

Sistema distribuído de votação via internet através do uso de *smart contracts*

RESUMO

No Brasil, as urnas eletrônicas sempre foram alvo de críticas pois os eleitores não sabem se de fato os votos foram para os candidatos desejados. Assuntos como imutabilidade, integridade e transparência dos votos sempre emergem. Dessa forma, este artigo sugere o uso de duas tecnologias, que são o blockchain e smart contracts, como proposta de serem usados em um sistema distribuído de votação, feito a partir da Internet, que tem seus dados registrados e validados através de uma rede de computadores, o que garante o chamado consenso. Com o grande impacto das criptomoedas, temos o surgimento da plataforma Ethereum, onde é possível realizar transações online através do uso de smart contracts, não somente para aplicações financeiras de moedas digitais. O presente artigo propõe ainda uma análise exploratória sobre essas tecnologias. Para tal, criamos uma simulação de votação através da plataforma Ethereum e de um smart contract programado em Solidity para demonstração da aplicação. Com resultados positivos da simulação, o uso das tecnologias aqui abordadas deixa evidente que sua implementação seria um grande passo para democracia, além da redução de custos, desperdícios, e da melhora da imagem corporativa.

PALAVRAS-CHAVE: Ethereum. smart contracts. Blockchain. Democracia. sistemas distribuídos.

Wesley Felix de Lima

Universidade Nove de Julho, Barra Funda, São Paulo.

wesley.felixdelima96@hotmail.com

Daniela Manetta Vasconcelos

Universidade Federal do Estado de São Paulo, São Paulo.

daniela.manetta78@gmail.com

Flavio Grassi

Universidade Nove de Julho, Barra Funda, São Paulo.

flaviograssi.fg@gmail.com

INTRODUÇÃO

O sistema de votação do Brasil é um ato de cidadania e democracia que, desde que foi implementado, passou por inovações a fim de garantir um processo seguro e confiável (TSE, 2016). Mesmo na emissão do Boletim de Urna (BU), toda validação ocorre na própria urna eletrônica, onde não existem garantias para o cidadão se esta foi adulterada.

As urnas eletrônicas trazem muitas dúvidas para os eleitores, principalmente por situações que já ocorreram no passado, como foi o caso estudado das eleições para vereadores em 2008 e 2012, representando o distanciamento e o desrespeito à democracia (Carlomagno, 2016). Um exemplo foi o popularmente chamado “efeito Tiririca” (Carlomagno, 2016), em que o eleitor não está votando no candidato e sim no partido (coligação) à qual o candidato pertence, no intuito de somar todos os votos e dividir pelo número de cadeiras disponíveis, através da manipulação do algoritmo da urna.

É notável que os eleitores brasileiros não têm participação ativa nos processos eleitorais. Apesar de utilizar uma tecnologia moderna para as eleições, não há confiança na mesma. Com os avanços tecnológicos, podemos optar por sistemas mais seguros que garantam a integridade dos votos. Uma alternativa seria optar pela tecnologia Blockchain, um sistema totalmente distribuído que propõe empoderamento para seus usuários e conta com uma rede descentralizada em que os participantes têm transparência no que ocorre em todo ecossistema, garantindo que todas as transações feitas sejam íntegras (Arruda, 2017).

Na era da informação, a tecnologia está a serviço da democracia e podemos utilizar os recursos disponibilizados para assegurar a integridade de votos em eleições, em decisões de board de diretores de empresas privadas, transações bancárias, entre outras ocasiões. Nesse contexto, conforme Clack, et al. (2016), os smart contracts, são contratos inteligentes escritos em linguagens de programação (algoritmos) que têm regras e ações, que se assemelham à contratos tradicionais, mas diferentemente destes, fazem uso de técnicas que garantem integridade das transações através do uso de rede de computadores, estrutura de dados e protocolos apropriados. Eles são armazenados em um banco de dados descentralizado, e o Blockchain faz com que o eleitor participe de forma direta na auditoria da eleição, tendo assim um sistema mais transparente e menos suscetível às falhas de segurança (Cachin et al. 2017).

O presente artigo está dividido em dez seções, sendo a Seção 1 a Introdução e, posteriormente:

- Seção 2: Objetivos;
- Seção 3: Metodologia utilizada;
- Seção 4: Apresenta características do sistema eleitoral brasileiro e suas controvérsias;
- Seção 5: Expõe definições sobre o que é Blockchain e seu princípio de funcionamento;
- Seção 6: São elucidados os smart contracts;
- Seção 7: Trata do blockchain nas eleições;
- Seção 8: Simulação da aplicação de votação;

- Seção 9: Custos envolvidos;
- Seção 10: Conclusões.

OBJETIVOS

O objetivo deste artigo é apresentar uma abordagem inovadora de sistema de votação eleitoral baseado em blockchain, utilizando a plataforma Ethereum e smart contracts programados em Solidity, além de explorar a aplicação do blockchain na área de votação eleitoral, destacando seus benefícios, como transparência, integridade e redução de custos. Serão analisados os processos de criação de eleitores, candidatos e realização de votos, bem como as considerações sobre os custos envolvidos na implementação de um sistema de votação baseado em blockchain. Espera-se que este artigo contribua para a compreensão das possibilidades e desafios do uso de blockchain em sistemas eleitorais e estimule o debate sobre sua aplicação na modernização de processos eleitorais.

METODOLOGIA

A metodologia utilizada neste artigo consistiu em uma análise exploratória e uma simulação de votação utilizando a plataforma Ethereum e um *smart contract* programado em *Solidity*. A análise exploratória envolveu a revisão da literatura sobre o sistema eleitoral brasileiro, as controvérsias em torno das urnas eletrônicas, o conceito de blockchain e *smart contracts*, e o uso do blockchain nas eleições.

Em seguida, foi realizada a simulação de votação utilizando a plataforma Ethereum, que é uma plataforma de blockchain que permite a criação e execução de contratos inteligentes. Um *smart contract* foi programado em *Solidity*, que é a linguagem de programação utilizada na plataforma Ethereum, para simular o processo de votação. Foram considerados aspectos como a criação de eleitores, candidatos, e a realização de votos, que foram registrados na blockchain.

Após a simulação de votação, foram analisados os resultados obtidos, destacando os benefícios do uso de *blockchain* e *smart contracts* em um sistema distribuído de votação, como a transparência, integridade e redução de custos. Além disso, foram apresentadas considerações sobre os custos envolvidos na implementação de um sistema de votação baseado em blockchain.

É importante destacar que a metodologia utilizada foi uma simulação e não uma implementação real de um sistema de votação utilizando *blockchain* e *smart contracts*. A simulação foi realizada com o objetivo de demonstrar a aplicação dessas tecnologias em um contexto de votação eleitoral e explorar suas possíveis vantagens.

SISTEMA ELEITORAL BRASILEIRO

Eleições seguras são o desejo de eleitores que anseiam exercer seu papel na democracia. Nesse contexto, o sistema eleitoral brasileiro adotou a tecnologia das urnas eletrônicas a fim de ter transparência e integridade dos votos. Apesar de existir algum mecanismo que garanta toda a segurança das eleições, os eleitores não participam de forma direta na auditoria de seus votos, gerando assim

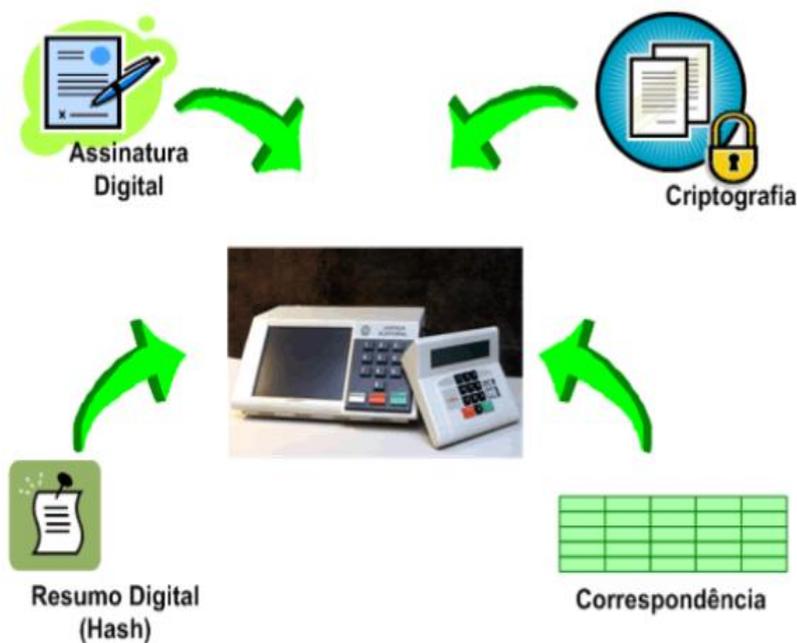
desconfiança referente à manipulações, pois a interação do eleitor se resume a se dirigir até a urna eleitoral e efetuar seu voto. A partir de então, ele aguarda o resultado final. Para qual candidato foram os votos, e como de fato funcionam os processos de segurança das urnas eletrônicas ainda não estão claros para muitos eleitores.

A urna eletrônica foi criada e implantada no Brasil em 1996 e, segundo o Tribunal Superior Eleitoral - TSE (2016), apenas 32% dos eleitores a utilizaram. Com o passar dos anos, ocorreram adaptações e melhorias no intuito de fazer com que todos pudessem exercer seu papel na democracia. Assim, a partir das urnas eletrônicas teríamos um sistema transparente que garantisse a integridade dos votos. Os últimos modelos lançados foram os UE-2011 e UE-2013, já equipados com coletor biométrico e possuem acessibilidade para pessoas com deficiência, por exemplo (TSE, 2013).

Apesar do Tribunal Superior Eleitoral dar garantias que as urnas são seguras, ainda pairam dúvidas sobre esse aspecto, pois, apesar do fato da urna não estar conectada à Internet, não significa que o algoritmo não possa ter sido elaborado ou modificado para contabilizar mais votos para candidatos pré-determinados, ou ainda que possam ocorrer manipulações dos votos durante o processo de totalização destes.

Em relação a segurança das urnas eletrônicas, vemos representada pela Figura 1 o modelo de sistema de segurança atual, que inclui assinaturas digitais, criptografia e resumo digital (*hash*). Entretanto, nenhum desses itens garante que não tenha sofrido manipulações no processo de fabricação

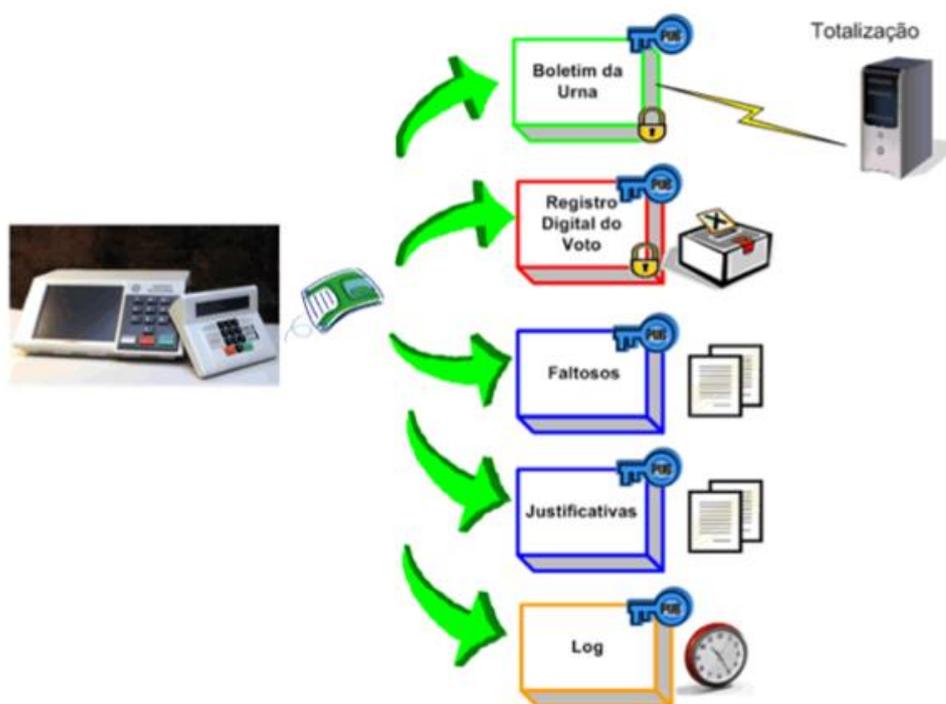
Figura 1 - Segurança do processo das urnas eletrônicas.



Fonte: Tribunal Superior Eleitoral (2012). Recuperado de <http://www.justicaeleitoral.jus.br/arquivos/tse-seguranca-do-processo-eletronico-de-votacao>.

Todos os processos contêm assinatura digital e são criptografados até chegar na fase de envio para totalização, onde é realizada uma auditoria para saber o resultado final, como mostra a Figura 2. Todos os Tribunais Regionais Eleitorais (TRE) fazem a soma de todos os votos válidos a partir dos Boletim de Urna (BU), sendo que os eleitores aguardam pela apuração de todos os votos. Apesar das urnas não estarem conectadas à Internet, os TREs trabalham com servidores e precisam expor os resultados finais através de rede de computadores, o que constitui na real possibilidade da ação maliciosa dos chamados *crackers*, os quais fazem ataques e invasões e colaboram com a falta de credibilidade na segurança da informação (Melo, 2016).

Figura 2 - Produtos gerados pelas urnas.



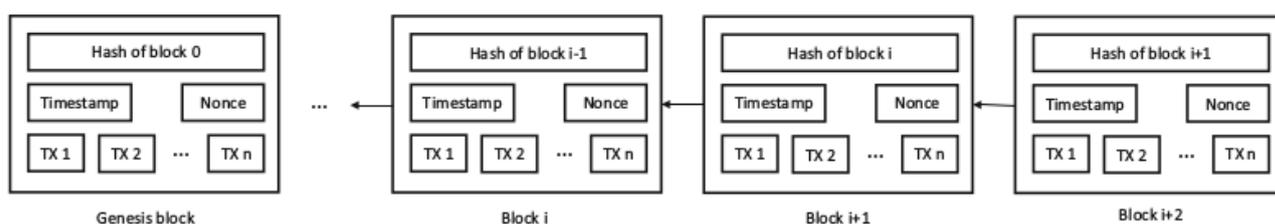
Fonte: Tribunal Superior Eleitoral, 2012 Recuperado de <http://www.justicaeleitoral.jus.br/arquivos/tse-produtos-gerados-pela-urna-eletronica>.

A totalização ocorre no mesmo dia das eleições, os resultados finais são exibidos pelas principais mídias, e assim se encerra o processo eleitoral no Brasil, onde o único momento em que o eleitor participa é na votação, e não na auditoria dos processos em que seus votos estão envolvidos. No sentido de estabelecer uma eleição mais transparente e ágil, onde todos os votos têm sua integridade garantida, podemos utilizar a tecnologia *Blockchain*, que tem inovado diversos segmentos, desde transações financeiras até Certificação de cumprimento de cláusulas de contrato (Pires, 2016).

Blockchain pode ser a solução para transações feitas eletronicamente sem que precise de um intermediário para que seja validada e, segundo Mougayar (2017), o Blockchain possui mais três definições, as quais são:

1. Técnica: base de dados de back-end que mantém um registro distribuído abertamente;
2. Corporativa: rede de trocas para valores em movimentos em partes;
3. Legal: um mecanismo de validação de transações que não requer apoios intermediários.

Figura 3: Representação do Blockchain.



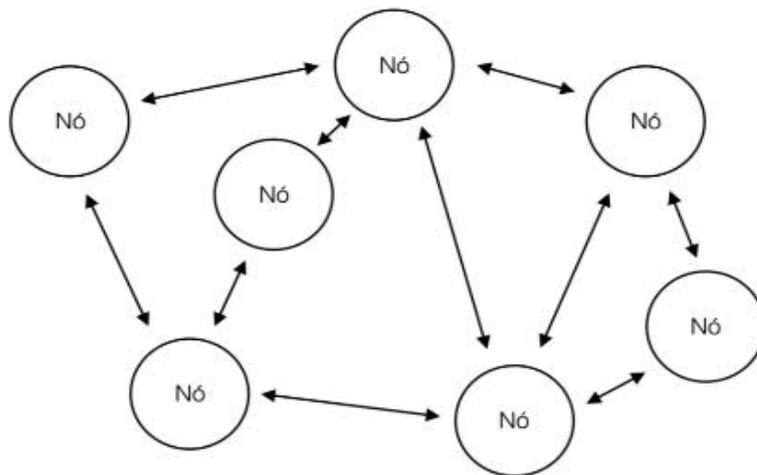
Fonte: Nofer, Gomber, Hinz, e Schiereck, 2017.

A Figura 3 é um exemplo de como funciona o Blockchain. Segundo Nofer, Gomber, Hinz, e Schiereck (2017), o primeiro bloco criado é o Gênesis, que contém informações de todos os blocos e até mesmo regras de como o sistema irá se desenvolver. Cada bloco contém múltiplas transações (TX1-n), assinatura digital, hash (do próprio bloco) e a hash do bloco anterior, timestamp; que é a hora que o bloco foi criado e o nonce, que é um número aleatório gerado para verificação da hash.

A cada bloco criado, todos os participantes da rede fazem parte da auditoria para validar os dados contidos naquele bloco. A rede funciona com o chamado consenso, de que se ao menos 51% entender como válido as informações contidas naquele bloco, ele será registrado na rede (Divino, 2018). Cada participante da rede tem suas chaves criptografadas, sendo elas públicas e privadas, que segundo Messer (2017) são elas que são responsáveis pela segurança das informações de seus usuários, pois a chave pública se encarrega de mostrar informações das transações e as chaves privadas são as que garante o sigilo de quem fez as transações.

Em suma, o Blockchain tem seu funcionamento em uma rede peer-to-peer (P2P) que, de acordo com Pires (2016), são redes descentralizadas em que cada máquina, chamada de nó, faz o papel de cliente-servidor ao mesmo tempo. Neste sentido, por ser uma rede descentralizada, todas transações feitas estarão disponíveis, pois não conta com um servidor único e sim de um todo, para que o sistema continue funcionando como, mostra a Figura 4:

Figura 4 - Arquitetura de rede P2P.



Fonte: Pires, 2016.

Apesar de ter seu início com as criptomoedas, mais especificamente a bitcoin, a tecnologia Blockchain pode ser utilizada para diversas aplicações, que segundo Nofer, Gomber, Hinz, e Schiereck (2017) podem ser, dentre outras:

1. Seguro: bens como, por exemplo, imóveis, automóveis, dentre outros, podem ser registrados usando a tecnologia Blockchain. As seguradoras podem verificar o histórico de transações.
2. Notário público: autorização central por notário não é mais necessária.
3. Armazenando e validando a assinatura e timestamp de um documento usando Blockchain: compartilhamento de documentos sem a necessidade de um terceiro, utilizando uma plataforma de armazenamento em nuvem distribuída peer-to-peer.
4. Aplicações da Internet: em vez de governos e corporações, os Servidores de Nomes de Domínio (DNS) são controlados por todos os usuários de maneira descentralizada.

Além disso, Vilela e Coutinho (2018) relatam que praticamente qualquer tipo de negócio jurídico que envolva uma condição para execução, seguida de transação de valores ou propriedades - sejam elas contratos de seguros, sistemas de governança coletiva, fundos de investimentos, bolsas de valores entre outros - pode ser otimizado com o desenvolvimento de uma aplicação baseada em *Blockchain*. É notável que a utilização desta tecnologia é rica de tantos benefícios (Juliandson et al, 2017), além do Blockchain ser confiável, ele pode fazer uso dos chamados *smart contracts*, que são contratos inteligentes, similares aos de papel, mas funciona com autonomia.

SMART CONTRACTS

De acordo com Divino (2018), define-se *smart contracts*, ou contratos inteligentes, um algoritmo armazenado e executado no *Blockchain*, que é gerido de maneira autônoma e automática, sem a interferência de terceiros. Hoje em dia, os *smart contracts* possuem aplicações em diversos mercados, criando um mundo de possibilidades (Mougayar, 2017), empoderando empresários, cientistas e técnicos das mais diversas áreas, por trazer benefícios como a comodidade e praticidade (Divino, 2018). Um exemplo é a implementação através da plataforma *Ethereum*, em que é possível realizar várias aplicações, como apólices de seguro, registro de títulos de propriedades, até uma transferência bancária.

Os *smarts contracts* podem ser definidos como uma representação de um acordo em que se verifica o cumprimento com as condições que foram estabelecidas anteriormente (Gonçalves e Camargos, 2018). São linhas de códigos, algoritmos, que seguem uma lógica em que o contrato será regido, de tal maneira que se faz cumprir por si só, sendo assim um sistema autoexecutável. Podemos utilizar o exemplo dado pelo idealizador do *smart contracts*, da máquina de refrigerante, que seria um modelo de *smart contracts* primitivo. Na máquina em questão temos uma variedade de produtos e o contrato nela contida é simples: se inserido o valor programado, então a posse do refrigerante será transferida. Podemos ver que o contrato da máquina é autoexecutável, o que interessa somente ao cumprimento de suas exigências (Szabo, 1997).

Enquanto o *Blockchain* de uma moeda digital fornece uma plataforma para armazenamento descentralizado, o de um contrato inteligente fornece uma plataforma para computação descentralizada (Pires, 2016). O autor ainda sugere que, no sentido de administração pública, os *smarts contracts* podem ser utilizados para prover transparência em:

Certificação de cumprimento de cláusulas de contrato: uma grande dificuldade na gestão dos recursos públicos é a garantia do cumprimento dos contratos de licitações feitas entre governo e empresas. A utilização de contratos inteligentes em conjunto com uma solução de Internet das Coisas (IoT) permitiria que o pagamento por um determinado produto fosse feito a partir do resultado de sensores de estoque com tecnologia Radio-Frequency Identification (RFID), ou de uma balança digital.

Registro de ponto eletrônico de servidores públicos: a tecnologia de contratos inteligentes pode ser utilizada para registrar e tornar público os horários de trabalho de deputados e demais servidores públicos. Além disso, o pagamento de salários pode ser realizado automaticamente a partir dos registros de horas trabalhadas.

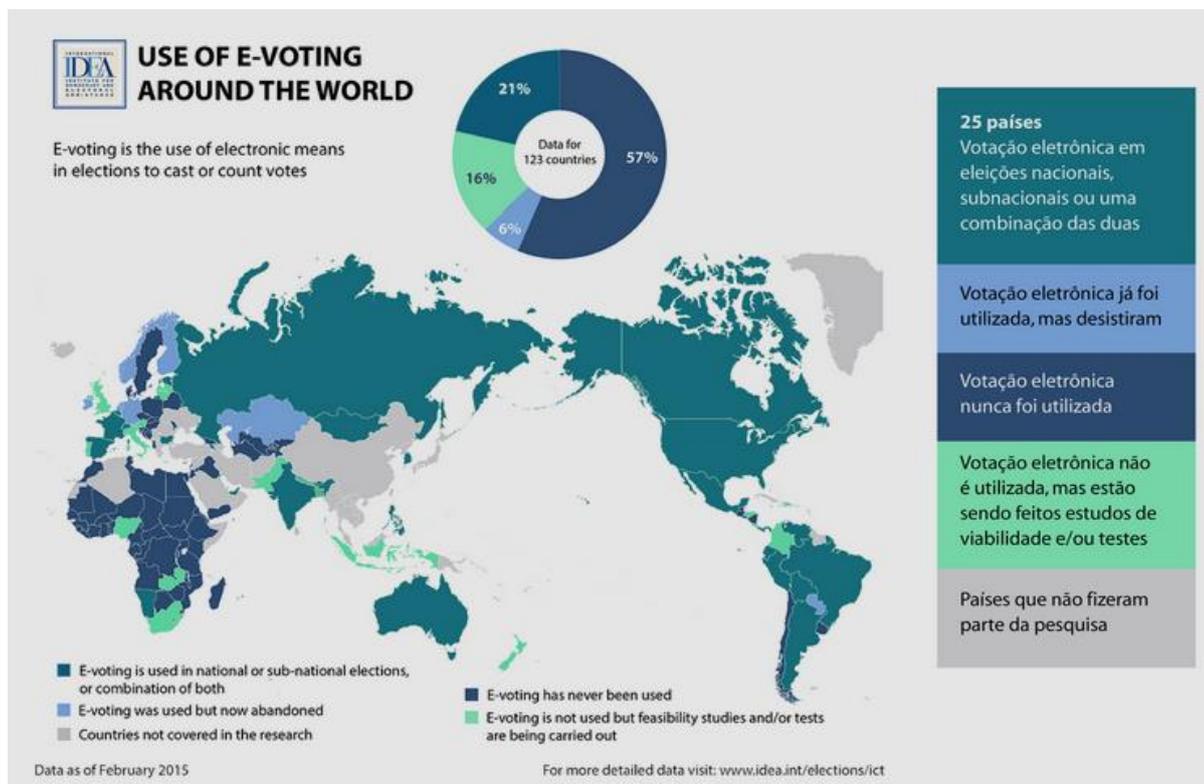
São inúmeras aplicações que podem utilizar essa tecnologia, tanto no âmbito público quanto privado. No âmbito público, a utilização do *Blockchain*

regido por *smart contracts* pode ser utilizado para substituição das urnas eletrônicas.

BLOCKCHAIN NAS ELEIÇÕES

Segundo o Institute for *Democracy and Electoral Assistance* (IDEA, 2015), o uso de tecnologias em processos eleitorais, já estão presentes em 25 países, como demonstra a Figura 5:

Figura 5 - Uso de sistemas eletrônicos de eleições ao redor do mundo (2015).



Fonte: Democracy and Electoral Assistance (IDEA). Adaptado por TSE. Recuperado de <https://www.idea.int/news-media/media/use-e-voting-around-world>.

Atualmente, a utilização do Blockchain como ferramenta de votação vem crescendo, além de se expandir em outros ramos do mercado. Muitas startups vêm desenvolvendo projetos a fim de implementar tal tecnologia em empresas para votações internas; alguns exemplos dessas startups são: FollowMyVote, Polys e Agora. Como já descrito nas seções anteriores, a transparência e segurança são as principais características que levaram diversos estudos a cogitar a utilização de tal tecnologia nos sistemas eleitorais governamentais.

A votação através da Internet é um grande passo para a democracia, pois na comodidade de casa cada eleitor pode registrar e auditar seu voto. A Estônia em 2015, antes mesmo do Blockchain, foi o primeiro país a realizar votação via internet, com o i-Voting (2005). Porém, após sofrer ataques cibernéticos, a rede e-Estonia passou a utilizar a KSI Blockchain para garantir todas as informações

governamentais (e-Estonia, i-Voting. Disponível em: <<https://e-estonia.com/solutions/e-governance/i-voting/>> Acesso em 23 de abril de 2019).

Contudo, os benefícios de aderir à tecnologia Blockchain para criação de um sistema de votação são muitos. Na implementação de Blockchain em um sistema de votação via internet, Curran (2018) diz que não podem faltar os requisitos:

Verificabilidade pública: todos os envolvidos podem ver o processo de votação (registrado no Blockchain) e verificar o resultado da eleição.

Verificabilidade individual: todos os eleitores podem verificar se sua cédula foi registrada na contagem final.

Confiabilidade e Consistência: o Blockchain deve ser não atacável e aceitar o mesmo resultado da eleição.

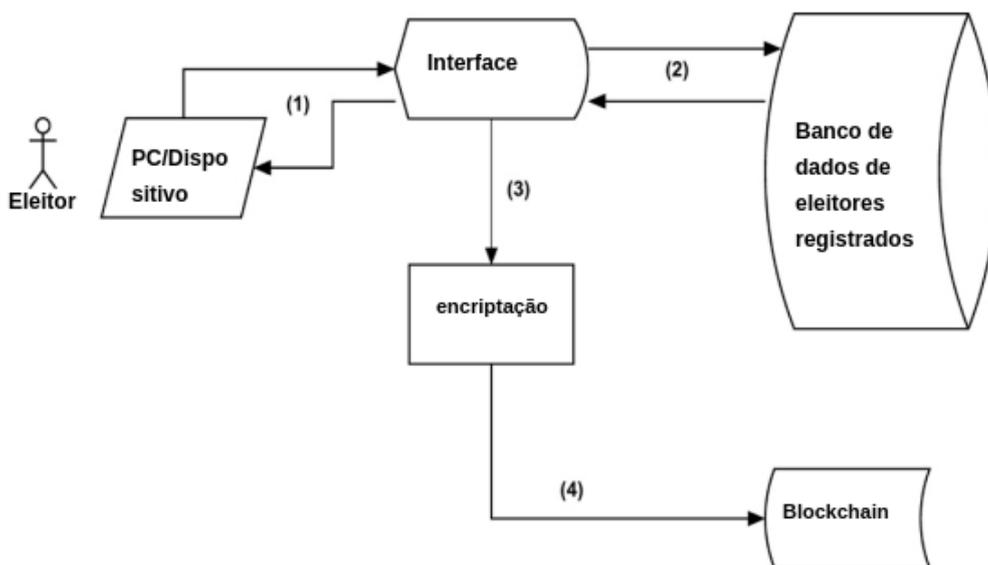
Auditoria: o processo de votação no Blockchain é auditável após a eleição pelo público ou por terceiros.

Anonimato: todas as cédulas não têm conexão com seus eleitores (mas cada eleitor pode confirmar seu voto).

Transparência: a transparência Blockchain garante que o procedimento esteja aberto ao escrutínio público.

Para entendermos como seria a estrutura dos processos desse sistema de votação, temos um exemplo de uma aplicação de votação utilizando blockchain na Figura 6:

Figura 6 - Representação simplificada de um i-Voting System.



Fonte: Adaptado de Ayed (2017).

Na aplicação de votação de Ayed (2017), via Blockchain segue as etapas abaixo:

1. Solicitando a votação: O usuário terá que fazer o login no sistema de votação usando suas credenciais;
2. Votar: Os eleitores terão que escolher entre votar em um dos candidatos ou votar em protesto, a transmissão da votação será feita por meio de uma interface de usuário amigável;
3. Criptografar votos: Após o usuário dar o seu voto, o sistema irá gerar uma entrada que contém o número de identificação do eleitor seguido do nome completo do eleitor, bem como o hash da votação anterior;
4. Adicionando o voto ao blockchain: Depois que um bloco é criado, e dependendo do candidato selecionado, a informação é registrada no Blockchain correspondente. Cada bloco é vinculado ao voto anterior.

A garantia da confidencialidade, integridade e disponibilidade dos sistemas de eleição baseados em *blockchain*, que são pilares importantes da segurança da informação, tem sido objeto de estudo em várias pesquisas científicas. Tsai e Lu (2019) propuseram um sistema de voto eletrônico seguro baseado em blockchain, que utiliza criptografia avançada e algoritmos de consenso para garantir a confidencialidade dos dados eleitorais. Kshetri (2017) e Fernández-Caramés e Fraga-Lamas (2018) também destacam a integração potencial entre *blockchain* e Internet das Coisas (IoT) como uma medida de segurança adicional para sistemas eleitorais.

O funcionamento do *blockchain*, sua arquitetura descentralizada e a criptografia avançada utilizada têm sido estudados para garantir a integridade dos dados eleitorais. Zohar (2015) e Narayanan et al. (2016) fornecem uma visão detalhada sobre o funcionamento interno do *blockchain* e suas características de segurança. Além disso, medidas de segurança, como algoritmos de consenso e chaves criptográficas, são amplamente discutidas por Swan (2015).

No entanto, é importante observar que os sistemas de *blockchain* também enfrentam desafios de segurança, como ataques de hackers. Episódios recentes de ataques por hackers em sistemas de *blockchain* têm causado prejuízos financeiros consideráveis. Portanto, a implementação de medidas adicionais de segurança, como monitoramento constante, auditorias de segurança e atualizações regulares, é essencial para garantir a disponibilidade e a proteção contra ameaças cibernéticas.

A maneira que o sistema irá funcionar seria de fácil manuseio ao eleitor e contaria com processos simples e extremamente seguros. Com os avanços tecnológicos, a implementação de tal sistema nas eleições seria um grande passo para democracia assim como foram as urnas eletrônicas em nosso país.

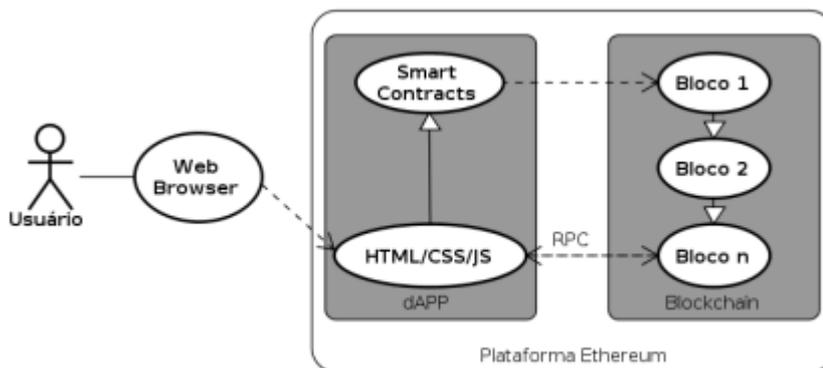
APLICAÇÃO

Como aplicação iremos utilizar a plataforma *Ethereum* que, diferente da *Bitcoin*, permite estender o *Blockchain* para diversas aplicações, não apenas para transações financeiras, através dos contratos inteligentes. A linguagem de programação dos *smarts contracts* na plataforma *Ethereum* é a *Solidity*, sua criptomoeda é chamada *Ether* e possui dois tipos de contas (Mccorry, Shahandashti e Hao, 2017): uma conta de propriedade externa, que é um par de

chaves pública-privada controlada pelo usuário, e uma conta de contrato, que é um *smart contract* que é controlado por seu código.

Para representação de uma aplicação distribuída na plataforma Ethereum temos a Figura 7:

Figura 7 - Plataforma *Ethereum*.



Fonte: adaptado de *Ethereum* (2016).

Como podemos ver, o usuário acessa a aplicação através de um navegador web (*web browser*) onde tem a sua interface gráfica programada em HTML/CSS/JavaScript. Nossa aplicação segue essa mesma linha. Neste trabalho iremos executar o sistema de votação em uma rede local, para fazermos uma representação de como seria uma votação com a tecnologia *Blockchain*.

Inicialmente, utilizaremos o *Ganache CLI* é uma ferramenta que simula uma *blockchain Ethereum* local para o desenvolvimento e teste de aplicativos descentralizados. Ao iniciá-lo, são geradas 10 contas de teste, conforme mostra na figura 8, cada uma com um endereço *Ethereum* único e uma chave privada associada. Essas contas são usadas para simular usuários e suas interações com a *blockchain* local. As contas possuem saldos iniciais de *Ether* para permitir transações durante o desenvolvimento. As chaves privadas são usadas para autorizar operações nas contas. O *Ganache CLI* fornece um ambiente seguro e isolado para testar contratos inteligentes, sem a necessidade de interagir com a rede *Ethereum* principal.

Figura 8 - Inicializando o Ganache.

```
Ganache CLI v6.1.8 (ganache-core: 2.2.1)

Available Accounts
=====
(0) 0x96c523f6df13e528941e09ce421addc9c859c767 (~100 ETH)
(1) 0x521621038789c464a8a4bc389f7a412ecbf82a25 (~100 ETH)
(2) 0x41c5147566a1115a3d0dc05b011e515d17bd5e36 (~100 ETH)
(3) 0xfa579515e4b95f822882ed64f95f1e46a019130e (~100 ETH)
(4) 0x3b954a84931b62d642de95dd5667607c47209792 (~100 ETH)
(5) 0x5272a1d9bde2d38344b35d83b2eb3ef13c25cfdb (~100 ETH)
(6) 0x139e3c936a7d017a29465f2e6891381d43bf71c8 (~100 ETH)
(7) 0xcdeb764fb593e17f99364d33339356e6ac534fcb (~100 ETH)
(8) 0x0370612a431dd655529497b1d3fc1a2b95b77d34 (~100 ETH)
(9) 0x52385519ecaede7161fe3911e45c5e86bf0fc933 (~100 ETH)

Private Keys
=====
(0) 0x14cb79755d85527e363ac834107e70bc1fca87dbd7cf184856438e9b06e0b262
(1) 0x1998c6ee09633d3da726b3d0bb4e5e3e25c2227008f8702fa0a168cfad80920d
(2) 0xef93c8921b7f2577d4bec6677bec8ee6e9d0fbd8eb3bfc4b45d732cdb6ddb444
(3) 0x394ec165ed9ad846b01caa05463bf92ef9640d34292a1bcc92ebba350cb8d373
(4) 0x4df05b2fe77505f427bb21e58c4251ac623d409f6bad54552617ce09871e6c8d
(5) 0xd6a4de275936616b07206c66ee36fbc043b4dc1ce268bd275281bc5391fc8031
(6) 0xc678c57b56565f0d14fed27c11b3c4e6ddb16a2d34318a41bf64de0a4df192b7
(7) 0x170b64b6ec50c8a8bb1b812336d754ae8861ba884887f34556ede9a8d8a15a39
(8) 0x67163e283792ec04fa8c1b2d4fa43744a771d4d67792bbfe105dea69dfb87aea
(9) 0x1b27a82958f6ee4b08f5603214a57fba20464e13e968c6ca0cf6507a0aee34e0
```

Fonte: Elaborado pelos autores.

A figura 8 mostra os seguintes elementos: *Available Accounts* que são 10 contas geradas pelo *Ganache CLI* para simular usuários na *blockchain* local. Cada conta possui um endereço *Ethereum* único e é representada na imagem pelos endereços listados. Saldo Inicial de Ether: Cada conta de teste possui um saldo inicial de *Ether*, que é exibido ao lado de cada endereço. Esse saldo permite que as contas realizem transações durante o desenvolvimento e teste dos aplicativos, *Private Keys*: Para cada conta de teste, o *Ganache CLI* gera uma chave privada exclusiva. As chaves privadas são exibidas na imagem, fornecendo acesso e autorização para operações específicas em cada conta.

Após a inicialização do *Ganache*, utilizaremos um interpretador de *JavaScript*, popular para aplicações *backend*, o *NodeJS*. Ele fará a execução do *web3.js*, que é uma coleção de bibliotecas que permitem interagir com um nó na plataforma *Ethereum*, seja local ou remoto. O *NodeJS* será responsável pela interação entre o *Ganache* e nossa aplicação. Após a interação com o *Ganache*, começamos a criar nossa aplicação a partir do *NodeJS*. Nesta etapa, iremos importar o *smart contract*, que foi programado na linguagem *Solidity* e recebeu o nome de “Eleicao”, como consta na Figura 9:

Figura 9 - Smart contract programado em Solidity.

```

1  pragma solidity ^0.4.18;
2
3  contract Eleicao {
4
5      mapping (bytes32 => uint8)
6
7      public votosRecebidos;
8
9      bytes32[] public candidatos;
10
11     constructor(bytes32[] nomes) public {
12         candidatos = nomes;
13     }
14
15     function listarVotosPara(bytes32 candidato) view public returns (uint8) {
16         require(validarCandidato(candidato));
17         return votosRecebidos[candidato];
18     }
19
20     function votarNoCandidato(bytes32 candidato) public {
21         require(validarCandidato(candidato));
22         votosRecebidos[candidato]++;
23     }
24
25     function validarCandidato(bytes32 candidato) view public returns (bool) {
26         for(uint i = 0; i < candidatos.length; i++)
27             if (candidatos[i] == candidato) return true;
28         return false;
29     }
30
31 }

```

Fonte: Elaborado pelos autores.

Faremos a implementação do *smart contract* no nosso bloco gênese. Neste sentido, o *smart contract* fará com que nossa aplicação se torne um sistema de votação distribuído, pois nele estão contidas as regras definidas em nosso *smart contract*. Iremos simular a votação de um segundo turno presidencial. Na Figura 10 vemos que o bloco gênese foi criado no *Ganache*.

Figura 10: Criação do bloco gênese.

```

=====
2000000000

Gas Limit
=====
6721975

Listening on 127.0.0.1:8545
eth_accounts
eth_sendTransaction

Transaction: 0x357f4f5642264fb28e851210b8fc06684e59f0b52fe3ac0b4583c3cc59e27e2
4
Contract created: 0x2403f95dc90492db7c27511ab1c85c5b8144ecdb
Gas usage: 347852
Block Number: 1
Block Time: Wed Apr 10 2019 14:38:37 GMT-0300 (-03)

eth_newBlockFilter
eth_getFilterChanges
eth_getTransactionReceipt
eth_getCode
eth_uninstallFilter

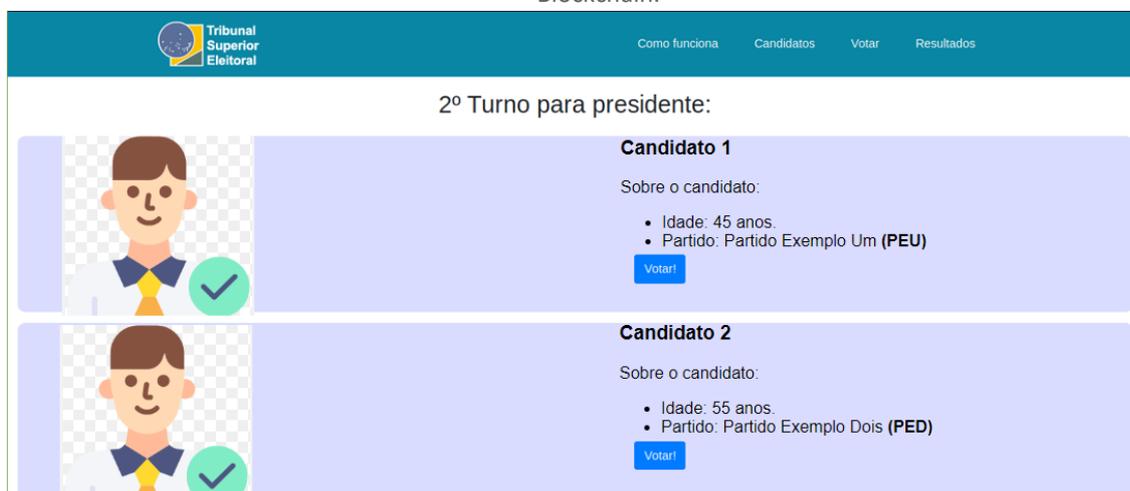
```

Fonte: Elaborado pelos autores.

Para realizar o teste de votação, criamos uma página em HTML/CCS/JavaScript para que possamos efetuar a simulação do segundo turno

presidencial do Brasil de 2018 com candidatos fictícios. Como podemos observar na Figura 11, o site tem um visual limpo e apresenta informações relevantes dos candidatos, semelhantes às informações contidas nas urnas eletrônicas.

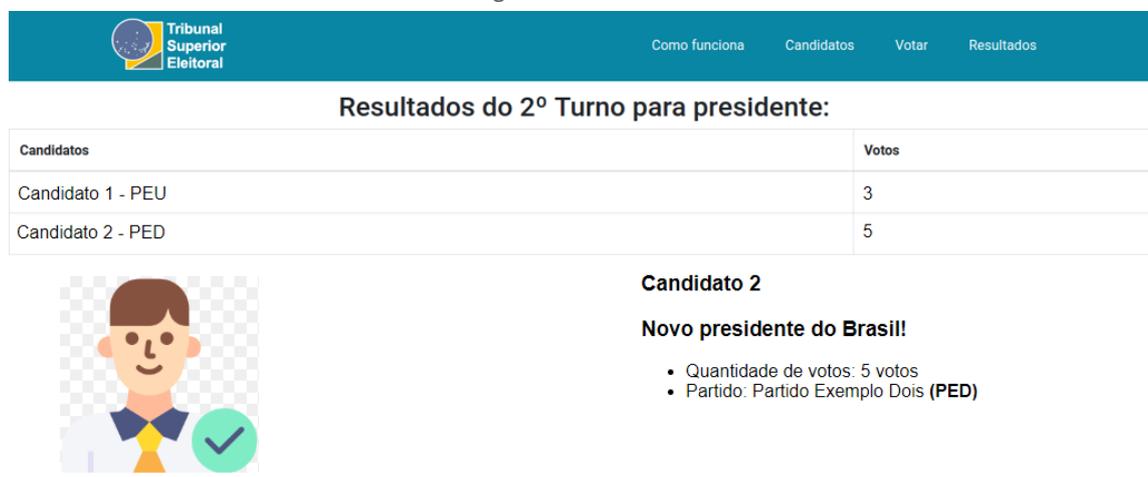
Figura 11: Site de simulação do 2º turno presidencial do Brasil em 2018 utilizando Blockchain.



Fonte: Elaborado pelos autores.

A votação é efetuada de forma simples, sem complexidade e, para nossa simulação, efetuamos 8 votos. A Figura 12 mostra os respectivos resultados e o candidato eleito:

Figura 12: Resultado do 2º Turno.



Fonte: Elaborado pelos autores.

Com o resultado da votação finalizada, veremos o que aconteceu em nosso simulador de *blockchain*, Ganache. Como cada voto feito é um novo bloco criado, temos que ter essa quantidade de blocos em nosso *blockchain*. O resultado da soma são 8 votos, sendo 5 deles para o Candidato 2 e 3 votos do Candidato 1, ou seja, o nosso simulador de *blockchain* vai conter 9 blocos, pois é a soma dos votos efetuados mais o bloco gênese, conforme a Figura 13:

Figura 13: Os novos blocos criados.

```
eth_sendTransaction
Transaction: 0xf7567e8e99fe626337fb5df996d046a8a5548ab518d7c945bb6cd202d6f8efc
Gas usage: 29447
Block Number: 8
Block Time: Mon Apr 22 2019 23:31:56 GMT-0300 (-03)

eth_call
eth_accounts
eth_sendTransaction
Transaction: 0xc146de756d96cef6e87082305e06591041a0988e416368990f5d0c2f6d63c6f0
Gas usage: 29447
Block Number: 9
Block Time: Mon Apr 22 2019 23:32:02 GMT-0300 (-03)

eth_call
eth_call
eth_call
eth_call
eth_call
```

Fonte: Elaborado pelos autores.

Para tratamento dos votos, foi criado um arquivo chamado Eleicao.js. Ele tem a responsabilidade de garantir a atribuição correta dos votos dos eleitores aos respectivos candidatos, além de fornecer mecanismos para a contagem precisa desses votos.

Ao lidar com a atribuição e contagem dos votos, o Eleicao.js desempenha um papel crucial para a integridade e transparência do processo eleitoral. Ele utiliza a biblioteca Web3.js para estabelecer a comunicação com a rede *Ethereum* e interagir com os contratos inteligentes relacionados à eleição. A Figura 14 a seguir mostra o código contido no arquivo Eleicao.js:

Figura 14: Arquivo Eleicao.js.

```
Eleicao.js
1 web3 = new Web3();
2
3 var abi :[[outputs: any[] constant: bo... = [{
4   "constant": true,
5   "inputs": [],
6   "name": "constructor",
7   "outputs": [],
8   "payable": false,
9   "stateMutability": "nonpayable",
10  "type": "function"
11  }]];
12
13 var Contrato = web3.eth.contract(abi);
14
15 var copiaDoContratoSubmetido = Contrato.at( index: '0xbe5b98217aba551ee42ff07213aecdf67d0849fa2');
16
17 usage
18 function votarNoCandidato(candidato) :void {
19   try {
20     copiaDoContratoSubmetido.votarNoCandidato(candidato, {from: web3.eth.accounts[0]}, function() :void {
21       $("#" + candidato).html(copiaDoContratoSubmetido.listarVotosPara.call(candidato).toString());
22       alert("Você votou no candidato: " + candidato);
23     });
24   } catch (err) {
25     alert(err.toString());
26   }
27 }
28
29 $(document).ready(function() :void {
30   $("button.votar").click(function() :void {
31     var candidatoSelecionado = $(this).data("candidato");
32     votarNoCandidato(candidatoSelecionado);
33   });
34 });
```

Fonte: Elaborado pelos autores.

Nesse sistema, os eleitores podem selecionar um candidato clicando no respectivo botão "Votar". Ao clicar no botão, a função `votarNoCandidato()` é acionada, registrando o voto no contrato inteligente correspondente. O código atualiza a contagem de votos do candidato selecionado na página, fornecendo um feedback imediato ao eleitor. Dessa forma, o arquivo `Eleicao.js` oferece uma solução transparente e segura para a designação dos votos dos eleitores em um sistema de votação baseado em Ethereum, garantindo a integridade do processo eleitoral.

A votação feita a partir deste site nos mostra que é possível uma implantação de *blockchain* nas eleições. A criação desta aplicação poderia revolucionar o modo de que participamos da democracia, pois todos os eleitores poderiam votar e auditar as eleições na comodidade de casa, bastando ter um dispositivo com acesso à internet, seja ele computador, um tablet ou smartphone.

CUSTOS

A transformação da máquina de votar no Brasil acompanha o Código Eleitoral de 1932, o qual defende a redução de custos em comparação com o primeiro sistema adotado, os quais exigiam material gráfico e mão de obra para operacionalização. Entretanto, a forma que foi usada para acompanhar tal diminuição, levou em consideração apenas a possibilidade de diluição dos gastos do uso da urna em várias eleições (TSE, 2011), excluindo a dificuldade de deslocamento de regiões remotas, cujos custos não são levados em consideração, além da necessidade de descarte do equipamento eletrônico.

Dentre as diretrizes do uso das urnas eletrônicas, uma delas aponta que as urnas eletrônicas são de fácil transporte, por ser leve e pequena, porém, no item de "Gestão Patrimonial" do site do TSE observa-se a relação de materiais utilizados no processo, como veículos, sendo a maioria de grande porte, e a condição de uso descrita como: "em uso, recuperável e irrecuperável", sem apontar valores ou outras análises que reforcem a viabilidade e o impacto, tanto financeiro, quanto ambiental. Além disso, ainda segundo o próprio TSE, a Justiça Eleitoral tem cerca de 500 mil urnas eletrônicas que são utilizadas em todo Brasil, sendo o valor monetário demonstrado na Tabela 1 para 21.616 urnas, na relação de bens patrimoniais de 2018, além de contarem com 15% a mais de urnas para as zonas de contingência. Outra questão que apresenta desvantagem na utilização da urna eletrônica é a necessidade de depósitos nos 26 estados para armazená-las, acarretando gastos inerentes a esses locais, como manutenção, preparação para proteger de inundações, climatização, disposição de um espaço de 2.580 metros quadrados e um pé direito superior a 5 metros (TSE, 2018).

Tabela 1: Balanço quantitativo dos bens patrimoniais do Tribunal Superior Eleitoral, com foco na urna eletrônica.



TRIBUNAL SUPERIOR ELEITORAL - TSE
SECRETARIA DE ADMINISTRAÇÃO - SA
COORDENADORIA DE MATERIAL E PATRIMÔNIO - COMAP
SEÇÃO DE GESTÃO DE PATRIMÔNIO - SEPAT

Relatório Quantitativo (Conta Contábil)

03/07/2018 15:54:15

Órgão: 001 - TRIBUNAL SUPERIOR ELEITORAL
U.G.: 070001 - SECRETARIA DE ADMINISTRAÇÃO - TSE

Material	Qtd.	VL. Aquisição (R\$)	VL. Líquido (R\$)
Conta Contábil: 123110201 - EQUIPAMENTOS DE PROCESSAMENTO DE DADOS			
SCANNER DE MICROFILME	1	39.000,00	3.900,00
SCANNER DE PRODUÇÃO	9	166.818,79	23.863,90
SERVIDOR DE DADOS	80	2.262.072,11	545.003,44
SERVIDOR DE REDE - SOLUÇÃO DE ACELERAÇÃO PARA CLIENTES MÓVEIS	1	490.000,00	56.350,00
SERVIDOR DELL 2950	1	15.003,36	1.500,34
SERVIDOR GERADOR DE CARACTERES	2	9.167,00	916,70
SERVIDOR REDE -- ACELERAÇÃO/OPTIMIZAÇÃO DE TRÁFEGO PARA A REDE	2	1.380.000,00	293.250,00
SERVIDOR SUN SERVER X4-2	2	277.286,00	85.958,66
SISTEMA DE ARMAZENAMENTO	5	429.682,42	42.968,25
STORAGE AREA NETWORK - SAN (HARDWARE)	4	8.673.574,81	4.363.933,63
SUPORTE PARA MONTAGEM DE MONITOR EM RACK	1	885,35	825,59
SWITCH CAMADA 7	4	1.260.000,00	126.000,00
SWITCH CENTRAL	2	797.163,96	79.716,40
SWITCH COMUNICAÇÃO DE DADOS	5	22.515,00	17.314,01
SWITCH DE ACESSO	42	3.932.841,15	393.284,11
SWITCH DE REDE	16	3.861,96	1.915,78
SWITCH EXADATA DATABASE X2-2	2	90.351,56	28.008,94
SWITCH PARA CONSOLE	2	181,34	18,14
SWITCH PARA SAN (FIBRA ÓTICA)	3	500.014,38	204.904,36
SWITCH SUN 10GB ETHERNET	2	266.151,12	82.506,90
SWITCH TOPO DE RACK	4	568.365,92	56.836,60
TAPE LIBRARY	1	409.821,86	40.982,19
TECLADO COM CONEXÃO USB	69	2.637,57	263,86
TECLADO PARA MICROCOMPUTADOR	2.567	126.934,70	66.428,63
TERMINAL DO ELEITOR	2	116,68	11,66
TESTADOR DE FIBRA ÓTICA	1	556,50	556,50
TRILHO PARA RACK	1	1.926,40	1.666,30
UNIDADE DE ARMAZENAMENTO VIRTUAL (BIBLIOTECA)	1	818.400,00	81.840,00
UNIDADE DE DISCO RIGIDO	14	2.274.819,95	976.516,00
UNIDADE DE GRAVAÇÃO E REPRODUÇÃO DE ÁUDIO DO TIPO PENDRIVE	1	60,00	58,20
UNIDADE DE SEGURANÇA PARA REDE DE COMPUTADOR	2	277.551,75	27.755,18
UNIDADE DRIVE DE DISQUETE USB DE 3/4	1	100,00	97,00
UNIDADE /DRIVE GRAVADORA E LEITORA DE DVD-ROM	2	114,86	11,48
UNIDADE EXTERNA CAPTURA SINAL TV	2	1.150,56	115,06
URNA ELETRÔNICA	21.616	19.293.750,10	2.658.584,06
URNA ELETRÔNICA (MODELO DE ENGENHARIA)	1	647,09	64,71
Total da Conta Contábil:	49.149	83.195.739,75	26.656.916,27

Fonte: Relatório Quantitativo - Tribunal Superior Eleitoral, 2018.

Contrastando com o valor apresentado acima, em estudo semelhante a esse, McCorry, Shahandashti e Hao (2017) fizeram a primeira implementação de um sistema descentralizado e forneceram uma análise financeira dos custos (em dólares) de execução que não dependem de autoridades confiáveis para calcular os registros e manter a privacidade do eleitor. Os autores fizeram uma simulação na rede oficial Ethereum com 40 eleitores e 1 administrador e, estimaram o custo computacional e financeiro de cada eleitor, chegando no valor total de US\$ 31.98, representando US\$ 0.73 (por eleitor), sendo considerado razoável, já que o OpenVote apresenta máxima privacidade e é publicamente verificável, funcionando como a computação de consenso. Além de apresentar o custo e a segurança como variáveis no sucesso da implementação desse novo sistema de votação, a melhora da imagem corporativa também está atrelada a todos esses benefícios, uma vez que acompanha a modernização e a necessidade dos cidadãos se sentirem mais seguros devido a imutabilidade do voto. Vale ressaltar outra vantagem importante, que é a da geração de empregos para as futuras gerações que se dispuserem a continuar cuidando não só da atualização do sistema de votação, como também de estudos e planos de gestão dos resíduos, tema pouco

abordado na literatura, como analisado na Tabela 2, mas que dentro dessa vertente engloba questões socioeconômicas, empresariais e ambientais.

Tabela 2: Levantamento dos artigos relacionados à gestão dos resíduos no processo eleitoral.

Trabalho	Autor	Ano
Responsabilidade civil do candidato frente ao dano causado pela campanha eleitoral	Santos	2015
Processo eleitoral brasileiro: Impactos ambientais, e o direito ao meio ambiente ecologicamente equilibrados.	Bedran	2013
Diagnóstico e proposta de modelo de gestão dos resíduos eletrônicos gerados nos ministérios do governo brasileiros.	Freitas	2010

Fonte: Os Autores, 2019.

CONCLUSÕES

Com o passar dos anos, é evidente que os recursos tecnológicos vêm evoluindo de forma constante e inovadora. O grande impacto das criptomoedas, obteve uma notoriedade no ramo financeiro, a Bitcoin mostrou seu potencial não somente nas suas transações financeiras e sim na tecnologia por trás dela.

As tecnologias Blockchain e Smart Contracts vem revolucionando a maneira que podemos validar dados via internet a partir de uma grande rede de computadores sem ao menos ter um terceiro para remediar a transação que está sendo feita (Divino, 2018).

Neste sentido, podemos olhar para um futuro em que muitas de nossas necessidades, sejam elas validações de apólices, contratos e afins, poderão ser supridas no conforto de nossas casas e tendo papel ativo nas auditorias de tais validações apenas tendo um dispositivo com acesso à Internet. Muitas empresas estão adotando tais tecnologias a fim de garantir qualidade no serviço prestado e até mesmo para uso interno no quesito de votações para eleger algo.

Mas o que de fato implica nosso artigo, é o questionamento sobre o funcionamento das urnas eletrônicas do Brasil, que até então não temos a garantia de integridade e imutabilidade dos votos dos eleitores. Apesar de ter um sistema que utiliza a tecnologia a fim de garantir uma eleição segura, os eleitores não participam da auditoria da apuração dos votos.

Pensando em melhorias neste assunto, o artigo apresenta uma possível solução e um grande passo para democracia. Seguindo a literatura aqui abordada, com o uso das tecnologias blockchain e smart contracts a partir da plataforma Ethereum, podemos então criar um sistema de votação online em que todos os eleitores que tenham seus dispositivos, sejam eles smartphones ou computadores, possam votar e auditar seus votos.

A simulação em que fizemos nos mostra uma aplicação totalmente funcional e de fácil acesso. Desde uma interface limpa e de simples entendimento, algo semelhante a tela das urnas eletrônicas, o eleitor poderia efetuar seu voto sem grandes dificuldades.

A implementação de tal tecnologia não traz somente benefícios relacionados a transparência e integridade dos votos, e sim, também, como custos eleitorais e desperdícios causado pelas urnas eletrônicas. Este artigo visou a compreensão de tais tecnologias e os benefícios gerados pela sua adoção, e é uma sugestão de implementação no cenário eleitoral brasileiro, tornando assim eleições mais transparentes, seguras, com menos custos e o principal, eleitores ativos na auditoria de seus votos.

Distributed voting system via the internet through the use of smart contracts

ABSTRACT

In Brazil, electronic voting machines have always been subject to criticism because voters do not know if their votes have actually been registered for their desired candidates. Issues such as immutability, integrity, and transparency of votes always arise. Therefore, this article suggests the use of two technologies, namely blockchain and smart contracts, as a proposal to be used in a distributed voting system conducted over the Internet, where data is recorded and validated through a network of computers, ensuring what is known as consensus. With the significant impact of cryptocurrencies, the emergence of the Ethereum platform allows for online transactions using smart contracts, not only for financial applications of digital currencies. This article also proposes an exploratory analysis of these technologies. To that end, we created a voting simulation using the Ethereum platform and a Solidity-programmed smart contract to demonstrate the application. With positive results from the simulation, the use of the technologies discussed here clearly indicates that their implementation would be a significant step towards democracy, as well as cost reduction, waste reduction, and improvement of corporate image.

KEYWORDS: Ethereum. smart contracts. Blockchain. Democracy. distributed systems.

REFERÊNCIAS

- Melo, R.G.V. **Análise de Percepções de Segurança da Informação por meio da Engenharia Semiótica e da Teoria do Umwelt.** (Dissertação de mestrado). Universidade Federal da Bahia, Salvador, BA, Brasil, 2016.
- Ferreira, J. E., Pinto, F. G. C., & Santos, S. C. **Estudo De Mapeamento Sistemático Sobre As Tendências E Desafios Do Blockchain.** 108–117, 2017.
- Pires, T. P. **Tecnologia Blockchain E Suas Aplicações.** 1–57, 2016.
- Curran, K. **E-Voting on the Blockchain.** *The Journal of the British Blockchain Association*, 1(2), 1–6, 2018. Disponível em: < [https://doi.org/10.31585/jbba-1-2-\(3\)2018](https://doi.org/10.31585/jbba-1-2-(3)2018)> Acesso em: 5 mar. 2019.
- Divino, S. B. S. **Smart Contracts: Conceitos, Limitações, Aplicabilidade E Desafios,** 2018. Disponível em: <https://www.academia.edu/37733887/SMART_CONTRACTS_CONCEITOS_LIMITAÇÕES_APLICABILIDADE_E_DESAFIOS> Acesso em : 2 abri. 2019.
- Carlomagno, M. C. **Sistema proporcional , puxador de votos e um problema inexistente: os mais votados já são os que se elegem.** *Newsletter. Observatório de Elites Políticas e Sociais Do Brasil. NUSP/UFPR*, 3(10), 1–14, 2016.
- Ben Ayed, A. **A Conceptual Secure Blockchain Based Electronic Voting System.** *International Journal of Network Security & Its Applications*, 9(3), 01–09, 2017. Disponível em: <<https://doi.org/10.5121/ijnsa.2017.9301>>. Acesso em: 22 mar. 2019.
- Arruda, G. O. de. **A tecnologia a serviço da democracia: o processo eleitoral na era da informação.** *Revista Da Advocacia Pública Federal*, Vol. 1, pp. 139–148, 2017. Disponível em: <<http://anafenacional.org.br/seer/revista/issue/download/1/1>>. Acesso em: 10 fev. 2019.
- Clack, C. D., Bakshi, V. A., & Braine, L. **Smart Contract Templates: essential requirements and design options.** 1–15, 2016. Disponível em: <<http://arxiv.org/abs/1612.04496>> Acesso em: 01 abri. 2019.
- Cachin, C., Androulaki, E., De Caro, A., Kind, A., Osborne, M., Schubert, S., ... Vukolic, M. **Blockchain, Cryptography and Consensus - IBM Research – Zurich,** 2017. Disponível em: <<https://cachin.com/cc/talks/20170622-blockchain-ice.pdf>> Acesso em: 15 abri. 2019.
- Pedro Vilela Resende Gonçalves, & Rafael Coutinho Camargos. **Blockchain, Smart Contracts E 'Judge As a Service' No Direito Brasileiro,** 2018. Disponível em: <https://s3.amazonaws.com/academia.edu.documents/54422335/Anais_II_Seminario_-_Globalizacao_Tecnologias_e_Conectividade.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527564500&Signature=tJKkqqCAXWRA9Y33VOVUsF5jWas%3D&response-content-disposition=inline> Acesso em: 05 mar. 2019.

Szabo, Nick. **The idea of smart contracts**. Nick Szabo's Papers and Concise Tutorials, n. c, p. 1–2, 1997.

Mougayar, W. **Blockchain para negócios**: Promessa, prática e aplicação da nova tecnologia da internet. (Alta Books Editora), 2018.

Meeser, F. L. **Decentralized , Transparent , Trustless Voting on the Ethereum Blockchain**. *Journal of Medical Systems*, 1–6, 2017. Disponível em: <<https://doi.org/10.1007/s10916-016-0574-6>>. Acesso em: 08 jun. 2019.

Santos, F. M. **Responsabilidade civil do candidato frente ao dano ambiental causado pela campanha eleitoral**, 2015. Disponível em: <<http://www.ri.unir.br/jspui/handle/123456789/411>>. Acesso em: 15 jul. 2019.

Freitas, D. M. S. **Diagnóstico e proposta de modelo de gestão dos resíduos eletroeletrônicos gerados nos Ministérios do governo brasileiro**, 2010. Disponível em <<https://bdtd.ucb.br:8443/jspui/handle/123456789/1598>>. Acesso em: 11 maio 2019.

Bedran, K. M. **Processo eleitoral brasileiro : impactos ambientais e o direito ao meio ambiente ecologicamente equilibrado**, 2013. Disponível em: <<http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/4071>>. Acesso em: 22 fev. 2019.

FollowMyVote, 2019. Disponível em : <<https://followmyvote.com/>>. Acesso em: 20 de março de 2019.

Polys, 2019. Disponível em : <<https://polys.me/>>. Acesso em: 20 de mar. de 2019.

Agora, 2019. Disponível em : <<https://www.agora.vote/>>. Acesso em: 20 de mar. de 2019.

Tsai, W. T., & Lu, Y. C. (2019). A Secure E-Voting System Based on Blockchain Technology. *International Journal of Information Security and Cybercrime*, 8(2), 79-88.

Kshetri, N. (2017). Can blockchain strengthen the internet of things. *IT Professional*, 19(4), 68-72.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). Towards the integration of blockchain and internet of things. In *Internet of Things (IoT)* (pp. 375-392). Springer.

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM*, 58(9), 104-113.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media, Inc. 05/07/2022.

Recebido: 01/02/2023

Aprovado: 05/02/2024

DOI: 10.3895/rts.v20n59.16365

Como citar:

LIMA, Wesley Felix de; VASCONCELOS, Daniela Manetta; GRASSI, Flavio. Sistema distribuído de votação via internet através do uso de smart contracts. *Tecnol. Soc.*, Curitiba, v. 20, n. 59, p.195-218, jan./abr., 2024. Disponível em:

<https://periodicos.utfpr.edu.br/rts/article/view/16365>

Acesso em: XXX.

Correspondência:

Direito autoral: Este artigo está licenciado sob os termos da Licença Creative Commons-Atribuição 4.0 Internacional.

