p. e0163477, 2016.