## # Tecnologia EtherVoltz Para Eleições Auditáveis

## Resumo

Este artigo apresenta uma proposta de sistema eleitoral independente de software que remove do administrador a responsabilidade de garantir a disponibilidade, integridade e confiabilidade dos registros digitais dos votos. A metodologia adotada inclui pesquisa bibliográfica, análise de problemas no sistema eleitoral brasileiro w a construção de uma prova de conceito. A estratégia utilizada para alcançar os objetivos envolve a construção de uma aplicação distribuída empoderada por tecnologia blockchain e a infraestrutura formada pelos milhares de nós da rede Ethereum.

## 1. Introdução

Em sistemas eleitorais e primeira, segunda e terceira geração, os registros digitais dos votos ficam salvos na memória dos equipamentos que precisam ser levados dos locais de votação de volta para as centrais para que ocorra a apuração dos votos. Além dos custos envolvidos para garantir que estes equipamentos não sejam alterados ou destruídos durante o transporte, o administrador também precisa guardar estes registros após a apuração de votos para posteriores auditorias.

Uma solução trivial que alguém pode propor, é a utilização de um sistema cliente-servidor para a gerência destes registros. Entretanto, sistemas que utilizam esta arquitetura apresentam falhas que podem aumentar o custo das eleições significativamente e que introduzem novos pontos de falha ao sistema:

1. **Ataques de negação de serviço**: É imprescindível que eleições não sejam atrasadas devido a um possível ataque de negação distribuído.
2. **Vazamento de chaves**: Se as credenciais utilizadas para a administração do sistema são adquiridas por um atacante, este tem o poder total sobre o resultado das eleições.
3. **Ataques internos**: As vulnerabilidades de um sistema aumentam proporcionalmente ao seu tamanho. Ataques internos se tornam um problema à medida que mais e mais pessoas estão envolvidas no processo de desenvolvimento dos muitos componentes que protegem o sistema.

Após o período eleitoral, caso um cidadão queira auditar os resultados das eleições ele precisa interagir com o administrador do processo eleitoral para ter acesso os registros digitais, aos equipamentos e aos registros independentes de software (caso o administrador tenha optado por sistemas que utilizem VICE). Cabe ao administrador decidir se ele tem ou não permissão para realizar a auditoria e quais são condições para a realização da mesma.

Os problemas deste tipo de centralização de poderes ficam evidente no Brasil. Embora não seja objetivo deste documento discutir os efeitos da centralização de poderes em sistemas eleitorais, alguns casos bem documentados são brevemente listados a seguir:

1. **O Caso Marília, SP - 2004**: Em auditoria, os Arquivos de Espelhos de Boletins de Urna da 400º Zona Eleitoral indicavam que muitas seções eleitorais tiveram seus resultados recebidos para apuração **antes do início da votação**. Dois processos judiciais foram iniciados decorrentes destas constatações, ambos encerraram em 2009 sem julgamento final. [1]
2. **O Caso Itajaí, SC - 2008**: Foi constatada burla intencional na cerimônia de carga e lacração das urnas em que nenhuma urna preparada para a votação passou pelo teste obrigatório prescrito pelo Art. 32 da Res. TSE 22.712/08. Um caso foi o da 97ª Zona Eleitoral onde a urna da seção 236 que foi sorteada para o teste obrigatório **foi substituída por outra** na hora do teste, preparada exclusivamente para este fim. A urna que foi utilizada para o teste foi posteriormente colocada à parte e recarregada, procedimento que destruiu eventuais provas nela gravadas. [2]
3. **O Caso Diadema, SP - 2000**: Foram negados a todos os partidos que solicitaram o acesso aos registros digitais dos votos realizados nas urnas eletrônicas. Somente 9 meses após a eleição os partidos obtiveram acesso, não aos registros dos votos, mas aos Arquivos de LOG das urnas que apontaram que **todas** as urnas haviam sido carregadas **fora** da cerimônia oficial de carga e lacramento das urnas. [3]
4. **O Caso Alagoas - 2006**: Diversas irregularidades nos arquivos gerados pelas urnas foram detectadas por auditores externos [4]. Frente as evidências, o administrador negou acesso aos arquivos solicitados pelos auditores e transferiu ao requerente uma cobrança antecipada no valor de R$ 2 milhões para que fosse desenvolvida uma perícia das urnas. Diante do não pagamento do valor proibitivo, o requerente foi multado e condenado por litigância de má-fé.  
   Mesmo tendo apresentado provas de inconsistência no funcionamento das urnas, a perícia das mesmas não foi permitida. [5]
5. **Assinaturas Divergentes - 2002 e 2008**: Nas eleições de 2º Turno de 2002 e 2008, foram detectadas durante verificação dos arquivos carregados nas urnas eletrônicas, a presença de um conjunto de arquivos com resumos digitais diferentes das publicadas nas respectivas cerimônias oficiais de lacramento dos sistemas. A providência tomada pelo administrador frente a estas descobertas, foi a de publicar novas Tabelas de Hash, calculadas **a portas fechadas e fora de uma cerimônia oficial**. A perícia das urnas foi indeferida e as Tabelas de Hash originais que demonstravam a impropriedade, foram removidas do local. [6]

Este projeto propõe a utilização do *blockchain* *Ethereum* como o *backend* que gerencia e armazena os registros digitais dos votos. Embora algumas características da estratégia estejam listadas abaixo, as vantagens ficarão mais evidentes na Seção 4.4 Auditorias deste documento.

1. Decentralização: Como a máquina virtual não possui um dono ou entidade responsável por sua administração, nenhuma instituição ou pessoa possui poder de censurar ou de alguma forma impedir que aplicações hospedadas na plataforma se mantenham em execução.
2. Distribuição: Diferente de sistemas que utilizam a arquitetura cliente-servidor, aplicações que executam na máquina virtual *Ethereum* são resistentes a ataques de negação de serviço distribuídos.
3. Todas atualizações na base de dados são registradas permanentemente no blockchain estão disponíveis para auditoria por qualquer pessoa, a qualquer momento em qualquer lugar.

## 2. Conceitos e Definições

Para facilidar a explicação altamente abstrata do funcionamento da solução proposta, são definidas nesta seção diversos termos utilizados ao longo do documento. Embora definidos brevemente aqui, o leitor se beneficiará se possuir conhecimento sobre os mecanismos envolvidas em sistemas eleitorais, desenvolvimento de software e criptografia. O Leitor se beneficiará principalmente se possuir conhecimento sobre o funcionamento de *blockchains* como o Bitcoin e Ethereum.

### 2.1 Princípio da Independência de Software em Sistemas Eleitorais

A tradução da definição apresentada pelo autor do termo, que é também um dos autores da chave de assinatura digital RSA [7]:

Um sistema eleitoral é independente do software se uma modificação ou erro não-detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da apuração.

### 2.2 VICE

O VICE ou Voto Impresso Conferível Pelo Eleitor é um documento em papel que é apresentado ao eleitor no momento da votação. O VICE é apresentado para que ele possa confirmar visualmente o voto, mas ao qual ele não tem contato físico (e nem leva para casa). [8]

Os termos VICE e registro de voto físico são utilizados de forma intercambiável neste documento e significam a mesma coisa.

### 2.3 Livro Razão Público

Livro razão é o nome dado a um documento que agrupa modificações ordenadas do estado de alguma informação. *Blockchains* são comumente comparados a livros razão públicos, pois são uma sequência de alterações de estado ordenadas uma após a outra e cujas alterações dependem necessariamente do estado anterior:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Remetente | Operação | Parâmetros | Destinatário |
| .. | ... | ... | ... | ... |
| 3925 | João | enviou | 3 reais | para Alice |
| 3926 | Alice | enviou | 2 reais | para Carlos |
| 3927 | Carlos | enviou | 1 real | para João |
| 3928 | João | enviou | 1 real | para Alice |
| ... | ... | ... | ... | ... |

No exemplo acima, a transação número 3927 só será incluída no livro razão se Carlos possuir 1 real ou mais.

### 2.4 Estado

O estado da aplicação é o conjunto de todas as informações e variáveis da aplicação em um determinado instante e que um sistema deve rastrear.[9] [10] Em sistemas mais simples isto pode ser apenas o balanço de contas e em sistemas mais complexos, estruturas de dados que fazem parte da aplicação.

### 2.5 Transação

Uma transação é uma mensagem enviada à aplicação e que inclui dados sobre determinada operação que o remetente deseja executar. As transações discutidas neste documento possuem, além de outras informações: - O endereço do destinatário. Na maioria dos casos aqui discutidos, o destinatário é a aplicação EtherVoltz. O endereço também é a chave pública do destinatário. - Uma assinatura criptográfica que comprova o remetente da transação. - Informações sobre a operação a ser realizada, como o nome da operação e parâmetros. [9] [10] [11]

Sempre que uma transação é confirmada, um *hash* que identifica esta transação individualmente é gerado a partir do conjunto de informações contidas nela e na história do blockchain até o momento. Com este *hash* é possível solicitar à EVM informações sobre a transação. Este recurso é explorado no EtherVoltz para garantir a rastreabilidade das operações realizadas na aplicação durante uma auditoria.

### 2.6 Bloco

Um bloco "b" é um pacote de dados contendo uma lista de transações T, também uma referência à um bloco anterior "d" e opcionalmente, mais informações. [9] [10] A inclusão de um bloco no blockchain implica na atualização do estado, mas o bloco só é incluído se for considerado válido. [11] [12] Um bloco b é considerado válido se:  
1. Todas as transações t pertencentes a T listadas nele são válidas. 3. O bloco "d" ao qual ele faz referência é válido. 2. As condições impostas pelo protocolo de consenso são atingidas.

### 2.7 Blockchain

Um blockchain B=[b0,b1,b2,b3...] é uma sequência de blocos bn em que cada bloco faz referência ao bloco precedente até o bloco gênesis "b0". Um *blockchain* é dito válido se cada bloco b pertencente a B for válido. Em discussões sobre desenvolvimento de aplicações distribuídas empoderadas por tecnologia blockchain - e em alguns trechos neste documento-, é comum se referir ao mesmo como um banco de dados distribuído, visto que existem copias dela armazenadas nos computadores dos milhares de nós e mineradores espalhados pelo mundo. Neste documento o termo blockchain será utilizado para se referir especificamente ao blockchain utilizado na máquina virtual Ethereum, mas vale lembrar que esta estrutura de dados também é utilizada em outros sistemas como Bitcoin e Litecoin. [8] [9] [12]

### 2.9 Nó Completo

Neste documento, "Nós" são computadores conectados à rede ethereum através de algum cliente como *geth* ou *pyeth* e que possuem uma cópia completa ou parcial do blockchain. O termo "nó completo" é utilizado para explicitar que o nó em questão possui uma copia do blockchain completa e válida, já que existem nós ditos leves, que podem possuir apenas uma cópia parcial do blockchain. [10]

### 2.10 Maquina virtual Ethereum, EVM, Computador Mundial

A máquina virtual Ethereum ou EVM (do inglês Ethereum Virtual Machine) é, em um sentido técnico, um computador mundial que pode ser utilizado e programado por qualquer pessoa. Possui apenas um processador e um *thread* para executar programas, mas tanta memória quanto for necessária. [13]

Qualquer pessoa pode escrever programas que podem executados por este computador, fazer upload deles à máquina virtual e fazer requisições ao programa para serem executadas. Por isto, a máquina virtual Ethereum é frequentemente referenciada como sendo um Computador Mundial.

O computador é formado por uma rede *peer-to-peer* de computadores que dedicam hardware e eletricidade para executar estes programas e recebem em troca uma recompensa financeira para isto.

Outra característica importante é a de que, em um sentido técnico, cada programa possui seu próprio armazenamento que persiste entre execuções. Enquanto houver demanda, a máquina virtual e todos os programas estarão disponíveis. A EVM não pode ser desligada.

Programas no computador mundial, executam exatamente como programados. A implicação disto é de que um desenvolvedor pode escrever um programa que só pode receber requisição de certas pessoas, podendo inclusive revogar o direito do próprio criador do programa de interagir com ele para garantir transparência a terceiros. Este é um recurso utilizado no núcleo do projeto EtherVoltz em que o administrador do processo eleitoral revoga parte do próprio poder de interação com o programa para dar transparência e imutabilidade ao processo. [14]

### 2.11 Contrato, Contrato Inteligente, *Smart Contract*

*Smart contract*, contrato inteligente ou simplesmente contrato, é um termo utilizado informalmente para referir a código que executa no computador mundial [10] [13]. O núcleo da prova de conceito concebida no projeto EtherVoltz é um contrato inteligente escrito na linguagem de programação Solidity.

Formalmente, são contas que contém e são controladas por código na máquina virtual Ethereum. Por padrão, contratos só podem ser controlados diretamente por chaves privadas se isto for definido em código. O efeito disto, é que um contrato não possui "dono" após *deployment*. [10]

### 2.12 Criptomoeda, Token, VoltToken

Uma criptomoeda é um bem digital projetado para servir como meio de troca utilizando criptografia para assegurar transações e controlar a emissão de novas unidades da moeda. [15]

VoltToken é uma criptomoeda proposta e implementada na prova de conceito deste projeto, para servir como um meio do eleitor expressar sua intenção de voto.

Neste documento, a palavra *Token* é ocasionalmente utilizada para evidenciar que diferente de criptomoedas comuns, esta não pode ser transferida livremente de uma pessoa para outra.

### 2.13 Carteira

Embora incorreto tecnicamente, o termo "carteira" é utilizado em discussões sobre criptomoedas como uma boa analogia para explicar o efeito de possuir a uma chave pública e sua chave privada associada capaz de assinar transações. [10] [12]

O hash da chave pública funciona como um "endereço" que pode ser utilizado para receber criptomoedas de outras carteiras.

A chave privada pode ser vista como uma "senha" que deve ser mantida em segredo, capaz de "destrancar" a "carteira" para enviar criptomoedas a outro "endereço".

### 2.14 Conta

Contas, assim como carteiras, possuem um balanço intrínseco e uma contagem transações mantidas como parte do estado Ethereum, mas também podem possuir código Ethereum e um estado de armazenamento associado. Cada conta possui um endereço único que a identifica.[13]

Um programa hospedado na máquina virtual como o que é proposto neste documento, é uma conta cujo código é o definido no contrato inteligente.

## 3 Estratégia

A estratégia utilizada envolve transformar os votos de uma dada eleição em uma criptomoeda que existirá para ser os registros digitais dos votos, de forma que um voto seja a transferência de uma moeda pertencente a uma carteira associada a uma urna para uma carteira associada um candidato. Nota: O candidato não possui nenhum poder administrativo sobre a carteira que receberá os votos.

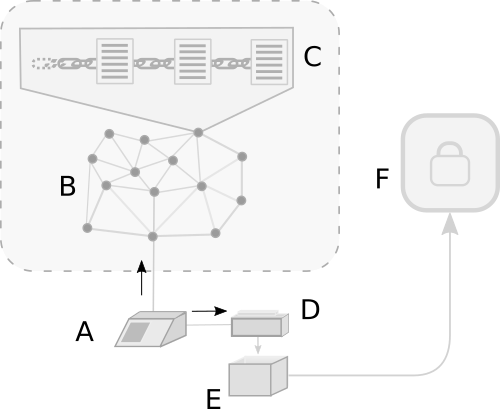
A regulamentação da transferência destas criptomoedas e o processo de emissão de novas unidades é definido através do código disponibilizado publicamente no contrato inteligente quando o sistema é criado.

Após *deployment* na máquina virtual, a regras não podem ser alteradas por ninguém, mas todas as alterações de estado e o código fonte do programa podem ser auditados por qualquer um a qualquer instante.

Na prova de conceito do projeto EtherVoltz, a criptomoeda foi batizada de VoltToken e será discutida em mais detalhes na seção 4.1.

Para garantir o principío de independência ao sistema, o projeto propõe o uso de um registro físico do voto ou VICE que fica sobre posse do administrador do processo eleitoral. A diferença deste modelo de VICE aos modelos propostos nas urnas de segunda e terceira geração, é que esta inclui o hash resultante da transferência do VoltToken. Detalhes sobre este modelo de VICE são discutidos na Seção 4.2.

Portanto, em cada voto são produzidas duas provas que se referenciam: Uma é o VICE que fica sobre controle do administrador do processo. A outra é o registro digital e que fica salvo no blockchain e sobre qual o administrador não possui controle.



Na figura, as imagens rotuladas pelas letras A, B, C, D, E e F representam respectivamente: - Um computador conectado à rede Ethereum. - A rede Ethereum composta por milhares de nós ao redor do mundo. - Uma cópia do blockchain em nó na rede. - Uma impressora para imprimir o registro de voto físico. - Caixa lacrada para coleta dos VICE - Cofre para armazenamento dos VICE sob controle do administrador

Note que de "A" saem duas setas, elas representam os destinos dos registros digitais e físicos respectivamente. A área demarcada por linha tracejada representa a base de dados decentralizada, isto é, a região do sistema sobre a qual nenhuma entidade central possui controle. Dados e programas que executam nesta região, são resistentes a censura e operam exatamente como definidos nos contratos.

## 4 O Caminho do Voto

Esta seção apresenta uma explicação de alto nível de como uma eleição comum funciona sobre o sistema EtherVoltz.

### 4.1 A Produção e Auditoria do Código Fonte

Os requisitos que o contrato inteligente utilizado da prova de conceito pretende atender estão listados a seguir: - A transferência de VoltTokens só pode ocorrer durante o período eleitoral. Portanto, votos só podem ser emitidos nesta janela de tempo. - Apenas endereços de carteiras registradas no contrato podem transferir VoltTokens. - Apenas endereços de carteiras que representam candidatos podem receber VoltTokens. - Todas as urnas e suas respectivas carteiras são identificadas através de suas chaves públicas e estão definidas no contrato inteligente. - O número total de moedas em circulação é definido no momento da criação do sistema. - Nenhuma nova unidade da moeda pode ser emitida após a criação do sistema. - Cada urna recebe precisamente o número de VoltTokens correspondente ao número de eleitores que devem votar naquela urna. - As regras anteriores são auditáveis por qualquer um através do código fonte do contrato disponibilizado pelo administrador.

Muito antes do período eleitoral, o administrador publica uma proposta do código fonte do contrato inteligente que será utilizado para regulamentar a emissão e controle de transferência das criptomoedas, para que o grande público possa propor melhorias e descobrir falhas.

Após as melhorias serem implementadas, em cerimônia oficial, o administrador compila o código, envia o contrato à EVM e publica o endereço do mesmo para que o público possa acompanhar auditar todas as mudanças de estado que ocorrerem no programa.

O administrador publica o código fonte do contrato inteligente para que qualquer auditor possa comparar o *byte code* resultante da compilação, com o *byte code* do contrato no endereço disponibilizado na cerimônia oficial.

### 4.2 O Procedimento do Voto

Do ponto de vista do eleitor, o voto ocorre da mesma forma que em uma urna de segunda geração comum, exceto que a impressão do VICE ocorre em duas etapas.

A seguir são detalhados eventos relevantes que ocorrem durante a emissão de um voto. 1. O eleitor, após ser autorizado pelo mesário, digita o código do candidato. 2. A impressora imprime o VICE que fica visível para que o eleitor possa conferir. 3. Se os dados estão corretos o eleitor pressiona "confirma". 4. A urna envia uma transação à aplicação que está no endereço publicado na cerimônia oficial para transferir 1 VotltToken da carteira da urna para a carteira que representa o candidato. 5. Após a confirmação da transação, a urna recebe um *hash* que identifica unicamente este voto no blockchain. 6. A impressora imprime este hash no VICE. 7. O VICE é cortado e cai em uma caixa lacrada.



### 4.3 Pós-Voto

Após o período eleitoral existem dois registros de cada voto contado. Um deles é o registro digital do voto que está gravado no blockchain da máquina virtual Ethereum. O outro é o voto impresso conferível pelo eleitor.

Os registros digitais dos votos podem ser solicitados por qualquer pessoa a qualquer momento para auditoria e possuem as seguintes informações: - De qual urna o voto foi emitido. - Qual candidato recebeu o voto. - O hash que identifica unicamente esta transação no blockchain

Já os registros físicos do voto, ficam sob controle do administrador da eleição e possuem as seguintes informações: - De qual urna o voto foi emitido. - Qual candidato recebeu o voto. - O hash que identifica unicamente esta transação no blockchain

A apuração dos votos é instantânea e consiste em apenas solicitar ao computador mundial, o balanço das carteiras criadas para receberem os votos dos candidatos.

### 4.4 Auditorias

Os passos para uma auditoria simples de uma urna estão listados a seguir. 1. O auditor solicita à maquina virtual uma lista com todas as transações realizadas pela urna em questão, passando a chave pública da urna. 2. O auditor solicita ao administrador da eleição, a caixa contendo os votos impressos conferíveis pelo eleitor, da mesma urna. 3. O auditor compara as duas provas, atento as regras listadas abaixo. - O número de VICE's na caixa deve ser exatamente igual ao número de registros de voto digital retornados pela máquina virtual Ethereum - Cada registro digital de voto retornado pela máquina virtual Ethereum precisa ter um VICE associado na caixa que o administrador entregou ao auditor. - Cada VICE precisa ter um *hash* válido.

Um *hash* impresso no VICE é considerado válido se: - Ele existir no blockchain Ethereum - O endereço do remetente for igual ao da urna que está sendo auditada - O endereço da carteira do candidato que recebeu o voto for o mesmo que o impresso no VICE - O endereço do contrato da criptomoeda for o mesmo publicado na cerimônia oficial.

## 4. Conclusão

EtherVoltz é uma proposta que visa decentralizar o processo eleitoral e de auditorias ao transferir a responsabilidade de gerenciar dos registros digitais de votos a um programa que executa em uma máquina virtual que não possui autoridade central, é imutável e resistente a censura.

Ao transformar o voto do eleitor em uma criptomoeda, o sistema imediatamente ganha todas as propriedades de segurança do protocolo de consenso e de disponibilidade da rede *peer-to-peer* utilizado na plataforma.

Embora ainda exista a necessidade da emissão e controle dos VICE para garantir o Princípio da Independência de Software ao sistema, a separação do destino das duas provas produzidas no momento do voto dá aos eleitores poder de auditoria com limitada necessidade do envolvimento de intermediários.

## 5. Referências

[1] 1º Relatório do Comitê Multidisciplinar Independente - pg 27.

[2] 1º Relatório do Comitê Multidisciplinar Independente - pg 34.

[3] 1º Relatório do Comitê Multidisciplinar Independente - pg 24.

[4] Fernandes, C.T. - Radiografia das Urnas Eleitorais. S. J. dos Campos: ITA, dezembro de 2006.

[5] 1º Relatório do Comitê Multidisciplinar Independente - pg 27.

[6] 1º Relatório do Comitê Multidisciplinar Independente - pg 25.

[7] RIVEST, Ronald L. - On the notion of 'software independence' in voting systems.

[8] Brunazo, Amilcar - Modelos e Gerações dos Equipamentos de Votação Eletrônica - acesso em http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm#3o, 27/08/2017

[9] GAVIN WOOD - ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER - pg 2-6

[10] Ethereum Wiki, Glossary - acesso em https://github.com/ethereum/wiki/wiki/Glossary, 27/08/2017

[11] Ben Yuan, Wendy Lin, and Colin McDonnell - Blockchains and electronic health records - pg 3

[12] Bitcoin Vocabulary - acesso em https://bitcoin.org/en/vocabulary, 27/08/2017

[13] GAVIN WOOD - ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER - pg 15-16

[14] Ethereum Wiki, What is Ethereum - acesso em https://github.com/ethereum/wiki/wiki/What-is-Ethereum - 27/08/2017

[15] Usman W. Chohan - Cryptocurrencies: A Brief Thematic Review