EtherVotes: Blockchain e Canais de Estado Para Eleições Auditáveis

Matheus Faria de Alencar

13 de agosto de 2017

Resumo

Os problemas segurança de processos eleitorais serviram como combustível para uma série de estudos e avanços tecnologicos para melhorar detectabilidade de fraudes e ao mesmo tempo prover celeridade na apuração de votos. Estes avanços acarretaram em um aumento de complexidade dos processos e sistemas, que por consequencia colocaram barreiras de tempo e custo em processos de auditoria além de centralizarem o poder de condução das mesmas no administrador. P1: Definir custos, centralização de poder, dificuldades de auditoria

A utilização de sistemas cliente-servidor também não são soluções viáveis para a condução de processos eleitorais já que oferecem pontos de falha vulneraveis a ataques de negação de serviço e dependem da confiança nos envolvidos no processo para adminstração das chaves. P2: Apresentar problema de soluções com servidores

Este artigo documenta uma prova de conceito de sistema eleitoral chamado EtherVoltz (pronunciado Íter vÔltz) que não depende de software e faz uso do blockchain de um computador global decentralizado (1) e distribuído (2) para baratear e simplificar os processos de eleição e auditoria. Esta proposta também remove do administrador a tarefa e o poder de controlar os registros digitais dos votos após a votação sobrando ao mesmo a tarefa do gerenciamento dos votos impressos para posteriores auditorias. P3: Apresentar EtherVotes como possível solução para o problema

Abstract

Security issues in election processes fueled a series of worldwide studies and technological advances to improve fraud detectability and speed up the vote counting process. These advances caused an increase in the complexity of the electoral process and as consequence placed time and cost barriers on the auditing process as well as a concentration of powers in the administrator.

The use of the client-server architecure has also been proven to be challenging since they are vulnerable to denial-of-service attacks and still rely on trusting the ones involved on the processes to manage the keys that guarantee its safety.

This article documents a proof of concept of an electoral system called EtherVoltz that does is software-independent and leverages the blockchain of global computer that is decentralized and distributed to simplify and cheapen the election and auditing processes. This proposal also removes from the administrator, the burden and power

of managing the digital records that are generated during the election process, leaving the task of managing the paper trails generated.

Palavras-chaves: ethervotes. blockchain. ethereum. eleições. raiden.

---

1 Introdução

A medida componentes eletrônicos foram sendo barateados e miniaturizados, sistemas eletrônicos para votação vem sendo desenvolvidos para aumentar a velocidade de apuração de votos e através de soluções com registros de voto digital. A primeira geração destas urnas são as chamadas dependentes de software e utilizam apenas o registro digital de votos ou DRE e é o sistema que o Brasil utiliza desde a sua concepção 1996. P1: Introdução à area

De fato, a urna brasileira de primeira geração em uso até 2018, utiliza apenas o registro digital de voto e não gera nenhum documento auditável pelo eleitor e portanto não adere ao princípio da independência de software (3). Não possibilita aos representantes da sociedade conferir e auditar o resultado da apuração eletrônica dos votos. Foi rejeitada por todos os mais de 50 países que a avaliaram [1] que optaram por soluções que utilizam documento auditável como urnas de segunda e terceira geração. P2: Motivação

1.1 Custos

A Reforma Eleitoral de 2015 reintroduz o voto impresso ao processo eleitoral brasileiro que propiciona independência de software ao processo. O preço de cada urna em 2018 segundo estimativas do TSE sobe de 600 doláres para 800 dolares com a utilização de impressoras, sendo necessárias aquisições de mais de 830 mil impressoras e mais de 400 mil novas urnas segundo o TSE [2]. Além das dispesas relacionadas a aquisição das urnas, o registro digital de voto das urnas requer um amplo esquema de segurança envolvendo as forças armadas, para realizar o transporte dos registros de voto digitais e das urnas. P3: Problemas

Uma solução trivial, porém falha para baratear o controle dos registros digitais muitas vezes proposto é a construção de um sistema cliente-servidor para a coleta e apuração dos dados. Três problemas cruciais desta solução são: 1. Torna servidores alvos extremamente valiosos a ataques externos e malwares. Os custos para a proteção destes sistemas sobe proporcionalmente a complexidade deles. 2. Elevado custo de manutenção dos servidores por necessidade de redundância para proteção contra ataques ataques de negação de serviço (4). 3. Deposita uma enorme quantidade de confiança em todos envolvidos processo de produção e manutenção do software, o que torna o sistema sucetível a ataques internos indetectáveis. No EtherVotes estes problemas são resolvidos ao delegar a tarefa de garantir a integridade, confiabilidade e disponibilidade dos dados a um blockchain em um computador global formado por uma rede p2p chamado Ethereum. Mais detalhes serão descritos na seção 5 deste documento. P3: Apresentar dificuldades financeiras do uso bases de dados comuns devido a vulnerabilidade a ataques DDoS, ataques internos.

1.2 Centralização

P1: P2: P4: Apresentar ethervotes como proposta para barateamento das eleições através de uma aplicação distribuida, a transformação do voto em uma criptomoeda infracionável e um minicomputador (como o raspberrypi) como interface com a urna.

P5: Dificuldades de auditorias de fraude devido a centralização do poder

P6: Experimentos desenvolvidos P7: Organização do texto

Nota 3: 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. [3]

2 Motivação: Eleições Caras e Opacas

P1: Apresentar altos custos das eleições em

2.1 Eleições de Primera Geração e Seus Custos

P1: Apresentar quantos países utilizam a urna DRE sem vice e a opinião internacional sobre ela.

P2: Apresentar o caso Marília, o caso Itajaí, o caso Diadema e o caso Alagoas

P3: Apresentar custo de urnas DRE sem e com VICE

P4: Concluir introduzindo a necessidade de VICE e conceito de independência de software, e proposta do trabalho para baratear e aumentar a segurança de sistemas eleitorais com VICE ao mover a urna à máquina virtual ethereum.

3 Informações Contextuais

P1: Apresentar a maquina virtual ethereum como um computador global e a linguagem de programação solidity

P2: Apresentar desafios de escalabilidade atuais e o conceito de canais de estado

4 Estado da Arte

P1: Apresentar desafios de escalabilidade do blockchain citando e-vox e follow-my-vote

P2: Apresentar problemas de auditabilidade de soluções dependentes de software

5 EtherVotes

P1: Descrever que os objetivos da proposta são delegar a responsabilidade da integridade e disponibilidade dos votos à EVM

5.1 Arquitetura e Metodologia

P1: Apresentar problemas de soluções baseadas apenas em blockchain (tempo de transação, limitações da evm)

P2: Apresentar canais de estado (Rede raiden) como solução

P3: Concluir com a criação de VoteToken.sol e o procedimento de transferência de tokens para carteiras de candidatos.

P4: Notar que estes contratos são simples, ficam disponíveis no enderenço na EVM após deployment e seus códigos-fonte podem e devem ser publicados para inspeção independente.

5.2 VoteToken

P1: Descrever o procedimento da emissão de moedas fazendo um paralelo ao bitcoin.

P2: Notar sobre a vantagem de segurança contra ataques internos, já que só possuem poder de voto carteiras que receberam votetokens que o STE emitiu.

5.3 Controle de carteiras

P1: Descrever o contrato MachineRegistry.sol como solução para exposição e controle de carteiras (chaves públicas)

P2: Descrever efeito da impressão da carteira da urna nas boletas contra fraudes

5.4 Apuração de Votos

P1: Descrever o que ocorre após as eleições no modelo antigo. Forças armadas, logística e transporte das urnas e boletas para apuração dos votos, perigo de fraude através da destruição de evidências (destruir urnas e boletas não favoráveis.

P2: Descrever que no ethervotes os votos estão registrados no blockchain, por isso não há necessidade de segurança no transporte do equipamento eletrônico. Na verdade, o mesmo poderiam ou deveriam ser destruídas para evitar o vazamento de chaves privadas.

P3: Descrever o processo de apuração atual e autoridade responsável.

P4: Descrever o processo de apuração no ethervotes (getBalance)

5.5 Auditorias

P1: Descrever processo de auditoria de uma única urna no ethervotes.

1-Solicitação de todas as boletas com a chave pública utilizada na urna a ser auditada (Ainda envolve o TRE)

P1: Explicar que não há necessidade de solicitar acesso a urnas, ou código fonte.

2-Solicitar um histórico de todas as transações realizadas por aquela chave pública à maquina virtual ethereum (não envolve o TSE)

P1: Explicar que o estado não tem controle sobre os dados digitalizados das urnas.

3-Comparar boletas entregues pelo TRE com as transações registradas no blockchain.

6 Conclusão

P1: Celeridade e Transparência nas auditorias

P2: Decentralização do poder

P3: Barateamento das eleições

7 Experimentos

P1: Apresentar prova de conceito construida e resultados