

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"

FACULDADE DE CIÊNCIAS - CAMPUS BAURU

DEPARTAMENTO DE COMPUTAÇÃO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

LUCCAS FERNANDES DE QUADROS

DEMOCRACIA LÍQUIDA POR MEIO DE BLOCKCHAIN

BAURU

2018

LUCCAS FERNANDES DE QUADROS

DEMOCRACIA LÍQUIDA POR MEIO DE BLOCKCHAIN

Trabalho de Conclusão de Curso do Curso
de Ciência da Computação da Universidade
Estadual Paulista “Júlio de Mesquita Filho”,
Faculdade de Ciências, Campus Bauru.
Orientadora: Profa. Associada Roberta Spolon

BAURU
2018

Luccas Fernandes de Quadros Democracia Líquida por meio de Blockchain/ Luccas Fernandes de Quadros. – Bauru, 2018- 31 p. : il. (algumas color.) ; 30 cm.
Orientadora: Profa. Associada Roberta Spolon
Trabalho de Conclusão de Curso – Universidade Estadual Paulista “Júlio de Mesquita Filho”
Faculdade de Ciências
Ciência da Computação, 2018.
1. Sistemas Distribuídos 2. Blockchain 3. Democracia Líquida 4. Votação Eletrônica

Luccas Fernandes de Quadros

Democracia Líquida por meio de Blockchain

Trabalho de Conclusão de Curso do Curso
de Ciência da Computação da Universidade
Estadual Paulista “Júlio de Mesquita Filho”,
Faculdade de Ciências, Campus Bauru.

Banca Examinadora

Profa. Associada Roberta Spolon
(Orientadora)
Depto de Computação - Faculdade de
Ciências
Unesp Bauru

**Profa. Dra. Simone das Graças
Domingues Prado**
Depto de Computação - Faculdade de
Ciências
Unesp Bauru

**Prof. Dr. Kelton Augusto Pontara da
Costa**
Depto de Computação - Faculdade de
Ciências
Unesp Bauru

Bauru, 12 de Novembro de 2018.

*Dedico este trabalho a minha Mãe, meu Pai, minha irmã Letícia e meu irmão Leonardo
que foram base fundamental para minha formação como ser humano. A formação
acadêmica, concretizada com este trabalho, é só um detalhe.*

Agradecimentos

Quero agradecer a algumas famílias. À de sangue, que me deu todo o suporte para sair de casa e ir em busca dos meus sonhos, e às que eu descobri neste caminho.

À república Havana, lugar onde estarei eternamente em casa, onde conheci mais 7 irmãos de outras mães que de alguma forma são responsáveis por quem eu sou. Obrigado pelas conversas de madrugada, pelos ombros pra chorar e por tudo que passamos juntos, dos perrengues aos momentos de alegria imensa onde tudo aquilo parecia ser pra sempre. "Havana quer dizer família". Eu amo todos vocês!

Ao Bauru Badgers que me apresentou as pessoas mais incríveis que eu poderia conhecer nesta faculdade, homens corajosos e que deram o sangue comigo dentro e fora das quatro linhas. Nada me fez crescer mais como pessoa do que aprender na prática, com cada um de vocês, o que é acreditar num sonho, num projeto e lutar por ele! Vocês são companheiros para a vida toda!

À minha amada Julia, que merecia uma página de agradecimentos pra si só, e foi crucial para minha vida nestes últimos 5 anos. Tudo que eu passei nessa graduação e na vida em Bauru foi um pouco mais fácil por poder ouvir sua voz todos os dias e chorar no teu colo sempre que possível. Você é a pessoa mais incrível que eu conheço, te amo!

E por fim pra todos aqueles que contribuíram com a parte acadêmica, professores, colegas de classe e principalmente todos aqueles que lutam por um ensino superior público, gratuito e de qualidade!

"Sou demasiado cético para ser incrédulo" (Benjamin Constant)

Resumo

Com os avanços tecnológicos, que culminaram numa sociedade cada vez mais conectada, alguns conceitos antigos como a democracia e a participação por voto ganharam novas roupagens e significados. É o caso da democracia líquida, conceito que vem sendo construído há mais de um século, mas que só se tornou possível na prática mais recentemente, com o advento da tecnologia *blockchain*, base para modelos organizacionais descentralizados. Tendo isso em vista, o presente trabalho versa sobre as possibilidades de uma democracia que se apresenta como um misto de direta e representativa, através da tecnologia emergente da *blockchain* e de aplicações descentralizadas. O objetivo é destrinchar esses conceitos e apresentar as etapas necessárias para a implementação de um sistema de votação eletrônico, seguro, auditável e que respeite os princípios do modelo da Democracia Líquida, resultando em uma aplicação descentralizada e facilmente aplicável para tomada de decisões em grupo.

Palavras-chave: Sistemas Distribuídos, Blockchain, Democracia Líquida, Votação Eletrônica.

Abstract

With the technological advances, which culminated in an increasingly connected society, some old concepts like democracy and participation by vote gained new clothes and meanings. This is the case of Liquid Democracy, a concept that has been built for more than a century, but which has only become possible in practice more recently, with the advent of blockchain technology, the basis for decentralized organizational models. With this in view, the present work deals with the possibilities of a democracy that presents itself as a direct and representative mix through the emerging blockchain technology and decentralized applications. The goal is to unravel these concepts and present the necessary steps for the implementation of an electronic voting system that is secure, auditable and that respects the principles of the Liquid Democracy model, resulting in a decentralized application for easy group decision making.

Keywords: Distributed Systems, Blockchain, Liquid Democracy, Eletronic Voting.

Lista de figuras

Figura 1 – Modelo de Democracia Líquida.	15
Figura 2 – Estrutura dos Blocos.	18
Figura 3 – Estrutura dos Blocos.	19
Figura 4 – Código em <i>Solidity</i>	21
Figura 5 – Funcionamento da ferramenta <i>Ganache</i>	22
Figura 6 – Interfaces para o usuário de ferramentas	23
Figura 7 – Exemplo de transação pública verificada através do Etherscan	25
Figura 8 – Interface para a votação de uma proposta	26
Figura 9 – Arquitetura aplicação descentralizada	27

Sumário

1	INTRODUÇÃO	11
1.1	Objetivos Gerais	13
1.2	Objetivos Específicos	13
1.3	Organização da Monografia	13
2	FUNDAMENTAÇÃO TEÓRICA	14
2.1	Democracia Líquida	14
2.2	Votação Eletrônica	16
2.3	<i>Blockchain</i>	17
2.3.1	Sistemas distribuídos e o problema dos generais Bizantinos	17
2.3.2	Funcionamento	18
2.3.3	Smart Contracts	18
2.4	Trabalhos relacionados	19
2.4.1	<i>LiquidFeedback</i>	19
2.4.2	Outras Experiências	20
3	METODOLOGIA	21
3.1	Tecnologias e Ferramentas Utilizadas	21
3.1.1	<i>Solidity</i>	21
3.1.2	<i>Truffle e Ganache</i>	21
3.1.3	Metamask e uPort	22
3.1.4	InterPlanetary File System	23
3.2	Métodos e Etapas	23
4	TESTES E RESULTADOS	25
4.1	Arquitetura da Aplicação	26
5	CONCLUSÃO	28
5.1	Trabalhos futuros	28
	REFERÊNCIAS	29

1 Introdução

A observação antropológica das tribos mais primitivas, desde as pré-agrícolas até as tribos indígenas que ainda vivem isoladas, revela que estas tendem a tomar decisões através de um consenso coletivo voluntário, mantendo a paz e a ordem dentro do grupo (OLSON, 1993). Ainda que hoje seja comum acreditar que a origem da democracia seja na Grécia por volta de 500 a.C, essas organizações resolviam naturalmente suas questões através de um consenso, algo muito próximo do que hoje se define como democracia.

Entretanto, a origem etimológica da palavra - *dēmokratiā*, que foi cunhado de *dēmos* ("pessoas") e *kratos* ("governo"), ou seja governado por pessoas - e o primeiro período do qual se tem registros históricos suficientes, é de Atenas no século 5 a.C. Existem muitas diferenças da democracia contemporânea para esta, principalmente em grau de participação.(CLARKE; FOWERAKER, 2003)

A democracia contemporânea no Brasil é mais próxima do que se conhece como Democracia Representativa. Na democracia representativa o voto da população é direcionado para um representante que, se eleito, tem o poder de votar nos tópicos pertinentes ao interesse público, representando assim seu eleitorado. O que difere da democracia direta na qual os cidadãos podem votar diretamente e decidir sobre os interesses da sociedade.

Quando a democracia representativa foi inicialmente estabelecida, ela resolveu diversos problemas políticos e práticos, superando assim a dificuldade da comunicação de longa distância e as restrições educacionais do séc XVIII, através da confiança da população em um grupo de representantes. Hoje no entanto a democracia representativa sofre com uma série de desafios endêmicos, resultado da própria natureza da democracia representativa, que não podem ser resolvidos meramente por freios, contrapesos ou outras pequenas iterações.(KAYE; SPATARO, 2016)

Há uma distinção clara que pode ser feita em termos de participação, do cidadão ateniense que tinha obrigações diretas com o destino da Cidade-Estado grega através de decisões coletivas, frente ao cidadão contemporâneo e o seu distanciamento com a classe política. Esta crise de representatividade foi apontada inclusive no estudo Índice de Percepção de Cumprimento das Leis (CUNHA et al., 2015) realizado pela Fundação Getúlio Vargas, que em sua última edição, relacionada ao 1o semestre do ano de 2015, apontou que o governo federal, o Congresso Nacional e os partidos políticos estão nas três últimas posições de um ranqueamento sobre confiança nas instituições, respectivamente com 17%, 15% e 5% de confiança por parte dos entrevistados.

Constant versou sobre este declínio da participação política do cidadão, da antiguidade à modernidade, sob o viés da liberdade. No trecho a seguir o autor discorre sobre

como esvaziamento do espaço democrático retira a soberania e a liberdade do cidadão moderno e a entrega a seus representantes.

Assim, entre os antigos o indivíduo quase sempre soberano nas questões públicas, é escravo em todos seus assuntos privados. Como cidadão, ele decide sobre a paz e a guerra; como particular, permanece limitado, observado, reprimido em todos seus movimentos; como porção do corpo coletivo, ele interroga, destitui, condena, despoja, exige, atinge mortalmente seus magistrados ou seus superiores; como sujeito ao corpo coletivo, ele pode, por sua vez, ser privado de sua posição, despojado de suas honrarias, banido, condenado, pela vontade arbitrária do todo ao qual pertence. Entre os modernos, ao contrário, o indivíduo independente na vida privada, mesmo nos Estados mais livres só é soberano em aparência. Sua soberania restrita quase sempre interrompida; e, se em épocas determinadas, mas raras, durante as quais ainda é cercado de precauções e impedimentos, ele exerce essa soberania, é sempre para abdicar a ela.

([CONSTANT](#), 2015)

Além de uma crítica à democracia representativa e o sistema eleitoral atual, Constant também expõe uma falha da democracia direta quando se refere a “limitação particular do indivíduo”. Se na democracia representativa o eleitor abdica de sua soberania, na democracia direta faltava força para os antigos exercerem suas liberdades individuais.

A abdicação da soberania pelo cidadão e a entrega a um grupo de representantes é a causa de um dos maiores males da nossa democracia, a corrupção. A teoria do seletorado, desenvolvida por [Mesquita e Smith](#) (2011), fornece um meio de entender esse problema:

A premissa fundamental na teoria do seletorado é que o objetivo principal de um líder é manter-se no poder. Para permanecer no poder, os líderes devem manter sua coalizão vencedora. Quando a coalizão vencedora é pequena, como em autocracias, o líder tenderá a usar bens privados para manter a coalizão. Quando a coalizão vencedora é grande, como nas democracias, o líder tenderá a usar bens públicos para satisfazer a coalizão.

([MESQUITA; SMITH](#), 2011)

É buscando um novo modelo democrático que surge uma terceira via, a democracia líquida, explorada em 2015 como uma forma promissora de tomada de decisões coletivas em um estudo da Google ([HARDT; LOPES](#), 2015). O modelo sugere um misto de democracia direta e democracia representativa, onde o cidadão poderia delegar seu voto para outro ou optar por votar diretamente no tópico em debate.

Ideias para uma aplicação mais granular da democracia têm sido propostas há anos, mas é somente agora com a Internet e o advento de sistemas como a tecnologia *blockchain* que esses mecanismos complexos e dinâmicos de tomada de decisões se tornam viáveis de implementar em contextos do mundo real. ([SWAN](#), 2015)

1.1 Objetivos Gerais

Analisar a democracia líquida, seus potenciais e limitações e implementar um protótipo de sistema, com todos seus requisitos, através do uso da tecnologia *blockchain*.

1.2 Objetivos Específicos

- Estudar o modelo de Democracia Líquida e descrever os requisitos mínimos para sua implementação
- Estudar sistemas de votação eletrônica, seus desafios e soluções
- Estudar a tecnologia *blockchain* e utilizá-la para suprir os requisitos levantados para a implementação da Democracia Líquida
- Desenvolvimento: Implementar em uma *blockchain* o protótipo de um sistema eleitoral atentando-se para as regras da democracia líquida.

1.3 Organização da Monografia

Esta monografia está organizada da seguinte forma.

O Capítulo 2 contém a fundamentação teórica, a origem e os detalhes da Democracia Líquida, da Votação Eletrônica e da *Blockchain*.

O Capítulo ?? descreve as etapas e os materiais utilizados no desenvolvimento do protótipo.

Já o Capítulo 4 discorre sobre os resultados obtidos e os testes realizados com a aplicação, além de apresentar a arquitetura final do projeto.

E finalmente o Capítulo 5 apresenta a conclusão obtida do trabalho e sugestões de pesquisas futuras a partir dos resultados e da pesquisa realizada nesta monografia.

2 Fundamentação Teórica

Nesta seção apresentam-se conceitos, fundamentos e teorias que dão suporte ao presente trabalho. Dentre eles, Democracia Líquida, Votação Eletrônica e Blockchain. Democracia Líquida é o objeto de estudo da monografia, a votação eletrônica é a forma de implementação prática e blockchain é a ferramenta utilizada para tornar esta implementação possível e em seguida produzir uma aplicação segura de democracia líquida.

2.1 Democracia Líquida

O primeiro registro de um modelo de democracia delegativa é de 1884; Lewis Carroll (Charles Lutwidge Dodgson), o autor de Alice no País das Maravilhas, em seu livro *The Principles of Parliamentary Representation* (DODGSON, 1884) descreve o conceito de proporcionar aos candidatos de uma eleição a escolha de: utilizar os votos recebidos para si mesmos, transferi-los para outros candidatos ou não utilizá-los. A proposta era uma forma de lidar com o “desperdício de votos” em eleições nas quais um grupo de representantes deve ser eleito, vale notar portanto que a transitividade dos votos se dava apenas de candidato para candidato, o eleitor não tinha poder de delegação em assuntos específicos, não quebrando com o modelo de democracia representativa. O autor ainda argumenta que não seria praticável deixar o eleitor decidir pra quem essa transferência de votos deveria ocorrer:

O eleitor deve entender que, ao dar seu voto para A, ele dá-lo como sua propriedade absoluta, para usar para si, ou para transferir para outros candidatos, ou deixar sem uso. Se ele não pode confiar no homem, para quem ele vota, ao ponto de acreditar que este vai usar o voto para o melhor, como o eleitor pode confiar nele para retribuí-lo como membro?

(DODGSON, 1884, tradução nossa.)

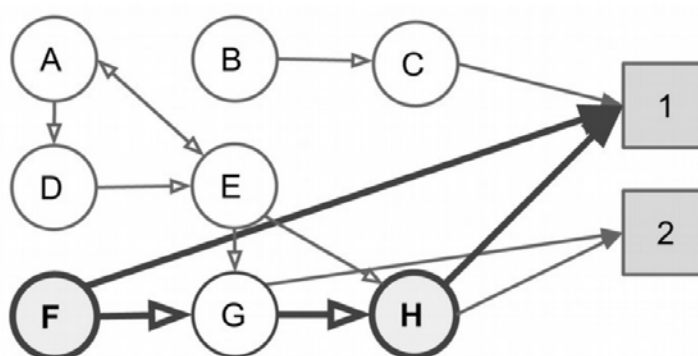
Esta proposta é bem distante do modelo abordado neste trabalho, mas é o marco inicial do pensamento de democracia transitiva, da possibilidade de delegação e de outras formas de representação. O modelo mais difundido atualmente e que será utilizado neste trabalho só foi descrito por Bryan Ford, em 2002, sob o nome de Democracia Delegativa (FORD, 2002) e parte de 6 princípios básicos:

- a) “Escolha de função”: Cada eleitor pode escolher entre ser um “indivíduo” com direito a privacidade, ou assumir o papel de delegado.
- b) “Facilidade para participar”: Deve ser fácil se tornar um delegado, não exigindo fazer uma campanha ou ganhar uma eleição competitiva

- c) “Delegação de autoridade”: Os delegados exercem seu poder em nome de si próprios e daqueles que o delegaram seus votos.
- d) “Privacidade dos Indivíduos”: Os votos feitos por indivíduos, ou seja não-delegados, deve ser secreto para todos.
- e) “Prestação de contas dos delegados”: Os votos de delegados são públicos, tanto para seus “eleitores” quanto para toda a comunidade
- f) “Especialização por re-delegação”: Delegados podem re-delegar os votos recebidos para outro delegado.

Vale ressaltar que a proposta de Ford compila alguns conceitos já formulados anteriormente por [Tullock \(1967\)](#), [Miller \(1969\)](#) e [Lanphier \(1995\)](#), mas nenhum destes autores havia contemplado simultaneamente todas as regras, que hoje compõem o modelo básico de democracia líquida.

Figura 1 – Modelo de Democracia Líquida.



Fonte: [Hardt e Lopes \(2015\)](#).

A Figura 1 mostra alguns casos previstos na democracia líquida, como por exemplo a possibilidade de revogar a delegação a qualquer momento. No exemplo, F delegou para G que por sua vez delegou - utilizando-se do princípio da re-delegação - para H que decidiu sobre o tópico 1. Entretanto F decidiu revogar sua delegação e votar diretamente no tópico 1 ([HARDT; LOPES, 2015](#)).

É interessante notar também que, no exemplo, muitos delegaram seus votos para H, isto é uma tendência em sistemas de democracia líquida, espera-se que H seja um especialista na área e de acordo com seu desempenho mais e mais eleitores deleguem seus votos para este.

Alguns estudos analisaram as vantagens e complexidades do modelo através de diferentes visões e são, portanto, estudos importantes para compreender as necessidades para a implementação do modelo. [Bloembergen, Grossi e Lackner \(2018\)](#) propõem o uso da teoria de jogos para analisar como se dá a acurácia das decisões tomadas em grupo

dentro de um modelo de Democracia Líquida. Já [Christoff e Grossi \(2017\)](#) discorrem sobre dois problemas do modelo: a ocorrência de ciclos de delegação e o efeito de delegações em propostas interdependentes, e propõem modificações para os solucionarem. E por último, [Kahng, Mackenzie e Procaccia \(2018\)](#), através de uma visão algorítmica, analisam se a democracia líquida é capaz de superar a democracia direta no sentido de tomar as melhores decisões.

2.2 Votação Eletrônica

Segundo [Vedel \(2006\)](#) a ideia de melhorar o processo democrático com o uso da tecnologia vem gradualmente sendo desenvolvida desde o final da segunda guerra, mas só depois de algum tempo o primeiro protocolo de votação eletrônica foi proposto por ([CHAUM, 2004](#)), o Voteegrity que permitia ao eleitor a verificação de que seu voto havia sido de fato computado.

Dois dos pais da Democracia Líquida citados na seção 2.1 já previam um futuro onde a votação por meios tecnológicos seria possível. [Tullock \(1967\)](#) afirma que seu modelo de democracia delegativa só seria possível com o desenvolvimento de computadores e afirma que:

Com a eletrônica moderna não há necessidade de todos os representantes se encontrarem no mesmo salão, consequentemente não há um número máximo de representantes. A votação pode ser feita facilmente através de fios, e o processo poderia ser transmitido. No caso extremo, parece não haver razão para que as pessoas que desejem não votem por si mesmas, e assim, preencham seus dias votando a favor e contra as várias propostas. ([TULLOCK, 1967](#), tradução nossa.)

A afirmação pode ser lida com certo anacronismo, mas reflete os avanços tecnológicos da época e a esperança de envolver tecnologia com os processos de decisão cívica. ([MILLER, 1969](#)), contemporâneo também exprime essa expectativa ao prever que em 20 ou 30 anos todas as casas teriam computadores e que cada eleitor poderia registrar votos nestes computadores sobre todos os assuntos políticos da sociedade.

Uma das iniciativas pioneiras de votação eletrônica é o caso da Estônia que desde 2005 permite que seus cidadãos votem pela internet. No começo de maneira tímida, apenas com 2% dos votos computados pela internet, mas mais recentemente em 2015 os votos eletrônicos representavam 30% do total computado ([VASSIL et al., 2016](#)).

Levando em conta os requerimentos de um sistema eletrônico de votação seguro ([WANG et al., 2017](#)) a tecnologia *blockchain* surge rapidamente como solução de implementação por permitir: transparência, segurança contra ataques de negação de serviço e imutabilidade ([HARDWICK; AKRAM; MARKANTONAKIS, 2018](#)).

2.3 Blockchain

Em 2008, um indivíduo (ou grupo) escrevendo sob o nome de Satoshi Nakamoto publicou um artigo (NAKAMOTO, 2008) que descreve um sistema de pagamento eletrônico, descentralizado através de uma rede *peer-to-peer*, sem a necessidade de confiança num intermediador. O artigo introduziu o termo *chain of blocks* que mais tarde o cunhou na palavra muito difundida atualmente *blockchain*.

De acordo com o gráfico de “Ciclo de Expectativas para Tecnologias de Governo Digital” (GARTNER, 2018) elaborado anualmente pela Gartner, a tecnologia que mais provoca expectativas na área de governo digital é a *blockchain*. Um estudo recente de Stanford (GALEN, 2018) sobre o real impacto social da tecnologia afirma que 53% das iniciativas analisadas que utilizam *blockchain* na área de Democracia e Governo, não seriam possíveis sem a ferramenta.

Segundo (ATZORI, 2015) a inovação introduzida pela tecnologia é que os participantes da rede não precisam conhecer ou confiar uns nos outros e as transações são verificáveis sem a necessidade de um ponto de controle ou intervenção humana. O que faz com que a *blockchain* desponte como solução importante para as necessidades de votação eletrônica, mais ainda para um modelo complexo como o de democracia líquida e, portanto, seja escolhida como produto de estudo deste trabalho.

2.3.1 Sistemas distribuídos e o problema dos generais Bizantinos

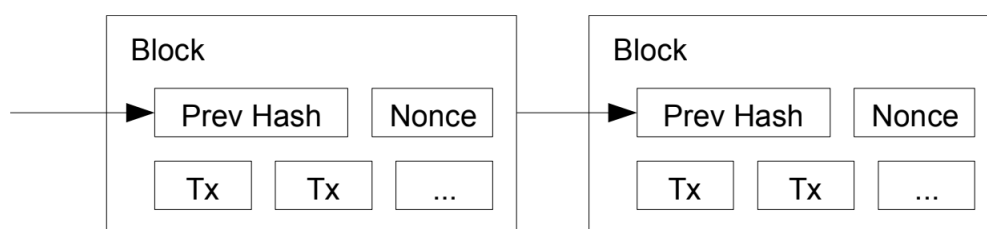
Segundo (BASHIR, 2017), para entender *blockchain* é necessário entender sistemas distribuídos, já que a tecnologia trata-se de um sistema distribuído descentralizado que soluciona um grande problema da área, o problema dos Generais Bizantinos. O problema proposto por Lamport, Shostak e Pease (1982) versa sobre um grupo de generais do exército Bizantino que lideram, cada um, partes diferentes da tropa que planeja atacar ou recuar de uma cidade. Alguns generais podem preferir atacar enquanto outros preferem recuar, o essencial para o sucesso da missão é que não ocorra um ataque parcial que ocasionaria em uma derrota, portanto é necessário chegar a um consenso. O problema surge pelo fato de a comunicação entre os generais ser feita através de mensageiros, portanto, alguns generais podem ser traidores e comunicar mensagens diferentes para os outros generais. Por exemplo, se em um grupo de 5 generais, 2 decidem por atacar e 2 por recuar, o quinto general, no caso um traidor, pode enviar um voto de retirada àqueles generais em favor da retirada, e um voto de ataque ao resto. Na analogia com sistemas distribuídos, cada general é um nó da rede e os generais traidores são nós maliciosos.

Esse problema foi inicialmente solucionado por (LAMPORT; SHOSTAK; PEASE, 1982), mas só teve sua primeira implementação prática com o advento da Bitcoin onde o protocolo de *Proof of Work* foi utilizado como um mecanismo de consenso.

2.3.2 Funcionamento

[Haber e Stornetta \(1990\)](#) propuseram uma estrutura para registrar a data de criação de propriedades intelectuais. A autenticidade era garantida usando funções hash, um tipo de criptografia que transforma dados em código hexadecimal de tamanho fixo, que não podem ser revertidas para recuperar o dado original. Cada novo registro era transformado em um hash que era combinado com o dado original do próximo e transformado em hash novamente e assim subsequentemente. Essa sequência era então divulgada publicamente para que qualquer interessado pudesse verificar.

Figura 2 – Estrutura dos Blocos.



Fonte: [Nakamoto \(2008\)](#).

O que Nakamoto desenvolve a seguir, para registrar transações financeiras, parte deste princípio. Cada bloco novo de transações possui uma função hash do conteúdo do bloco anterior que por sua vez possui uma função hash de seu antecessor e assim até o primeiro bloco da rede, como demonstra a figura 2. O que define se uma *blockchain* é privada ou pública é quem tem permissão de adicionar transações na rede, a *blockchain* responsável pelo método de pagamento Bitcoin criada por Nakamoto é pública.

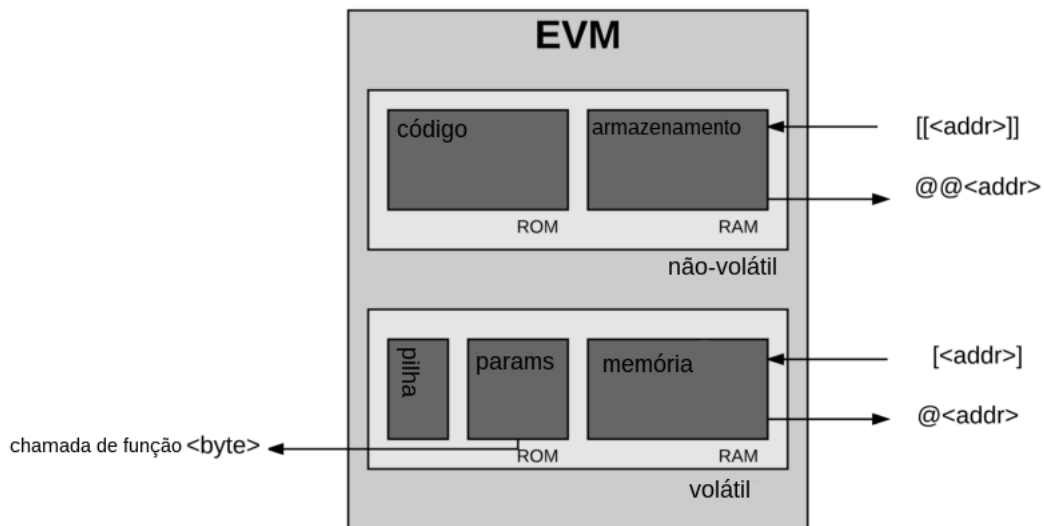
2.3.3 Smart Contracts

[Buterin et al. \(2014\)](#) propuseram o desenvolvimento de uma linguagem Turing-completa que permite o desenvolvimento de algoritmos arbitrários (*smart contracts*) para *blockchain* e aplicações descentralizadas, o que revolucionou o modelo inicial de Nakamoto onde a linguagem era bem limitada e permitia apenas operações básicas. Na prática o conceito de *smart contract* permite que partes que não se confiam estabeleçam um contrato com toda a verificação e auditoria que a *blockchain* permite.

As transações que ocorrem a partir destes contratos são registradas em blocos como as que ocorriam na *blockchain* proposta por Nakamoto, mas com algumas peculiaridades. Uma característica essencial para entender esses contratos inteligentes é a taxa decorrente de cada computação que ocorre nas transações, conhecida como "*gas*". Essa taxa é geralmente toda direcionada para o minerador responsável pelo *Proof of Work* do

bloco da transação. Essas taxas garantem que a rede não seja sobrecarregada de operações de alto custo computacional e que os *smart contracts* retenham-se apenas a operações básicas e verificações.

Figura 3 – Estrutura dos Blocos.



Fonte: Elaborada pelo autor.

Há diversas implementações atuais de *blockchains* com a possibilidade de *smart contracts*, a mais popular e que será alvo da nossa aplicação é a Ethereum. A rede realiza as computações necessárias em sua própria máquina virtual, a *Ethereum Virtual Machine* (EVM). Uma máquina de Turing Completa com uma arquitetura baseada em pilhas. A EVM tem memória volátil, onde os itens são armazenados como matrizes de bytes endereçadas pela palavra. Ao contrário da memória, o armazenamento é não volátil e é mantido como parte do estado do sistema. A EVM armazena o código do programa separadamente, em uma ROM virtual que só pode ser acessada por meio de instruções especiais. Desta forma, a EVM difere da arquitetura típica de von Neumann, na qual o código do programa é armazenado na memória ou no armazenamento, a figura 3 mostra a arquitetura da máquina virtual.

2.4 Trabalhos relacionados

2.4.1 *LiquidFeedback*

LiquidFeedback é um software desenvolvido pelo “Public Software Group” para possibilitar a tomada de decisões democrática, independente do espaço físico e garan-

tindo ao mesmo tempo a igualdade de todos os participantes no processo democrático (BEHRENS et al., 2014).

O *LiquidFeedback* foi concebido e desenhado para apoiar o processo interno de tomada de decisões do Partido Pirata Alemão em 2006, entretanto, atualmente o *LiquidFeedback* é promovido por uma associação sem fins lucrativos - Interaktive Demokratie - e ampliou seus campos de aplicação além de partidos e movimentos políticos. Ele agora é adotado também por organizações da sociedade civil e comunidades locais (CINDIO; STORTONE, 2013).

(CINDIO; STORTONE, 2013), (KLING et al., 2015) e (SWIERCZEK, 2011) discorrem sobre os avanços e atuais desafios da ferramenta que é a primeira do gênero e que junto ao Partido Pirata alemão contribuiu para a popularização da Democracia Líquida. Em julho de 2018 os criadores anunciaram que a ferramenta iria migrar sua tecnologia para a *blockchain* (BEHRENS et al., 2018).

2.4.2 Outras Experiências

Outras experiências, não tão difundidas, de democracia líquida e/ou votação eletrônica utilizando *blockchain* serviram de referência para este trabalho e devem ser citadas. É o caso do Democracy.Earth (EARTH, 2018), iniciativa sem fins lucrativos que mira um papel bem semelhante ao do *LiquidFeedback* de consenso cívico por meio de Democracia Líquida. Um aspecto a se notar aqui é que a aplicação, que iniciou seu desenvolvimento em 2012 de forma convencional e centralizada, já trabalha na migração e futuro lançamento do software baseado em *blockchain* desde 2015. Já a Votem empresa americana caso de estudo em Galen (2018) já opera como ferramenta de votação eletrônica para algumas eleições municipais nos Estados Unidos, permitindo aos cidadãos votar seguramente e de forma auditável sem sair de casa. Serra Leoa, por sua vez, foi pioneiro ao registrar 70% dos votos de sua eleição presidencial em 2018 na *blockchain* fornecida pela empresa Agora (AGORA, 2018), o que permitiu a recontagem e a validação dos votos.

3 Metodologia

Neste capítulo estão descritos as ferramentas utilizadas para o desenvolvimento da aplicação, como estas se integram e as etapas necessárias.

3.1 Tecnologias e Ferramentas Utilizadas

3.1.1 *Solidity*

Solidity é uma linguagem de alto nível orientada a contratos. É utilizada para implementar Smart Contracts e executar em uma *Ethereum Virtual Machine* (EVM). A linguagem é atualmente a principal forma de se desenvolver para *blockchain*, possui tipagem forte, suporta herança de classes, bibliotecas tipos definidos pelo usuário.

Figura 4 – Código em *Solidity*.

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Fonte: [Solidity \(2018\)](#)

A Figura 4 apresenta um exemplo de código escrito na linguagem, um contrato para armazenamento simples de um número. Ao invés da declaração de classes como nas linguagens orientadas a objetos, declara-se contratos. No exemplo, verifica-se alguns itens importantes da linguagem, a variável global *storedData* é chamada de "estado" e pode ser considerada como um item no banco de dados, sua definição e retorno estão definidos nas funções *set()* e *get()*.

3.1.2 *Truffle* e *Ganache*

Para acelerar o desenvolvimento de aplicações descentralizadas uma ferramenta importante é o *framework Truffle*, que permite que o desenvolvedor escreva testes de unidade automatizados e um ambiente repleto de funcionalidades que facilitam o desenvolvimento.

Figura 5 – Funcionamento da ferramenta *Ganache*.

```

ganache-cli
lucasqdrseIS0210 ~/Documents/LiquidTCC master ganache-cli
Ganache CLI v6.1.8 (ganache-core: 2.2.1)

Available Accounts
=====
(0) 0xcac44dee233acd71283628ace9966bd29091c27e (~100 ETH)
(1) 0x8424022b63ca16cbb40c11c8f13a5381e3688569 (~100 ETH)
(2) 0x708092a871395a58efa0663143eee0e55c104507 (~100 ETH)
(3) 0x7a29e4d737cf2c77c75ee18c7bc5c6d2b139aa85 (~100 ETH)
(4) 0xf45adc8dbf6bf859b1f494d8f1da4170cb9b13d (~100 ETH)
(5) 0xd34abe02b911f61d7f16630c202ab0da3a517e94 (~100 ETH)
(6) 0xae6b5ec7df40d64aa69befb76adaba8c5fae03a3 (~100 ETH)
(7) 0x4e91518df931405a6f41f85a596b54d97a83c6fe (~100 ETH)
(8) 0x185df648a10ae150d4b6024257f964d20cc31088 (~100 ETH)
(9) 0x49d6d12527a6aa6a0ed24d89726d84b47dcd37c6 (~100 ETH)

Private Keys
=====
(0) 0xc58866f18ae6b0d0165b0294284d4a3fe139c568fde95b3945dbca401a87dda
(1) 0x04f18d95c988f517be32087e57d16cde5fe5f17a01f67bf4448dd96b28514aca
(2) 0x01e78d4817ac004eeefc93aec6747bf536174a0bd176dd6377243beac08a76252
(3) 0xc4b53b4dc32ff3e1d81d259aad0c4c9c756b5544e40843c9fcb8aa879d2ced
(4) 0xc09afb0336857bd582854206507139e44db56eeb1a5357bd79aee2701cde8637
(5) 0x9868da402c12738c256521dfd9cdda9bc51566d2672c8d3f0b5682fa01440197
(6) 0x2c01ed19c66860a5d2d509d79ebec83924908a4496ac0adeb20715ba71db7829
(7) 0xdb8f4580665f8414052c553f357ba1fb72ebc2f5ade07a24ddb35bf652e02fdd
(8) 0xb0ab8a91beb752c8befb85bf56df680b946399de08c9591b1b49129c80200c28
(9) 0x60f79a3008802373b3d5d4a3880c55dd40fbef3b6f65d00665b74a164e91e6e

HD Wallet
=====
Mnemonic: latin voyage guess priority height explain rug glue damage perfect hair wild
Base HD Path: m/44'/60'/0'/0/{account_index}

Gas Price
=====
20000000000

Gas Limit
=====
6721975

Listening on 127.0.1:8545

```

Fonte: Elaborada pelo autor.

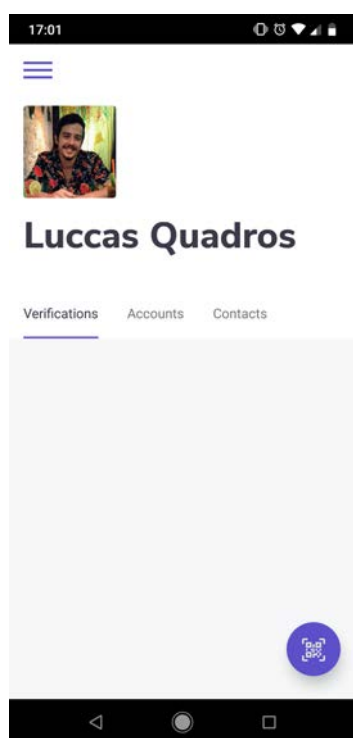
Para executar os testes escritos com o auxílio do *Truffle* é necessário que a aplicação esteja rodando em um ambiente controlado e, portanto, não em uma *blockchain* pública. Tendo isto em vista, o *Ganache* permite a criação de uma *blockchain* local para testes e desenvolvimento antes da migração da aplicação para uma rede pública. A aplicação cria usuários simulados, e exibe as chaves públicas, privadas e a quantidade de *Ethers* destes, como mostra a figura 5. O desenvolvedor pode assim verificar a quantidade de *gas* empenhada em cada transação e vasculhar possíveis falhas de segurança de seus contratos.

3.1.3 Metamask e uPort

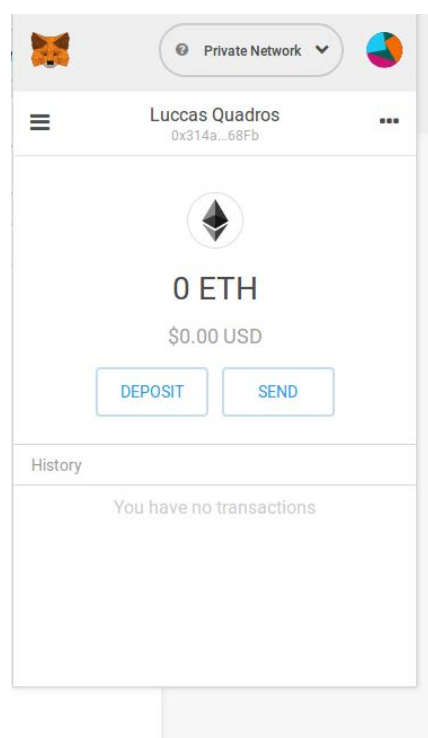
Metamask é responsável por fazer a ponte entre navegadores convencionais e aplicações descentralizadas. Permite que usuários convencionais acessem aplicações presentes na *blockchain* pública Ethereum sem a necessidade de o usuário ser um nó da rede, facilitando a entrada de novos usuários à aplicação e o desenvolvimento. A figura 6b mostra a interface com o usuário da ferramenta em sua versão para o navegador *Firefox*.

Ainda pensando em melhorar a experiência com o usuário, o uPort surge como solução para credenciais de acesso em aplicações descentralizadas, o protocolo utiliza o

Figura 6 – Interfaces para o usuário de ferramentas



(a) uPort no celular.



(b) Metamask extensão ao navegador.

Fonte: Elaborada pelo autor.

telefone celular do usuário para armazenar a chave privada e habilitar transações em aplicações desenvolvidas na *blockchain* Ethereum. Desta forma a identidade do usuário é mantida segura sem precisar ser armazenada em um local centralizado e ainda garante-se uma verificação dupla de segurança através da aplicação móvel, apresentada na figura 6a.

3.1.4 InterPlanetary File System

Conhecido popularmente como IPFS trata-se de um protocolo que permite o armazenamento e compartilhamento de arquivos de forma distribuída em uma rede *peer-to-peer*. A ferramenta nasceu baseada no protocolo da Bitcoin e hoje é amplamente utilizada para armazenar informações de aplicações descentralizadas, já que através de endereços *hashes* diminui o custo de armazenamento nos blocos da rede. É comum, consequentemente, que arquivos grandes de uma aplicação em *blockchain* como textos, imagens, vídeos e outras mídias sejam armazenados utilizando o protocolo.

3.2 Métodos e Etapas

A primeira fase deste trabalho concentrou-se no levantamento bibliográfico sobre Democracia Líquida. É essencial para o desenvolvimento de um *smart contract* que se

entenda todos os requisitos do modelo a ser implementado. A partir daí é necessário garantir que todas as regras do modelo estarão presente no contrato.

A fase seguinte relacionou-se com a tecnologia *blockchain*, desde o levantamento teórico e a compreensão dos protocolos envolvidos até a parte mais prática, onde foi essencial o estudo das tecnologias que auxiliam o desenvolvimento de aplicações descentralizadas. Dado que é uma área de desenvolvimento recente, algumas ferramentas se encontram em estágios muito iniciais e não eram passíveis de se utilizar neste trabalho.

A partir daí o foco do desenvolvimento foi, com o uso da linguagem solidity, implementar de forma segura e eficiente todos os requisitos levantados na primeira fase. Para agilizar os testes e o desenvolvimento nesta etapa inicial do projeto a IDE online da linguagem Solidity, a Remix ([REMIX, 2018](#)) foi essencial. Ela permitiu que não fosse necessário se preocupar com instalações ou ambientes complexos, já que o desenvolvedor tem todas as opções online na interface web.

Depois de definido e testado o *smart contract* foi necessário integrá-lo com um *front-end*, ou seja, criar a interface que se comunica com as funções implementadas no contrato e que o usuário interage durante todos os processos. Nesta etapa foi necessário observar os padrões atuais de desenvolvimento web em relação a experiência do usuário e, para a comunicação com o *smart contract*, o uso da biblioteca em *javascript* Web3.js que proporciona ao desenvolvedor a chamada do que está presente no contrato.

Com o *smart contract* implementado e devidamente conectado com o *front-end* chega-se a penúltima etapa do desenvolvimento, a mais extensa do projeto. Nesta deu-se todo o suporte a aplicação para que funciona-se em uma rede *blockchain* real, sendo essencial o uso das ferramentas citadas na seção 3.1.2. A extensão da etapa é justificada pela fase de testes, de muita importância no desenvolvimento de aplicações descentralizadas.

Somente na última etapa do desenvolvimento que dois módulos foram adicionados a aplicação. O referente ao uPort, para garantir a integridade da identidade dos usuários e o uso do protocolo IPFS, para reduzir o custo computacional observado na etapa anterior e tornar a aplicação de fato viável.

4 Testes e Resultados

Figura 7 – Exemplo de transação pública verificada através do Etherscan

The screenshot displays the 'Transaction Information' page on Etherscan. The interface includes tabs for 'Overview', 'Event Logs (1)', and 'Comments'. The transaction details are as follows:

- TxHash:** 0xa7807117f7efbfabedfb3084628e72c9eab334dc32e95aa83eb961f6ba500985
- TxReceipt Status:** Success
- Block Height:** 6750719 (10 Block Confirmations)
- TimeStamp:** 3 mins ago (Nov-22-2018 08:52:55 AM +UTC)
- From:** 0x3425d6f843d878ce555a67880c518fc10273a9c2
- To:** Contract 0x6c8dce6d842e0d9d109dc4c69f35cf8904fc4cbf (Etheremon_Energy) ✓
- Value:** 0 Ether (\$0.00)
- Gas Limit:** 53850
- Gas Used By Transaction:** 35900 (66.67%)
- Gas Price:** 0.000000004 Ether (4 Gwei)
- Actual Tx Cost/Fee:** 0.0001436 Ether (\$0.02)
- Nonce & {Position}:** 98 | {147}
- Input Data:**
 - Function: claimEnergy()
 - MethodID: 0x2ab34a91

At the bottom, there is a 'Private Note' section with a message: '<To access the Private Note Feature, you must be [Logged In](#)>'. Navigation links for 'Buy' and 'Loan' are visible in the top right corner.

Fonte: Elaborada pelo autor.

O resultado do projeto foi uma aplicação funcional, que permite ao usuário acessar uma aplicação web convencional e ter toda a segurança de uma aplicação descentralizada. É importante ressaltar que ainda que a identidade do eleitor possa ser mantida em sigilo, todas as transações que ocorrem na aplicação, a partir do momento que ela está hospedada em uma *blockchain* pública, podem ser verificadas por qualquer um através de aplicações como o Etherscan como mostra a figura 7, fornecendo assim transparência para as votações.

Para o usuário convencional e não muito atento às técnicas da aplicação, a interface é simples e garante um fácil uso independente do conhecimento técnico na área de *blockchain*. Um exemplo da interface para a votação de uma proposta simples está na figura 8, na qual verifica-se a possibilidade votar contra ou a favor de uma proposta ou ainda delegar para um outro usuário.

Como a aplicação não chegou a ser hospedada de fato na rede Ethereum, devido

Figura 8 – Interface para a votação de uma proposta

TCC Democracia Líquida - Luccas Quadros

Proposta #12: Comprar uma máquina de café?

A Favor! Contra

Delegar para...

- Fulano Especialista
- Zé Ninguém
- Maria Silva
- Cícrono das Neves
- Fernando Fernandes
- Jânio Quadros

Fonte: Elaborada pelo autor.

as taxas que cada transação do protótipo geraria, os testes ficaram restritos a *blockchain* local criada para este fim. Nestes testes foi possível observar o alto custo computacional que a tentativa de hospedar imagens no *smart contract* gera, o que seria inviável em um ambiente real e portanto ressalta-se a importância do protocolo IPFS. Além disso, em uma rede local como a utilizada, um ataque de 51%, no qual se altera a maioria dos nós da rede e desta forma forja-se transações, seria muito possível pela pouca quantidade de nós, ou seja, uma falha de segurança grave caso este fosse a rede final desejada para a aplicação. Caso a aplicação tivesse de fato sido hospedada na rede Ethereum este tipo de ataque seria praticamente impossível pelo custo computacional dada a quantidade de nós. Por fim vale ressaltar que a aplicação tem um tempo alto de latência em redes reais, devido ao protocolo *Proof of Work*, o que não ocorre em ambientes de teste.

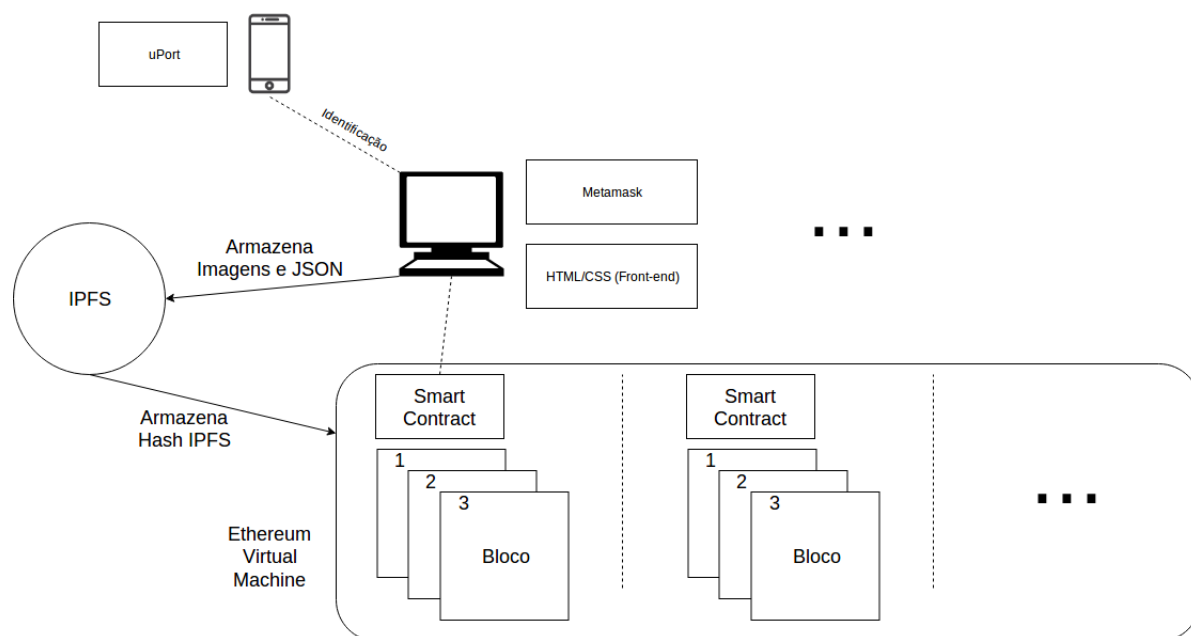
A seguir apresenta-se a arquitetura da aplicação, descrevendo como os módulos se unem e mais detalhes da aplicação final.

4.1 Arquitetura da Aplicação

A arquitetura do projeto pode ser observada na figura 9, o usuário interage com um web site padrão, por meio de qualquer navegador com a extensão MetaMask instalada. Para este *layout* foram utilizadas as tecnologias atuais de HTML/CSS e Javascript. Qualquer transação como votar, delegar ou fazer uma proposta é registrado, a partir do *Smart Contract* na rede *blockchain*. Para os testes deste protótipo esta rede é privada e gerada com o auxílio da ferramenta *Ganache*.

Para garantir a sua identidade é necessário que o votante habilite suas transações

Figura 9 – Arquitetura aplicação descentralizada



Fonte: Elaborada pelo autor.

através do aplicativo uPort que deve ser instalado em seu celular, através dessa verificação de duas vias a segurança das decisões é reforçada.

Informações do usuário, imagens, textos e anexos de propostas não são viáveis de armazenamento nos blocos já que consumiriam muito processamento, portanto, todas essas informações são armazenadas através do protocolo IPFS de forma distribuída. Na *blockchain* armazena-se apenas o endereço *hash* das informações.

O *Smart Contract*, presente em todos os nós e inalterável, garante que outras informações não serão adicionadas no bloco, que um eleitor não votará mais de uma vez, entre outras violações.

5 Conclusão

O presente trabalho apresenta ferramentas e etapas para a implementação de conceitos recentes ou pouco pesquisados. O objetivo foi desenvolver, com as tecnologias atuais, uma aplicação de democracia líquida simples e segura. Ainda que não muito popular, existe um grande espaço para pesquisa e validação de experiências de democracia líquida, que tem potencial para aumentar e melhorar a participação em tomadas de decisões, seja pública ou privada. A tecnologia abordada neste estudo, por sua vez, é considerada por muitos revolucionária, mas ainda não atingiu todo o seu potencial, assim aplicações na indústria e em processos estatais utilizando *blockchain* são esperadas nos próximos anos. O código de todo o projeto desenvolvido foi disponibilizado no Github, sob licença MIT, que garante permissão de cópia, reprodução, distribuição, publicação e venda para qualquer pessoa, o que vai de encontro com a comunidade da *blockchain* que preza pelo *software* livre e devido a isso foi de grande ajuda para o desenvolvimento deste trabalho.

5.1 Trabalhos futuros

Para trabalhos futuros, existem diversos caminhos a se explorar, tanto outras aplicações de democracia e votação eletrônica, como a aplicação de *blockchain* em outras áreas de necessidade humana; as próprias ferramentas utilizadas neste estudo, por si só, garantem conteúdo suficiente para uma pesquisa extensa. Vale citar que a plataforma base para a aplicação, Ethereum, está atualmente migrando do protocolo *Proof of Work* para um protocolo conhecido como *Proof of Stake*, que garantiria taxas menores para as transações e um menor gasto energético, este que é hoje a maior preocupação dos pesquisadores da área.

Um modelo interessante relacionado à democracia e votação eletrônica que surgiu durante as pesquisas deste trabalho e também pode ser explorado através de uma aplicação *blockchain* é o voto quadrático (LALLEY; WEYL, 2018), uma forma de ter diferentes pesos para votos dos eleitores além das delegações.

Na seção 2.4 desta monografia outras aplicações de democracia líquida por meio de *blockchain* foram citadas, mas nenhuma delas está em funcionamento em uma *blockchain* pública. O que deve se mostrar um objeto de estudos interessante no futuro é como essas ferramentas vão se adaptar às possíveis complicações que um uso mais intenso do modelo de Democracia Líquida pode gerar.

Referências

- AGORA. *Agora Whitepaper*. 2018. Disponível em: <<https://www.agora.vote/>>.
- ATZORI, M. Blockchain technology and decentralized governance: Is the state still necessary? 2015.
- BASHIR, I. *Mastering Blockchain*. [S.l.]: Packt Publishing Ltd, 2017.
- BEHRENS, J.; KISTNER, A.; NITSCHKE, A.; SWIERCZEK, B. *The principles of LiquidFeedback*. [S.l.]: Interaktive Demokratie, 2014.
- BEHRENS, J.; KISTNER, A.; NITSCHKE, A.; SWIERCZEK, B. The liquidfeedback blockchain. *The Liquid Democracy Journal*, v. 6, 2018.
- BLOEMBERGEN, D.; GROSSI, D.; LACKNER, M. On rational delegations in liquid democracy. *arXiv preprint arXiv:1802.08020*, 2018.
- BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.
- CHAUM, D. Secret-ballot receipts: True voter-verifiable elections. *IEEE security & privacy*, IEEE, v. 2, n. 1, p. 38–47, 2004.
- CHRISTOFF, Z.; GROSSI, D. Binary voting with delegable proxy: An analysis of liquid democracy. *arXiv preprint arXiv:1707.08741*, 2017.
- CINDIO, F. D.; STORTONE, S. Experimenting liquidfeedback for online deliberation in civic contexts. In: SPRINGER. *International Conference on Electronic Participation*. [S.l.], 2013. p. 147–158.
- CLARKE, P. B.; FOWERAKER, J. *Encyclopedia of democratic thought*. [S.l.]: Routledge, 2003. 238–248 p.
- CONSTANT, B. *A liberdade dos antigos comparada à dos modernos*. [S.l.]: Editora Atlas SA, 2015.
- CUNHA, L. G.; BUENO, R. d. L. d. S.; OLIVEIRA, F. L. d.; SAMPAIO, J. O.; RAMOS, L. d. O.; PIERI, R. G. d.; PEREIRA, A. *Relatório IPCLBrasil-1º semestre/2015*. [S.l.], 2015.
- DODGSON, C. L. *The principles of parliamentary representation*. [S.l.]: Harrison and Sons, 1884.
- EARTH, D. *The Social Smart Contract*. 2018. Disponível em: <<https://www.democracy-earth/>>.
- FORD, B. Delegative democracy. *Manuscript*. <http://www.brynosaurus.com/deleg/deleg.pdf>, 2002.
- GALEN, D. *SOCIAL IMPACT*. Tese (Doutorado) — Stanford Graduate School of Business, 2018.

- GARTNER. *Top Trends from Gartner Hype Cycle for Digital Government Technology*. 2018. Disponível em: <<https://www.gartner.com/smarterwithgartner/top-trends-from-gartner-hype-cycle-for-digital-government-technology-2018/>>.
- HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. In: SPRINGER. *Conference on the Theory and Application of Cryptography*. [S.l.], 1990. p. 437–455.
- HARDT, S.; LOPES, L. C. Google votes: A liquid democracy experiment on a corporate social network. 2015.
- HARDWICK, F. S.; AKRAM, R. N.; MARKANTONAKIS, K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. *arXiv preprint arXiv:1805.10258*, 2018.
- KAHNG, A.; MACKENZIE, S.; PROCACCIA, A. D. Liquid democracy: An algorithmic perspective. In: *Proceedings of the 32nd AAAI Conference on Artificial Intelligence (AAAI)*. Forthcoming. [S.l.: s.n.], 2018.
- KAYE, M.; SPATARO, N. Redefinindo a democracia: sobre um sistema democrático concebido para o século xxi e sobre como mudar permanentemente a democracia. Tribunal Superior Eleitoral, 2016.
- KLING, C. C.; KUNEGIS, J.; HARTMANN, H.; STROHMAIER, M.; STAAB, S. Voting behaviour and power in online democracy: A study of liquidfeedback in germany's pirate party. *arXiv preprint arXiv:1503.07723*, 2015.
- LALLEY, S. P.; WEYL, E. G. Quadratic voting: How mechanism design can radicalize democracy. In: *AEA Papers and Proceedings*. [S.l.: s.n.], 2018. v. 108, p. 33–37.
- LAMPORT, L.; SHOSTAK, R.; PEASE, M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, ACM, v. 4, n. 3, p. 382–401, 1982.
- LANPHIER, R. A model for electronic democracy. *Manuscript*. <http://robla.net/1996/steward>, 1995.
- MESQUITA, B. B. D.; SMITH, A. The dictator's handbook. *Why Bad Behavior Is Almost Always Good Politics*. Public Affairs, New York, 2011.
- MILLER, J. C. A program for direct and proxy voting in the legislative process. *Public choice*, Springer, v. 7, n. 1, p. 107–113, 1969.
- NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008.
- OLSON, M. Dictatorship, democracy, and development. *American political science review*, Cambridge University Press, v. 87, n. 3, p. 567–576, 1993.
- REMIX. *Remix - Solidity IDE*. 2018. Disponível em: <<https://remix.ethereum.org/>>.
- SOLIDITY. *Solidity Documentation*. 2018. Disponível em: <<https://solidity.readthedocs.io/en/v0.4.25>>.
- SWAN, M. *Blockchain: Blueprint for a new economy*. [S.l.]: "O'Reilly Media, Inc.", 2015.

SWIERCZEK, B. Five year of liquid democracy in germany. *The Liquid Democracy Journal*, v. 1, p. 2014–03, 2011.

TULLOCK, G. *Toward a mathematics of politics*. [S.l.]: University of Michigan Press, 1967. 144–157 p.

VASSIL, K.; SOLVAK, M.; VINKEL, P.; TRECHSEL, A. H.; ALVAREZ, R. M. The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. *Government Information Quarterly*, Elsevier, v. 33, n. 3, p. 453–459, 2016.

VEDEL, T. The idea of electronic democracy: Origins, visions and questions. *Parliamentary Affairs*, Oxford University Press, v. 59, n. 2, p. 226–235, 2006.

WANG, K.-H.; MONDAL, S. K.; CHAN, K.; XIE, X. A review of contemporary e-voting: Requirements, technology, systems and usability. *Data Science and Pattern Recognition*, v. 1, n. 1, p. 31–47, 2017.