UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ

Matheus Francisco Batista Machado

COLETOR DE MOEDAS METÁLICAS COM COMPENSAÇÃO EM CRIPTOMOEDAS

Araranguá

2019

Matheus Francisco Batista Machado

COLETOR DE MOEDAS METÁLICAS COM COMPENSAÇÃO EM CRIPTOMOEDAS

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina para obtenção de grau em Bacharel em Engenharia de Computação.
Orientador: Prof. Dr. Martín Vigil

Araranguá

2019

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Machado, Matheus Francisco B
COLETOR DE MOEDAS METÁLICAS COM COMPENSAÇÃO EM CRIPTOMOEDAS / Matheus Francisco B Machado ; orientador, Martín Vigil, 2019.
58 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Engenharia de Computação, Araranguá, 2019.

Inclui referências.

1. Engenharia de Computação. 2. Quiosque inteligente. 3. Criptomoeda;. 4. Moedas metálicas. 5. IOTA. I. Vigil, Martín . II. Universidade Federal de Santa Catarina. Graduação em Engenharia de Computação. III. Título.

Matheus Francisco Batista Machado

COLETOR DE MOEDAS METÁLICAS COM COMPENSAÇÃO EM CRIPTOMOEDAS

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de "Bacharel em Engenharia de Computação", e aprovado em sua forma final pela Universidade Federal de Santa Catarina.

Araranguá, 25 de Junho 2019.

Prof. Dr. Fabrício Ourique
Coordenador do Curso

Banca Examinadora:

Prof. Dr. Martín Vigil
Orientador

Prof. Dr. Tiago Weber

Juliano Almeida

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pelas oportunidades e pessoas que conheci durante os anos de graduação.

Agradeço à minha família, em especial aos meus pais, Martin Machado e Gisele Machado, que ao longo destes anos, foram compreensivos com a minha ausência e sempre me incentivaram a seguir em frente.

Agradeço a minha namorada, Mayara Stein, por estar junto comigo ao longo desses difíceis 4 anos. Foram maravilhosos momentos que passamos juntos. Agradeço pela paciência que você teve comigo nesses momentos, por estar sempre me apoiando nas minhas decisões e me incentivando para ser uma pessoa melhor a cada dia.

Aos meus amigos que longe ou perto demonstraram o verdadeiro significado de amizade, por compartilharem momentos incríveis comigo e pela parceria durante todo estes anos. Em especial, ao Augusto Lutz por ser um ótimo companheiro de casa durante os 5 anos, muitos bons momentos levarei comigo. Também não posso esquecer do Risadinha e seu Onix (Gabriel Medeiros) um grande amigo que ajudou nas horas mais difíceis. E aos meus amigos do time Ex-amigos do luanzinho, Gabriel Domene e Manão (Luan Rodrigues) muito obrigado pelas maratonas de programação e parcerias em trabalhos. Também agradeço ao meu amigo Luanzinho que nos inspirou para o nome do time da maratona e também me ajudou em momentos muito importantes que levarei comigo para o resto da vida.

Agradeço aos professores pelos ensinamentos, em especial, o Martin Vigíl, que aceitou o convite para participar deste trabalho, me orientando para sua melhoria. O professor Cristian Cechinel que me concedeu o projeto de iniciação científica, em que pude aprender muito. E aos professores Álvaro Junio Pereira Franco e Gustavo Mello que me incentivaram a participar de maratonas de programação.

Agradeço a todos os ex-membros da Empresa Júnior de Engenharia de Computação (EJEC) por proporcionar um enorme aprendizado sobre empreendedorismo e trabalho em equipe.

Não poderia esquecer do Arara Makerspace, os membros e o professor Marcelo Zanin, por acolher a ideia e tirar o projeto do papel.

Com o projeto foi possível vivenciar um ano de muito aprendizado, companheirismo e dificuldades. Que levarei para o resto da vida.

Por fim, gostaria de agradecer à Universidade Federal de Santa Catarina pela oportunidade de ter vivenciado tudo isso. E a todos que de alguma forma, direta ou indiretamente participaram da realização desse projeto.

Acredite sempre no seu potencial, você é capaz de fazer tudo o que quiser e chegar a qualquer lugar. Basta que se empenhe e acredite sempre que pode e é merecedor de conquistar seus sonhos e objetivos!

RESUMO

De acordo com a Federação Brasileira de Bancos, o Banco Central Brasileiro emitiu uma nota informando que 32% das moedas emitidas em 2015 estavam fora de circulação, devido a retenção das moedas. Alguns estudos relatam que a população não possui a cultura de portar moedas, juntando-as em gavetas, cofrinhos, carro e não colocam em meio circulante. Além dos viajantes, que deixam o país sem trocar as moedas. Algumas soluções foram implementadas por exemplo, as doações de moedas para instituições de caridade, máquina cata moeda e trocas de moedas por produto. Mas, as soluções citadas apresentam algumas desvantagens. Por exemplo, nas doações pode-se citar a falta de transparência, pois não é possível verificar se o valor doado é de fato transferido para uma instituição de caridade. A máquina de cata moeda, o cliente poderá trocar apenas moedas por produtos ou seviços fornecido pelo comércio. Levando isso em conta, o presente trabalho propõe um modelo de quiosque inteligente capaz de coletar moedas metálicas por criptomoedas. Isso é possível devido o uso de uma interface de interação e um hardware utilizando um Raspberry PI 3 e um display LCD touch 3.5 polegadas. Ao final, fez-se testes para verificar o funcionamento integral do sistema. O sistema foi capaz de realizar depósitos e transferências com todos os requisitos levantados. Além disso, foi possível desenvolver um protótipo com baixo custo. A partir do exposto, conclui-se que o coletor de moedas desenvolvido pode amenizar com o problema de falta de moedas no mercado, pelo fato do estabelecimento conseguir reter as moedas inseridas no quiosque, em troca o cliente recebe suas criptomoedas em suas contas. Além de oferecer ao mercado um produto de baixo custo.

Palavras-chave: Quiosque inteligente; Criptomoeda; Moedas metálicas; IOTA

ABSTRACT

According to the Brazilian Federation of Banks, the Brazilian Central Bank issued a note stating that 32% of coins issued in 2015 were out of circulation due to currencies retention. Some studies report that the population does not have the culture of carrying coins, joining them in drawers, piggy banks, car and do not put in circulating medium. Besides travelers, they leave the country without exchanging the coins. Some solutions have been implemented for example, donations of coins to charities, coin tasting machine and currency exchanges by product. However, the solutions cited have some drawbacks. For example, in donations one can cite the lack of transparency because it is not possible to verify if the amount donated is actually transferred to a charity. The coin collecting machine, the customer can exchange only coins for products or services provided by the trade. Taking this into account, the present work proposes a model of intelligent kiosk capable of collecting coins by crypto-coins. This is possible due to the use of an interaction interface and hardware using a Raspberry PI 3 and a 3.5 inch touchscreen LCD display. At the end, tests were carried out to verify the complete functioning of the system. The system was able to make deposits and transfers with all requirements raised. In addition, it was possible to develop a prototype with low cost. From the foregoing, it can be concluded that the developed coin collector can soften the problem of lack of coins in the market, because the establishment is able to retain the coins inserted in the kiosk, in exchange the customer receives their crypto coins in their accounts. In addition to offering the market a low cost product.

Keywords: Smart kiosk; Blockchain; Cryptocurrency; IOTA

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

De acordo com (AMATO, 2004), moedas fiduciárias refere-se as cédulas e moedas que estão em circulação, que não possuem nenhum valor intrínsico. Confiamos que o valor determinado nas moedas e notas representam a exata quantia de dinheiro. O autor ainda menciona que a moeda fiduciária tem curso forçado por lei. Além de possuir aceitação garantida. É utilizada principalmente como instrumento de troca, reserva de valor e unidade de referência ou de cálculo do valor.

No Brasil, o Banco Central tem por finalidade garantir a estabilidade do poder de compra da moeda, determinar a quantidade de cédulas e moedas a serem produzidas e garantir a circulação das mesmas (Banco Central, 2019). O Banco Central do Brasil possui poder sobre todo o dinheiro da economia, desde as reservas bancárias aos valores retidos pela população (SILVA, 2003). Segundo (MESQUITA, 2017) o valor médio de emissão de uma única moeda metálica equivale a R$ 0,38 centavos.

De acordo com (MATIAS-PEREIRA, 2010) a moeda surgi da necessidade do ser humano utilizar um meio monetário à realidade de sua economia, assim criaram diversas formas para trocas de produtos e serviços. Com o tempo foi criada uma moeda padrão que desempenha a função de intermédio de troca, isolar venda de compra, unidade contábil, denominador de valores, padrão de pagamento e a possibilidade de estoque de valor (MATIAS-PEREIRA, 2010). Segundo (MATIAS-PEREIRA, 2010) a moeda tornou-se importante na economia pela função de intermédio de trocas sem a necessidade da dupla coincidência de vontades. Assim ocorre o aumento da faixa de troca.

De acordo com a Federação Brasileira de Bancos, o Banco Central Brasileiro emitiu uma nota informando que 32% das moedas emitidas em 2015 estavam fora de circulação, devido a retenção das moedas. Alguns estudos relatam que a população não possui a cultura de portar moedas, juntando-as em gavetas, cofrinhos, carro, e não colocam em meio circulante. Apesar da principal função das moedas ser circular na economia (MATIAS-PEREIRA, 2010).

Os diretores de operação da Federação Brasileira de Bancos explicam que esse ato de reter moedas e não utilizá-las acaba abalando a economia nacional. Principalmente aos comerciantes pela restrição da circulação da mesma (FEBRABAN – Federação Brasileira de Bancos, 2016). Segundo (MESQUITA, 2017) desde o início do plano real até 2017, foram emitidos mais de 26 bilhões de moedas em um país que possui

aproximadamente 207,7 millhões de habitantes. Sendo uma média de 125,7 moedas para cada cidadão brasileiro. Portanto, se a quantidade de moedas retidas estivesse em circulação certamente o mercado não enfrentaria problemas com falta de troco (MESQUITA, 2017).

Segundo (MESQUITA, 2017) o Banco Central do Brasil em 2018 planejou colocar em circulação mais de 423.237.600 de moedas na tentativa de solucionar o problema de falta de moedas circulantes. Custando aos cofres públicos mais de 155 milhões de reais equivalente apenas ao custo de produção. O Banco Central informou que a falta de moeda no comércio aconteceu devido o período inflacionário que levou as moedas perderem poder de compra, fazendo a população acreditar que as moedas não possuiam valor(MATIAS-PEREIRA, 2010). E as restrições orçamentárias da produção de moedas que ocorreram no período de 1998 á 2000, ocasionando a falta no suprimento.

Outra situação propricia à retenção de moedas são os viajantes estrangeiros que não conseguem trocar suas moedas locais antes de deixar o país. Isso acontece porque geralmente são valores pequenos que as casas de câmbio não realizam a troca (Oliveira, Marina e Macena, Thaís , 2015). Consequentemente, essas moedas deixam o país definitivamente e portanto saem de circulação.

Algumas soluções foram adotadas por comerciantes para resolver o problema de falta de moedas. Por exemplo, a adoção de máquinas cata moedas que realizam a troca de moedas por cupom com bônus de 2 a 10% de desconto em compra. Outra solução é o fornecimento de produtos como bônus para pessoas que realizam os pagamentos em moedas. Pode-se citar também o troco solidário que tem sido adotada por farmácias e supermercados. Consiste basicamente em convidar o cliente a doar o troco de sua compra para entidades filantrópicas, como ocorre nos supermercados Giassi e Angeloni. Todavia, a falta de transparência gera um grande problema. Devido a falta de rastreabilidade do valor doado. Além das empresas não divulgar ou informar como acontece a tranferência. Cita-se como exemplo as doações feitas a Brumadinho, os canais de doações não permitem identificar o destino da transferência. Com isso, golpistas criaram canais falsos para doações com a intenção de transferir o dinheiro arrecadado para a própria conta (TRINDADE,Rodrigo, 2019,).

Com os avanços tecnológicos surgiram diversos meios de pagamentos virtuais que transformaram os meios de transações monetárias. As transações poderiam ser realizadas a qualquer momento e sem a necessidade de moedas físicas. Pode-se citar como exemplo os ambiente bancário online, a internet banking e o banco digital. Essas inova-

ções tecnológicas não só atendem os serviços solicitados pelos clientes como representam o valor agregado, ao reduzirem custos operacionais e ampliarem a disponibilidade dos serviços bancários (JESUS; ÓRGÃOS, 2017). As inovações tecnológicas citadas possui um ambiente centralizado e controlado pelo mesmo emissor da moeda. Esse modelo tem sido questionado devido às crises financeiras que dele emergiram. Motivado nisso, surgem as criptomoedas.

As criptomoedas apresentam-se como um novo mecanismo de troca de dinheiro, sem a necessidade de uma agência reguladora que estabelece tributação sobre as operações financeiras (ABREU, 2017). A emissão das moedas digitais ocorre de maneira descentralizada por regras definidas nos algoritmos (ANDRADE, 2018).

Atualmente as criptomoedas apresentam operações virtuais que determinam a confidencialidade, integridade e rapidez nas transações. Além de fornecer aos usuários liberdade de pagamento, segurança, taxas baixas e menor riscos de fraude (ANDRADE, 2018). De acordo com a autora a reputação da aparente segurança e proteção dos dados tornou-se um dos grandes atrativos para uso em transações. Podemos citar como exemplo de criptomoeda a IOTA, Bitcoin, Ethereum e entre outras. Essas criptomoedas utilizam técnicas de criptografia para realizar pagamentos em sistemas. Junto com o advento da moeda surgiu a tecnologia *blockchain* utilizada em sistemas de pagamentos. Essa tecnologia foi idealizada por Satoshi Nakamoto, como uma forma de resolver os problemas das transações online. Sendo necessário a participação de um intermediário (LUCENA; HENRIQUES, 2016). Mas com o surgimento do Bitcoin, Nakamoto propôs um modelo que armazena as transações em uma lista encadeada de acesso livre para qualquer membro da rede. Portanto, os dados tornam-se públicos e não precisa de um intermediário gerenciador para a rede e transações (NAKAMOTO, 2008).

A *Blockchain* é uma seqüencia de blocos onde cada bloco é ligado com o anterior. De acordo com (PALMA et al., 2019) no topo da *blockchain* pode ser desenvolvido um livro razão com as seguintes regras. Pares de usuários realizam transações transferindo moedas de suas contas para outras contas. Usuários chamados de mineiros verificam as transações. São selecionados para verificar se o emissor da transação realmente possuem as moedas a serem transferidas. O mineiro liga o novo bloco ao último bloco em sua *blockchain* e propaga o novo bloco na rede. Os outros mineiros analisam o novo bloco e o adicionam à sua *blockchain*. Ainda verificam se o bloco está ligado ao último bloco e se possui apenas transações válidas. O minerador é

recompensado com novas moedas ou taxas de transação para realizar serviço de verificação. (NAKAMOTO, 2008) explica que a rede considera sempre a cadeia com tamanho maior como correta e vão sempre trabalhando para extende-lá. Devido as transações conflitantes os pares podem transmitir versões diferentes da mesma cadeia. Neste caso, será identificada à cadeia correta quando os pares aceitarem a cópia que contém o *blockchain* maior. Os pares que estavam trabalhando na outra versão vão mudar e passar a trabalhar na versão maior. Por isso, as transações no *blockchain* são consideradas seguras, confiáveis e imutáveis (NAKAMOTO, 2008).

O trabalho de (BHATTACHARYA; WHITE; BELOFF, 2017) apresenta uma proposta de um novo quadro de intercâmbio P2P (Peer-to-Peer) e *Leftover Foreign Currency* (LFC), utilizando a tecnologia *blockchain* para os registros de compra e venda. Além de ajudar a resolver ou reduzir os desafios de colocar novamente as moedas estrangeiras em circulação. Neste trabalho foi proposto o uso de um quiosque inteligente com altas taxas de transações. Os quiosques são configurados com a moeda do país que o usuário está no momento. Por exemplo, se um estrangeiro estiver voltando para seu país ele deve depositar o dinheiro antes para conseguir realizar a retirada do valor no país de destino. Essa troca poderá ser realizada entre pessoas que possuem conta no quiosque. Mais precisamente, uma pessoa que deseja trocar moedas deverá vendê-las para outra pessoa que tenha as moedas desejadas. Por exemplo, se Alice quer trocar seus reais por euros e Bob possui euros, então alice utiliza o quiosque para comprar os euros de Bob pagando em reais. As taxas do quiosque incidem sobre o valor da troca. Assim, os viajantes poderiam depositar as moedas. Recebendo um saldo na sua conta que poderá utilizar em trocas, doações ou saques. O autor cita que a solução apresentou desvantagens pela falta de uso das criptomoedas, pois nas transações usariam a LFC. E a moeda deve ser depositada no quiosque em seu país, assim podendo trocar em outro que possua o quiosque. Embora a venda de moeda pode ser P2P o sistema é centralizado. Mais precisamente, a empresa controla as regras de negócio dos quiosques.

1.1 OBJETIVOS

O presente trabalho tem como objetivo amenizar os problemas da falta de moedas metálicas e de transparência em doações utilizando criptomoedas. Para alcançar o objetivo, será necessário identificar uma

criptomoeda de baixa taxas, desenvolver um software para realizar câmbio de moeda fiduciária para criptomoeda identificada e desenvolver o hardware para coleta de moedas.

A solução proposta neste trabalho é um sistema de troca entre moedas metálicas e criptomoedas. O protótipo funcional do quiosque será desenvolvido para realizar os testes nescessários no sistema de troca de moeda, como uma PoC (Prova de Conceito). O trabalho visa garantir o funcionamento do software de acordo com as regras de negócios do protótipo desenvolvido.

1.2 METODOLOGIA

Neste seção relata-se de que maneira se procede a pesquisa, para o desenvolvimento do quiosque inteligente. Quanto a abordagem da pesquisa, esta é classificada como uma pesquisa aplicada.

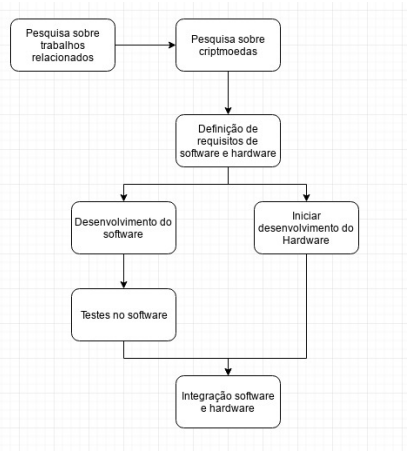


Figura 1 – Fluxograma do desenvolvimento

Na Figura 1 é apresentado o fluxograma do desenvolvimento da pesquisa. Inicialmente foi realizada uma pesquisa para contextualizar os assuntos relacionados ao tema. Na pesquisa foram encontrados poucos documentos publicados que abordavam os assuntos relacionados ao quiosque inteligente utilizando criptomoedas. Com essa lacuna na bibliografia, foi proposto o desenvolvimento de um quiosque inteligente utilizando criptomoedas.

Logo após, foi escolhida a criptomoeda que será utilizada nas transações. A IOTA foi a moeda de troca escolhida. Devido a alta escalabidade e a realização de microtransações sem cobranças de taxas. Logo em seguida, foi realizado o levantamento dos requisitos funcionais e não funcionais do sistema de software e hardware. Após o levantamento dos requisitos, iniciou-se o desenvolvimento do software e hardware. Por último, realizou-se os testes com o software desenvolvido, buscando identificar o tempo de cada transação.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 FUNÇÃO DE HASH

Segundo (PALMA et al., 2019) uma função hash criptográfica $h\{0,1\}^* \rightarrow\{0,\ 1\}^n$ mapeia o conjunto $\{0,1\}^*$ de todas as cadeias binárias para o conjunto $\{0,1\}^n$ de todas as cadeias de comprimento fixo n. Além disso, espera-se que essas funções sejam resistentes à colisão. Mais precisamente, é inviável encontrar quaisquer duas cadeias $x \neq x'$ tais que $h(x) = h(x')$. Para verificar a integridade dos dados, calcula-se o hash. Dado um p, podemos calcular seu hash $y = h(p)$ e checar que p não foi modificado desde então recomputando $h(p)$ e verificando se é igual a y. Exemplos de criptografia de funções hash que são usadas em *blockchains* Bitcoin e Ethereum são as SHA-256 e Keccak-256, respectivamente. Nos referimos para a avaliação $h(y)$ em alguma entrada y como o hash de y.

Portanto, a função principal é resumir os dados. As principais propriedades da função hash são: **resistência a pré-imagem** dado um hash definido como h deve ser difícil encontrar qualquer arquivo que tenha o mesmo hash de saída. **Resistência à segunda pré-imagem:** dado uma entrada, deve ser difícil encontrar uma segunda entrada que gere o mesmo hash de saída. Mais precisamente, dois arquivos com os mesmos hash. **Resistência a colisão:** deve ser muito difícil encontrar dois arquivos diferentes que gere o mesmo hash. A função hash geralmente é utilizada para verificação da integridade de arquivos e mensagens, verificação de senha, prova de trabalho, geradores de pseudo-aleatórios e derivação de chaves. Na implementação realizada neste trabalho a função hash é utilizada para garantir a integridade dos arquivos, informando os códigos de hash para comparar se não houve alteração no arquivo.

2.2 CRIPTOGRAFIA DE CHAVE PÚBLICA

Na *Blockchain* usa-se a tecnologia de criptografia de chave pública para autenticação, mais conhecida como assinatura digital. A assinatura digital é implementada através de criptografia de chave assimétrica. Nesse caso, é gerado uma chave privada usada para transferir moeda de uma conta para outra. E uma chave pública utilizada para verificação da autencidade pelos participantes da rede. A chave privada

é usada para confirmar a transferência. Então, o usuário deve manter sua chave privada escondida.

A assinatura digital deve garantir a autencidade e não permitir que o sistema forje a assinatura. A autenticidade garante a autoria da assinatura, que poderá ser verificada posteriormente. Como a assinatura digital é infalsificável, qualquer alteração no documento torna a assinatura inválida. Portanto, consegue-se preservar a integridade do documento e o assinante não pode negar depois a assinatura.

2.3 BLOCKCHAIN

O modelo de *blockchain* proposto por Nakamoto utiza a tecnologia como um livro distribuído que valida e registra informações das transações financeiras na rede P2P (NAKAMOTO, 2008). Neste sistema é considerado transação as transferências de uma conta para outra. A conta também chamada de carteira é identificada por um par de chaves. A chave pública para identificação e a chave privada para controle (PALMA et al., 2019). A validação da transação requer a verificação da conta do remetente, identificando se é válido o endereço. O remetente deverá fornecer uma assinaturra na transação utilizando sua chave privada. Logo após, é verificado se o saldo não é inferior ao solicitado para transferência. Após a validação da transação o livro razão é atualizado com as informações da transação.

O livro razão consiste em uma lista encadeada de blocos (PALMA et al., 2019). Um bloco contém um único conjunto de transações válidas. Cada dois conjuntos são separados. Além disso, outros blocos além do primeiro incluem um ponteiro para o bloco anterior. O ponteiro é um hash do bloco anterior.

A *blockchain* deve ser propagada para os participantes da rede. Para manter as cópias consistentes os participantes executam o protocolo de consenso (PALMA et al., 2019). O protocolo de consenso tem por finalidade identificar o próximo bloco a ser adicionado ao *blockchain*. Os participantes devem concordar que o próximo bloco contém novas transações válidas e um ponteiro para o último bloco (PALMA et al., 2019). Sem a necessidade de terceiros. Para se proteger contra ataque de *Sybil*, é utilizada a prova de trabalho. Consiste em um quebra-cabeça criptográfico que um participante deve resolver usando recursos computacionais significativos para ter o direito de ligar o próximo bloco na *blockchain* (PALMA et al., 2019). Os participantes são recompensados com moedas para resolver o enigma criptográfico.

2.4 TANGLE

Segundo (POPOV, 2018) o Tangle é a estrutura de dados e base de funcionamento da IOTA. A tecnologia por trás da IOTA é um tipo específico de gráfico direcionado, que contém transações ligadas. Cada transação é representada como um vértice, conforme mostra a Figura 2. Quando uma nova transação se une ao emaranhado de transações, ela escolhe duas transações anteriores para aprovar e adiciona duas novas arestas ao gráfico. Como mostra a Figura 2

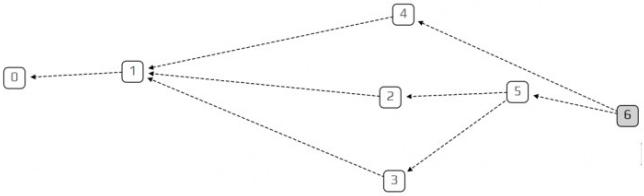


Figura 2 – Rede tangle

O emaranhado consiste em um fluxo de transações individuais entrelaçadas. Para participar desta rede um participante simplesmente precisa realizar uma pequena quantidade de trabalho computacional, que verifica duas transações anteriores. Para fazer uma transação, duas transações anteriores devem ser validadas. Sendo a validação de sua própria transação por alguma transação subsequente. Esse sistema de validação implementado não possui necessidade de fornecer recompensas. Por isso, a IOTA é completamente isenta de taxas. Além disso, é possível armazenar informações com segurança. Esse sistema possui alta escalabilidade de transações, quanto mais atividade, mais rápidas podem ser confirmadas as transações.

3 MODELO PROPOSTO

Neste capítulo, tem como objetivo detalhar o sistema proposto apresentando o modelo lógico e físico.

3.1 INTRODUÇÃO

A solução contém um quiosque inteligente para interação com o usuário e um sistema *web mobile* que fornece uma interface de transferência de criptomoedas. O sistema disponibiliza como funcionalidades o déposito de moedas, compra de criptomoeda, verificação do saldo associado ao *voucher*, verificação do valor da moeda de compra e transferência de criptomoeda.

Para detalhar o sistema foi subdivido o modelo em duas partes. O modelo lógico que descreve os componentes do sistema computacional e suas funcionalidades. E o modelo físico, detalha o hadware do sistema, bem como os componentes e tecnologias utilizadas.

3.2 MODELO LÓGICO

Na figura 3 é apresentado o modelo lógico do sistema proposto. Pode-se, observar três camadas: aplicação, serviços e banco de dados. Na camada de aplicação encontram-se os dois componentes externos ao servidor. O quiosque e a interface de interação. E a camada de serviço e banco de dados fazem parte do servidor de aplicação.

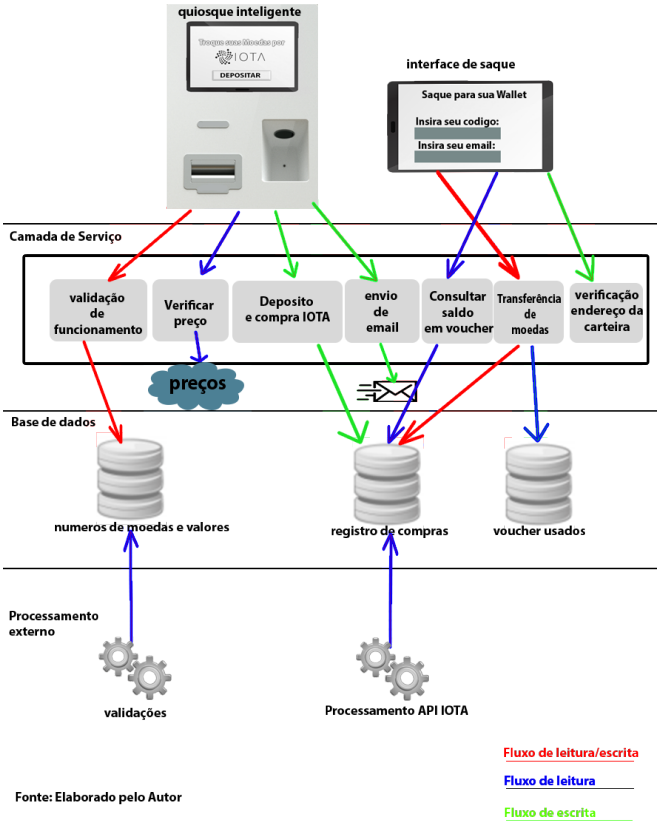


Figura 3 – Modelo lógico

3.2.1 Camada de Aplicação

A camada de aplicação envolve os componentes externos ao sistema principal. O primeiro é o quiosque inteligente que realiza a contagem das moedas fornecidas pelo usuário e converte o valor depositado em moedas metálicas para criptomoedas. No modelo desenvolvido foi utilizado a IOTA como valor de troca.

O quiosque possui um valor definido de criptomoedas em sua carteira. Então, é necessário realizar verificações de funcionamento para garantir que o usuário não deposite um valor maior de moedas

do que o valor disponível. Além de verificar o espaço disponível para armazenamento das moedas metálicas, garantindo que exista espaço suficiente para a quantidade depositada.

Já, a interface de interação incorporada ao quiosque tem como objetivo informar o usuário sobre cada ação executada. Por exemplo, se o usuário solicitar a ação de depósito na interface, será solicitado para inserir a quantidade moedas que deseja depositar.

Outro componente importante é a interface de transferência. Essa interface permite transferir as criptomoedas para a carteira do usuário utilizando o *voucher* enviado no email. Esta interface possui um *captcher* para inviabilizar tentativas de brute force. Além disso, é verificado na base de dados se o *voucher* informado contém a quantidade de criptomoedas solicitadas para realizar a transferência. O usuário precisa apenas inserir o endereço da carteira, que será verificada no servidor se é uma carteira *IOTA* válida.

3.2.2 Camada de Serviços

A camada de serviço disponibiliza um conjunto de funcionalidades aos componentes da camada de aplicação. Comporta-se como meio de entrada do sistema principal. Conforme mostra Figura 3 a um conjunto de serviços específicos disponibilizados que serão descritos nos parágrafos seguintes.

O serviço de funcionamento é realizado por duas operações que ocorrem simultaneamente. A verificação de espaço de armazenamento e a verificação da quantidade de criptomoedas na carteira. A operação de verificação do espaço de armazenamento das moedas metálicas é previamente configurado com a quantidade de moedas metálicas que o espaço suporta. E a cada solitação de depósito é verificado a quantidade de moedas que podem ser armazenados. O servidor consegue manter armazenado a quantidade de moedas inseridas e controlar o espaço de armazenamento. Quando o espaço estiver esgotado é emitido um alerta para a interface que bloqueará novos depósitos até que seja esvaziado.

A operação de verificação de quantidade de criptomoeda disponível na carteira do quiosque é acionado sempre que o usuário solicitar à ação de depósito na interface. Por exemplo, quando o usuário clicar no botão da interface em depositar, será informado o valor máximo de moedas que podem ser depositadas. Se a carteira do quiosque estiver vazia, será enviado um email para o suporte informando a falta de criptomoeda e é emitido um alerta na interface. Assim, o suporte

consegue verificar a falta de criptomoedas e realizar um novo depósito na carteira.

O serviço de verificação do valor da criptomoeda é acionado periodicamente a cada 1 segundo. Este serviço realiza a consulta do valor da criptomoeda IOTA. O valor da criptomoeda é armazenado em uma base de dados e enviado para a interface do quiosque. Assim, o usuário consegue visualizar o valor da criptomoeda no momento do depósito.

O serviço de depósito é acionado pelo usuário na interface. Após, a solicitação do depósito o usuário insere suas moedas no quiosque e o sistema automaticamente realiza a contagem das moedas depositadas. E informa na interface o valor depositado. Assim, o usuário poderá conferir se o valor depositado condiz ao valor mostrado na interface.

O serviço de compra e envio de email é acionado no momento em que o usuário inserir o email e confirmar a compra da criptomoeda. Após, a confirmação da compra é enviado um email para o usuário informando a hora da compra, voucher para realizar a transferência, valor da criptomoeda associado ao *voucher*, valor de moedas depositadas, valor da criptomoeda no momento da compra e um link para o usuário acessar e transferir as criptomoedas para uma carteira ou doar para alguma instituição filantrópica cadastrada.

O serviço de consulta do valor associado ao *voucher* é efetuado no momento que o usuário optar por transferir as criptomoedas. Faz-se uma consuta na base de dados a fim de verificar se o voucher informado contém o valor em criptomoedas.

O serviço de transferência de criptomoedas é requisitado pelo usuário pela interface de transferência. Quando um *voucher* não foi utilizado e contêm o valor de criptomoedas informado. É confirmada a transferência de criptomoedas associada ao *voucher* para o endereço válido da carteira *IOTA* informado.

O serviço de verificação de carteiras *IOTA* é acionado quando o usuário confirma a transferência e informa o endereço da carteira. Caso a carteira seja inválida é enviado para a interface de transferência uma mensagem de erro.

3.2.3 Camada de banco de dados

O conjunto de repositórios desta camada atuam na persistência de informações geradas pelos componentes da camada de aplicação. Possui a base d números de moedas e valores, registro de compras e *vouchers* usados, conforme mostra a Figura 3.

A primeira base é responsável pelo armazenamento da quantidade de moedas metálicas depositadas. As consultas realizadas nessa base informam o espaço disponível para novos depósitos e a quantidade de criptomoedas disponível na carteira do quiosque.

A base de registro de compra contém informações que são utilizadas pelo serviço de transferência. Tais informações representam os valores adquiridos pelos usuários e seus respectivos *voucher* para realizar a transferência.

Já a base dos *voucher* usados, garante que o usuário não utilize o mesmo *voucher* e nas verificações futuras seja gerado um *voucher* diferente a cada requisição de transferência.

3.3 MODELO FÍSICO

A modelagem física deste trabalho é apresentada na Figura 4. Nas seções a seguir serão detalhados os diversos componentes do sistema em relação aos aspectos internos.

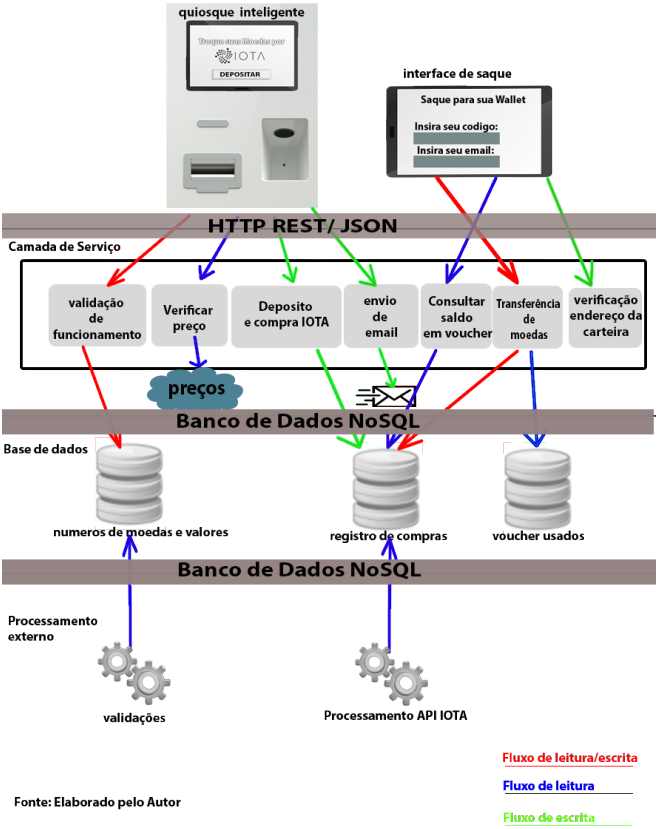


Figura 4 – Modelo Físico

3.3.1 Camada de aplicação

3.3.1.1 Quiosque inteligente

O quiosque inteligente apresentado no modelo lógico da Figura 3, foi construído de acordo com a Figura 5. Pode-se, observar a existência de três componentes principais: o Raspberry PI^{o} 3 Modelo B, um display LCD Touch RPi 3.5 polegadas e o sistema mecânico conectado a gpio do Raspberry PI^{o} para realizar a contagem das moedas.

O display LCD Touch RPi 3.5 polegadas responsabiliza-se por apresentar a interface de interação. Por sua vez, é hospedada no Raspberry PI® 3 Modelo B+, mostrada na Figura 5. O sistema irá iniciar no momento que o usuário requisitar a ação de depósito na interface de interação. Assim, o Raspberry PI® 3 Modelo B+ verifica o espaço de armazenamento e a quantidade de criptomoedas na carteira do quiosque utilizando o protocolo HTTP com REST. Caso o espaço esteja cheio, é emitido um alerta na interface e a ação de depósito é bloqueada. Caso contrário, é permitido seguir com o depósito. Caso a quantidade de criptomoedas seja inferior ao valor solicitado, à ação de depósito é bloqueada. E o sistema enviará um email para o suporte informando a falta de moeda na carteira e/ou o espaço insuficiente. No entanto, o sistema ficará pausado até que seja verificado as condições definidas anteriormente. Caso contrário, é iniciado o depósito ativando os sensores mêcanicos para contagem das moedas.

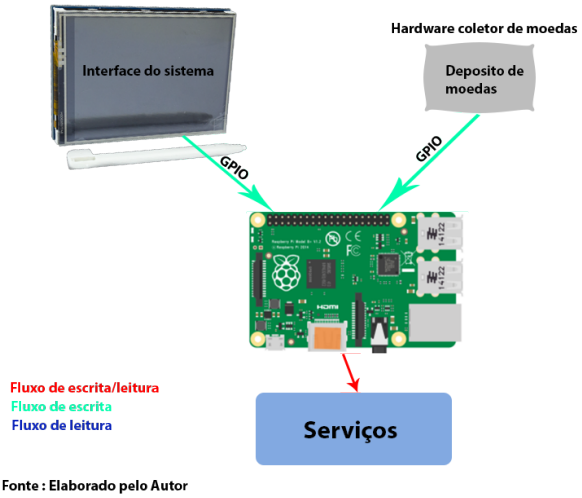


Figura 5 – Quiosque inteligente

O sensor mecânico para a contagem de moedas mostrado na Figura 6 foi projetado como um protótipo inicial para a validação do sistema. Ao iniciar a contagem das moedas a GPIO_OUT (General Purpose Input/Output) habilita um nível lógico alto e a GPIO_IN inicia a leitura. Mas está conectada em um *Ground* 0Volts (GND). Portanto, detecta um nível alto apenas quando uma moeda fecha o

circuito. Com isso, consegue-se realizar a contagem das moedas depositadas. E para detectar o valor da moeda foram montados 5 sensores mecânicos conectados as GPIO. Os valores de cada sensor foi definido inicialmente. No momento que a moeda passa pelo sensor é detectado o valor e armazenado.

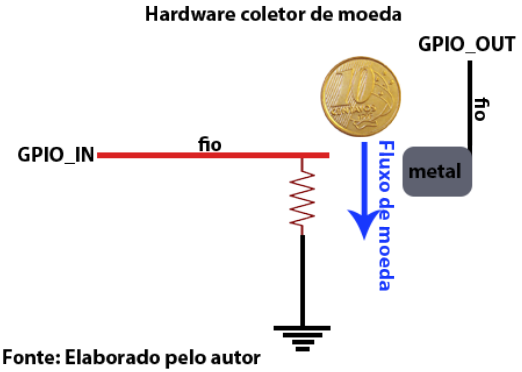


Figura 6 – Sensor mecânico coletor de moedas

Após, a finalização do depósito é criado um arquivo *JavaScript Object Notation* (JSON) mostrado na Figura 7. Em seguida, é renderizado o valor total na tela para o usuário. Caso o valor não esteja correto o usuário tem a opção de cancelar a compra e receber suas moedas novamente.

```
{

   "user-hashNumberGenerator":{
      "5 centavos":2,
      "10 centavos":3,
      "25 centavos":2,
      "50 centavos":1,
      "1 real":1
   },
   "totalValue":2.10
}
```

Figura 7 – Depósito de moedas
Fonte: Elaborado pelo Autor

Para o usuário confirmar a compra é necessário inserir o endereço do email. Assim, receberá a notificação da compra, o *voucher* e as informações de como realizar a transferência das criptomoedas. Na

Figura 8 é apresentada a interface que permite o usuário realizar a operação de compra das criptomoedas.

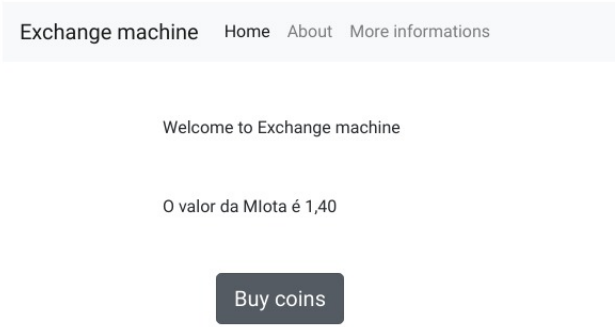


Figura 8 – Interface do interação do quiosque

Como parte do processo de implementação, foi desenvolvido uma PoC buscando realizar os testes do software. O resultado é mostrado na Figura 9. É possível verificar a interface de interação no Raspberry Pi com os serviços oferecidos. Quando o serviço de depósito é solicitado, o usuário deve inserir suas moedas no local indicado para iniciar os procedimentos detalhados anteriormente.

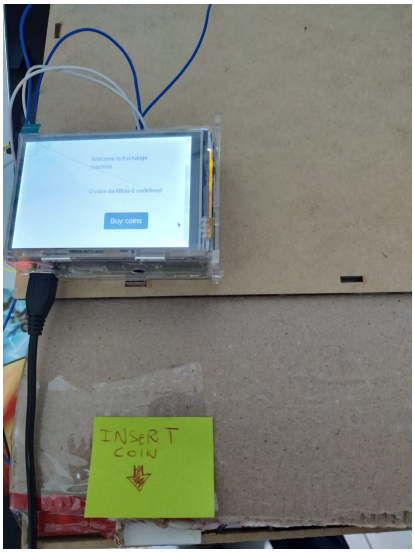
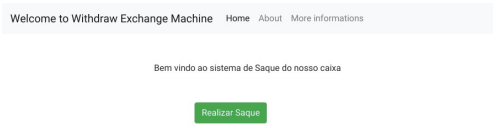


Figura 9 – Protótipo do quiosque inteligente

3.3.1.2 Interface de transferência

Como mencionado anteriormente, a interface de tranferência é destinada ao usuário. Após, a solicitação de tranferência das criptomoedas o usuário escolhe a carteira de sua preferência ou *exchanges*. Conforme apresenta a Figura 10, o serviço de transferência fica disponível na tela principal. No momento que o usuário acionar a ação de transferência deverá informar o *voucher* e o endereço da carteira que deseja receber o valor em *IOTA*. Se alguma isntituição filantrópica estiver cadastrada no quiosque, é possível realizar doações.

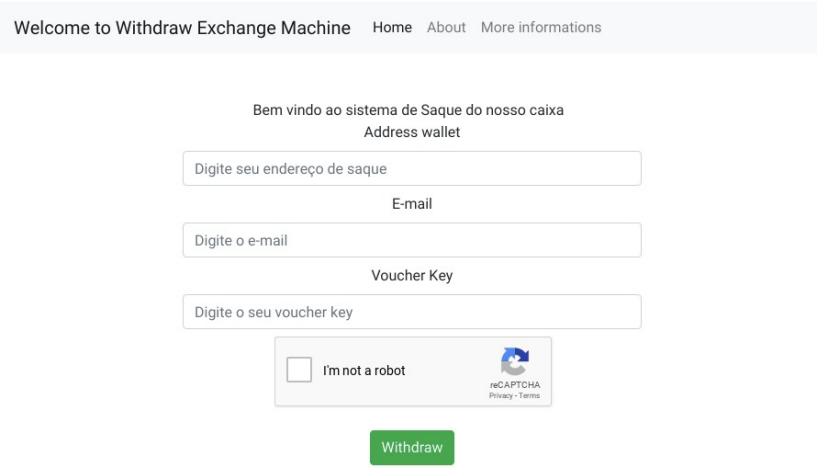
Figura 10 – Interface de tranferência



Fonte: Elaborado pelo Autor

Logo após, o usuário deverá passar pelo *captcher* utilizado para evitar ataques de *brute force*. Como mostra a Figura 11. O usuário deve informar o endereço de uma carteira válida, que irá receber o valor transferido. Inserir seu email de autenticação e informar o *voucher* recebido no momento que o depósito das moedas metálicas foi realizado. Quando o usuário confirmar as informações, inicia-se as verificações dos serviços de transferência. Por fim, a transferência é finalizada.

Figura 11 – Realizar transferência



Fonte: Elaborado pelo Autor

3.3.2 Camada de Serviço

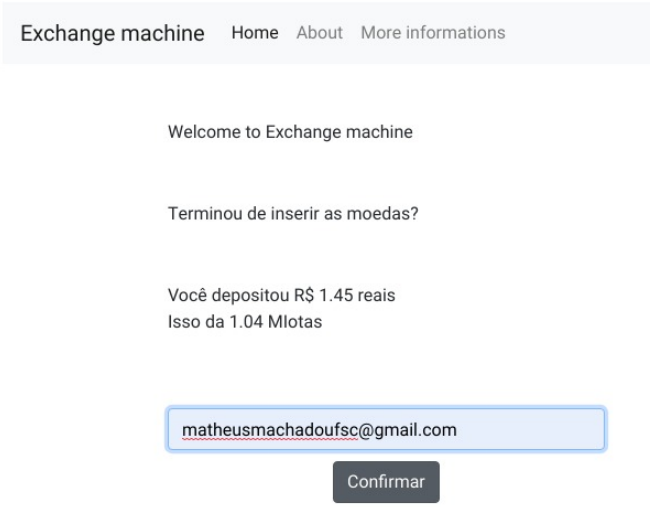
Como descrito anteriormente, a camada de serviços atua como porta de entrada do sistema para os componentes da aplicação. Conforme demostrado na Figura 4, utiliza-se sobre o HTTP e o REST um estilo arquitetural que opera como um modelo abstrato da arquitetura da *Web*. E o acesso aos recursos ocorrem por meio do método HTTP, como GET e o POST (FIELDING; TAYLOR, 2002). Para a implementação dos serviços REST utilizou-se a linguagem de programação *JavaScript* com a plataforma *NodeJS* para realizar o processamento das requisições.

O serviço de validação de funcionamento é acionado sempre que o usuário interage com o quiosque. Para implementação desse serviço foi utilizado a linguagem de programação *JavaScript*. Assim, consegue-se verificar se o valor disponível em criptomoedas na carteira é maior que o valor configurado no quiosque. Também é realizada a verificação do espaço de armazenamento. Para controlar a quantidade de moedas depositadas. Caso a quantidade seja maior ou igual a quantidade de moedas suportadas pelo quiosque. O quiosque é bloqueado para operações de depósitos.

O serviço de verificação de preço da criptomoeda *IOTA* é realizado a cada 1 segundo. Na implementação das consultas utilizou-se a linguagem de programação *JavaScript* que realiza um GET para a API da *exchange* escolhida pelo estabelecimento.

O serviço de depósito foi implementado utilizando a linguagem de programação *JavaScript* e um backend em *NodeJS* para realizar a conexão com a *API IOTA*. No momento que o usuário realizar o depósito, inicia-se a contagem das moedas. Logo após, é enviada para a interface a quantidade de moedas depositadas. Como mostra a Figura 12. Após, o usuário confirmar o depósito o valor é convertido para criptomoeda *IOTA*.

Figura 12 – Serviço de depósito



Fonte: Elaborado pelo Autor

Quando o usuário confirmar a compra o servidor *NodeJS* irá criar um JSON de compra. Como mostra a Figura 13. Em seguida, enviará um email ao usuário e será inserido o JSON na base de dados de registro de compra.

Figura 13 – JSON registro de compra


```
{
  "valorAtualIota":1.8,
  "valorDeMoedasDepositadas":2.5,
  "valorIotaComprada":1.38,
  "dataDaCompra":"21/3/2019 12:38",
  "email":"matheusmachadoufsc@gmail.com",
  "checkoutLabelValue":"inWalletExchange",
  "_voucher":"2d120bfceb2645d093aae6b1a8382176"
    ,
  "_id":"608qFhV1e3QvjWGV"
}
```


Fonte: Elaborado pelo Autor

O serviço de envio de email foi implementado utilizando a linguagem de programação *JavaScprit*, um servidor *NodeJS* e a biblioteca *node-mailer*.

O serviço de consulta de saldo do *voucher* é utilizado pela interface de transferência. Quando o usuário realizar a transferência deverá informar seu *voucher*. Assim, é realizado um POST com o *voucher* fornecido pelo usuário para o servidor *NodeJS*. Sendo verificado na base

de dados de registros de compra se o *voucher* existe e possui o valor de criptomoedas associado. Este serviço foi implementado utilizando a linguagem de programação *JavaScript*.

O serviço de verificação do endereço da carteira foi implementado utilizando a linguagem de programação *JavaScript*. Este serviço utiliza a *API IOTA* para verificar se o endereço da carteira fornecida para transferência é uma carteira *IOTA* válida.

O serviço de transferência de moedas utiliza internamente o serviço de consulta do saldo do *voucher* e verificação do endereço da carteira. Após a validação desses serviços, é conectado o serviço de transferência das moedas com a carteira do quiosque utilizando a *API IOTA*. Em seguida, é transferido as criptomoedas associadas ao *voucher* para a carteira informada. Para a implementação do serviço de transferência utilizou-se a linguagem de programação *JavaScript* e um servidor *NodeJS* para conectar a carteira via sua *API*.

3.3.3 Camada de Banco de Dados

As bases de dados do trabalho estão relacionadas ao servidor principal de serviços. Conforme mostra a Figura 4, tem-se três bases de dados detalhadas anteriormente no modelo lógico.

A tecnologia utilizada para implementação das base de dados baseia-se no conceito de banco de dados não relacionais, como o NoSQL. Este tipo de banco de dados é utilizado em aplicações de grande escala para superar o desempenho dos bancos de dados relacionais. Os dados são registrados em coleções, que não restringem os tipos de dados armazenados (BOICEA; RADULESCU; AGAPIN, 2012).

Neste trabalho optou-se pelo NeDB. Um sistema de banco de dados NoSQL baseado em documentos. O armazenamento procede-se no formato de JSON, baseado em chave e valor. O sistema desenvolvido neste trabalho possui um pequeno conjunto de dados armazenados, devido a quantidadde pequena de testes realizados. Mas, em um ambiente real resultaria em um número expressivo de compras, transferências e armazenamento de moedas. Por isso, na implementação utilizou-se o conceito de base de dados NoSQL.

Nas seções seguintes será detalhados os repositórios, considerando os aspectos internos como tipos de dados armazenadas e o momentos que são utilizados.

3.3.3.1 Base de dados números de moedas e valores

Como descrito na Seção 3.2.3 a base de dados números de moedas e valores controlam a quantidade de moedas depositadas e os valores das criptomoedas contidas na carteira do quiosque. Pode-se observar esse controle no JSON apresentado na Figura 14. O JSON mostra a quantidade de espaço dispónivel, a quantidade de moedas inseridas, valor em reais e a data que o depósito foi realizado.

Figura 14 – Base de dados armazenamento

```
{
   "uservoucher" : hash-owner,
  "armazenamento":{
     "5 centavos":0,
     "10 centavos":0,
     "25 centavos":0,
     "50 centavos":0,
     "1 real":0
  },
  "totalDeMoedas":0,
  "Valor em reais": 0;0,
  "espaco disponivel": 100
  "timestamp" :"2019-05-05 21:30:39.209"
}
```

Fonte: Elaborado pelo Autor

Essa base de dados iniciada com uma JSON mostrado na Figura 14. No momento que o usuário realizar um depósito é gerado o objeto JSON mostrado na Figura 15. Observa-se que foi realizado um depósito de 9 moedas e o *timestamp* (momento exato do depósito) ocorreu no dia 05 de Maio de 2019 às 22h31min, resultando no total de R$ 2,10. E o campo do espaço de armazenamento disponível reduziu de acordo com a quantidade que foi inserida. Mais precisamente, antes poderia ser inserido 100 moedas conforme mostra a Figura 14. Após o depósito das 9 moedas é permitido ser armazenado apenas 91 moedas.

Figura 15 – Armazenamento de quantidade


```
{
   "uservoucher" : hash01,
  "armazenamento":{
     "5 centavos":2,
     "10 centavos":3,
     "25 centavos":2,
     "50 centavos":1,
     "1 real":1
  },
  "totalDeMoedas":9,
  "Valor em reais": 2.10,
  "espaco disponivel": 91,
  "timestamp" :"2019-05-05 22:31:39.209"
}
```


Fonte: Elaborado pelo Autor

3.3.3.2 Base de dados registros de compras

Como descrito na Seção 3.2.3, a base de dados registros de compras realiza o armazenamento das compras no formato JSON. Como mostra a Figura 13. Pode-se observar o campo *checkoutLabelValue* está *inWalletExchange*. Isso indica que o *voucher* não foi utilizado. Mais precisamente, o usuário não realizou uma transferência para outra carteira usando o *voucher*. Na Figura 17, pode-se observar o campo *chekcoutLabelValue* como "voucher-usado", indicando que o valor referente ao *voucher* já foi enviado para uma carteira.

Figura 16 – JSON registros de compras utilizados


```
{
    "valorAtualIota":1.8,
   "valorDeMoedasDepositadas":2.5,
   "valorIotaComprada":1.38,
   "dataDaCompra":"21/3/2019 12:38",
   "email":"matheusmachadoufsc@gmail.com",
   "checkoutLabelValue":"voucher-usuado",
   "_voucher":"2d120bfceb2645d093aae6b1a8382176"
      ,
   "_id":"608qFhV1e3QvjWGV"
}
```


Fonte: Elaborado pelo Autor

3.3.3.3 Base de dados *vouchers* utilizados

A base de dados *vouchers* utilizados utiliza um arquivo *JSON* para armazenamento. Assim, posteriormente permite realizar consultas

a cada novo *voucher* gerado evitando a duplicação do mesmo número de *voucher*. Na Figura 17 é apresentado a lista de *vouchers* gerados.

Figura 17 – Lista de *vouchers* gerados


```
{
    "vouchers" : ["2d120bfceb2645d093aae6b1a8382
       176","2d120bfceb2645d093aae6b1asds213d6"]

}
```


Fonte: Elaborado pelo Autor

4 ANÁLISE DOS RESULTADOS

Nesse capítulo será apresentado os testes realizados e resultados obtidos. A partir da aplicação do modelo proposto materializado em um sistema computacional considerado uma prova de conceito. Será criado um cenário de aplicação para apresenta o cenário em que o sistema será testado e avaliado. Será detalhado o ambiente da simulação, os valores depositados e as transferências executadas pelo sistema. E a avaliação do protótipo é realizada a partir do cenário de teste proposto. Além de detalhar as interações de depósitos e transferência realizadas no quiosque.

4.1 AVALIAÇÃO DO PROTÓTIPO

Nessa seção é descrita a avaliação do protótipo e o cenário criado para realizar os testes. O ambiente consiste na verificação das funcionalidades do sistema por meio de ações definidas. Começando pela interação do usuário com o quiosque, com o objetivo de observar o comportamento e as funcionalidades do protótipo desenvolvido. Para isso, foram criados dois cenário o de depósito apresentado na Figura 18 e o cenário de transferência mostrado na Figura 19.

Figura 18 – Cenário de depósito

Fonte: Elaborado pelo Autor

Nos dois cenários é necessário que ocorra a interação do usuário

com o quiosque. A base de dados foi incializada com valor definido para a avaliação do sistema. Como mostra a Figura 20 inicio-se com o espaço de armazenamento máximo de 100 moedas. E na carteira do quiosque os testes iniciais foram realizados com simulações, sem definir a quantidade de *MIOTA*.

Figura 19 – Cenário de transferência

Fonte: Elaborado pelo Autor

4.1.1 Testes de depósito

Para os testes do protótipo referente ao sotware e hadware. Fez-se alguns depósitos com a finalidade de verificar o funcionamento geral do esquipamento. Inicialmente o quiosque está apto para realizar o depósito. Já foi definido a quantidade inicial das bases de dados. Como pode ser visto na Figura 20.

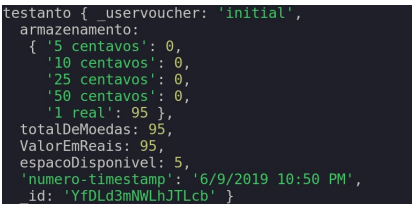
Figura 20 – Base de dados controle de moedas

```
testanto { _uservoucher: 'initial',
  armazenamento:
   { '5 centavos': 0,
     '10 centavos': 0,
     '25 centavos': 0,
     '50 centavos': 0,
     '1 real': 0 },
  totalDeMoedas: 0,
  ValorEmReais: 0,
  espacoDisponivel: 100,
  'numero-timestamp': '2019-05-05 21:30:39.209',
  _id: 'vjvCQzByJPiIqjPP' }
```

Fonte: Elaborado pelo Autor

Inicialmente foi realizado testes de inserções de moedas, contagem do valor em reais e contagem do espaço de armazenamento. Ao acionar a funcionalidade depósito a interface solicitou a inserção das moedas no local indicado. No teste foram inseridas 95 moedas de um real. Como mostra a Figura 21. Os dados foram enviados a interface indicando o total de moedas, o valor inserido em reais, o espaço disponível para armazenamento e a data do depósito.

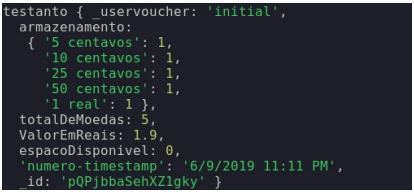
Figura 21 – Base de dados controle de inserção de moedas



Fonte: Elaborado pelo Autor

Como no teste anterior o espaço de armazenamento disponível ficou 5. Foi inserido no quiosque uma moeda de cada valor (5, 10, 25, 50 e 1). Pode-se observar o teste realizado na Figura 23. Portanto, a base de dados de armazenamento atingiu o espaço máximo permitido pelo quiosque. Os demais campos foram preenchidos corretamente com as informações de entrada.

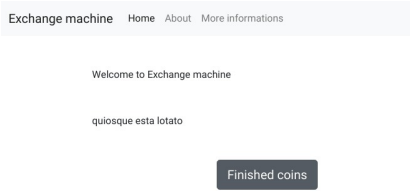
Figura 22 – Base de dados controle de inserção de moedas 2



Fonte: Elaborado pelo Autor

Seguindo as informações dos testes anteriores. Temos que o espaço de armazenamento no momento é zero. Então, foi realizado um novo depósito. Logo em seguida, o sistema emitiu uma notificação para a interface informando que o espaço de armazenamento do quiosque está cheio. O quiosque permaneceu bloqueado até o momento que o suporte esvaziou o espaço. A mensagem enviada para a interface pode ser observada na Figura 23.

Figura 23 – Quiosque sem espaço disponível



Fonte: Elaborado pelo Autor

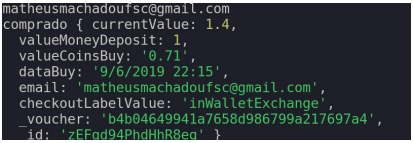
No momento que o depósito foi finalizado, foram inseridas as informações na base de dados. Em seguida, foi enviado um email com o *voucher* na conta informada. O email recebido pode ser visualizado na Figura abaixo.

Figura 24 – Teste de recebimento de email

Fonte: Elaborado pelo Autor

Na Figura 25, é apresentada as informações inseridas na base de dados de compras após finalizar o depósito. As informações refere-se ao valor depositado de 1,49 R$. Revertido em *IOTA* ficou 0,71 MIOTA. A data de depósito de 09/09/2019 às 22:15. O email de destino e o *voucher* recebido.

Figura 25 – Teste de depósito

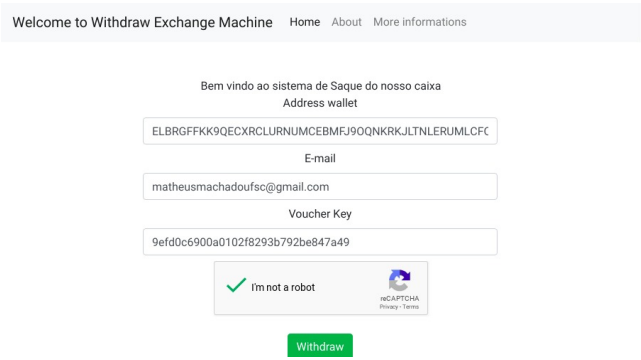


Fonte: Elaborado pelo Autor

4.1.2 Testes de transferência

Para o teste de transferncia seguiu o cenário apresentado na Figura 19. No momento que o usuário solicita a ação de transferência é redenrizado para a interface de transferência. Como mostra a Figura 26, foi preenchido o endereço da carteira, email e o *voucher* recebido no email. Ainda, houve a verificação pelo *Captcher*.

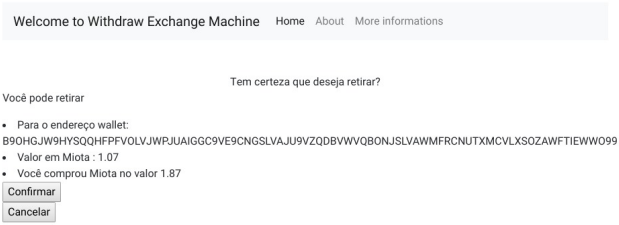
Figura 26 – Teste de resgate de voucher



Fonte: Elaborado pelo Autor

Após a aprovação do *Captcher*. O sistema verificou todos os dados da transação e enviou para a interface o resultado da consulta do *voucher*. Sendo possível conferir os dados recuperados e identificar se as informações estão corretas. Pode-se observar a ação na Figura 27. O *voucher* recuperado contêm um endereço de carteira, 1,07 de MIOTA e a MIOTA foi comprada por 1,87 MIOTA. Se o valor estiver errado o usuário pode reportar ao suporte o erro.

Figura 27 – Resultado da consulta do *voucher*



Fonte: Elaborado pelo Autor

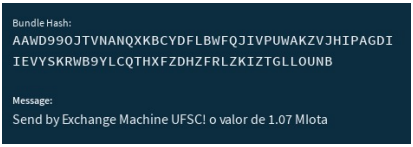
Após a confirmação da transferência. O sistema verificou o valor referente a transação realizada e identificou a carteira de destino. Então, enviou o valor para a carteira indicada. E inseriu na base de dados o endereço da carteira e o valor referente ao *voucher*. A Figura 28 mostra o *voucher* que foi recuperado.

Figura 28 – Teste de requisição de transferência

Fonte: Elaborado pelo Autor

Quando a ação de transferência foi finalizada. Foi enviado o hash da transferência no email indicado. Para o rastreamento da transferência. Pode-se observar na Figura 29, o hash da transferência do teste realizado.

Figura 29 – Endereço da transferência

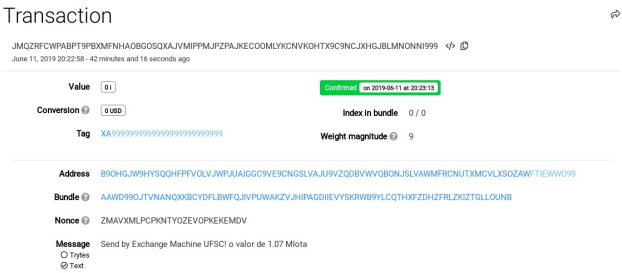


Fonte: Elaborado pelo Autor

O rastreamento da transferência, foi realizado no web site da *IOTA*. No site existe um espaço de busca para inserir o hash recebido.

O hash foi inserido e a consulta foi feita pelo sistema. Em seguida, as informações referente ao hash foram retornadas. Pode-se observar as informações na Figura 30.

Figura 30 – Verificação de transparência no envio



Fonte: Elaborado pelo Autor

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo amenizar os problemas de falta de moedas e de transparência em doações utilizando criptomoedas. Baseando-se nos conceitos de quiosque inteligente e criptomoedas.

Para atingir o objetivo geral, inicialmente foi projetado o modelo. Em seguida, foi definido o escopo do projeto e os componentes. Sendo, o sistema do quiosque, o servidor de serviços, as bases de dados, a interface do usuário, a identificação da criptomoeda adequada e os serviços disponibilizados no quiosque inteligente.

Com o modelo criado, foi desenvolvido o protótipo inicial do quiosque inteligente. Foi desenvolvido um software para realizar câmbio de moeda fiduciária para criptomoeda IOTA e construído o hardware. Para tanto, fez-se uso do display LCD Touch RPi 3.5 polegadas para apresentar os serviços oferecidos na interface de interação que por sua vez, é hospedada no Raspberry PI 3. E conectado sensores mecânicos que identifica o valor das moedas inseridas. Além disso, elaborou-se uma estrutura básica para agregar todos os componentes de leitura e processamento. Ao final, o sistema funcionou conforme os requisitos levantados e detalhados no trabalho. Mais precisamente, foi possível acionar o serviço de depósito, inserir as moedas metálicas, realizar a transferência das criptomoedas para uma carteira e as demais funcionalidades descritas.

Como forma de avaliar o sistema implementado, elaborou-se um cenário de testes e um diagrama de fluxo de execução utilizados como base na avaliação. Foi testada a funcionalidade de depósito, garantindo que funcionará até o armazenamento máximo permitido. O envio de email também passou pelos testes. Está sendo enviado email corretamente. E o último teste foi da verificação do espaço de armazenamento.

Ao final, o sistema demostrou os respectivos comportamentos esperados. Portanto, conclui-se que o objetivo final do trabalho foi atingido. Os testes comprovaram que o quiosque inteligente permite reter moedas metálicas e realizar a troca por criptomoedas. Além da solução desenvolvida apresentar baixo custo. Assim, pode vir a amenizar os problemas da falta de moedas. Mas, o equipamento desenvolvido não foi implantado em nenhum estabelecimento comercial até o momento. Para isso, deverá ser aperfeiçoado para disponibilização.

Como dificuldade, podemos citar a avaliação e testes de doações. Devido a necessidade de instituições filantrópicas ser cadastradas. No entanto, todas as funcionalidades estão implementadas no quiosque.

5.1 TRABALHOS FUTUROS

Como trabalho futuro pretende-se implementar uma interface mais agradável para o usuário e novas opções de depósitos. Como por exemplo, cadastros de organizações filantrópicas para receberem doações. Além disso, pretende-se incluir as impressoras térmicas. E utilizar outras criptomoedas para troca. E por último, pretende-se melhorar o coletor de moedas desenvolvido.

REFERĘNCIAS

ABREU, J. d. S. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, p. 561–563, 2017.

AMATO, C. P. A Moeda Fiduciária. p. 100–103, 2004.

ANDRADE, M. D. TRATAMENTO JURÍDICO DAS CRIPTOMOEDAS: A DINÂMICA DOS BITCOINS E O CRIME DE LAVAGEM DE DINHEIRO. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, p. 45–59, feb 2018. ISSN 2236-1677. <https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20 https://www.publicacoes.uniceub.br/RBPP/article/view/4897>.

Banco Central. *O que é e o que faz o Banco Central*. 2019. Disponível em: `https://www.bcb.gov.br/acessoinformacao/legado?url=https:Acessado em 16/04/2019.`

BHATTACHARYA, R.; WHITE, M.; BELOFF, N. A Blockchain based Peer-to-Peer Framework for Exchanging Leftover Foreign Currency. *2017 Computing Conference*, n. July, p. 1431–1435, 2017.

BOICEA, A.; RADULESCU, F.; AGAPIN, L. I. MongoDB vs Oracle - Database comparison. *Proceedings - 3rd International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2012*, n. September 2012, p. 330–335, 2012.

FEBRABAN – Federação Brasileira de Bancos. *Brasileiro guarda 7,4 bilhões de moedas*. 2016. Disponível em : `https://portal.febraban.org.br/noticia/2928/pt-br/`. Acessado em 07/11/2018. <https://portal.febraban.org.br/noticia/2928/pt-br/>.

FIELDING, R. T.; TAYLOR, R. N. Principled design of the modern Web architecture. *ACM Transactions on Internet Technology*, v. 2, n. 2, p. 115–150, 2002. ISSN 15335399.

JESUS, A. D. D.; ÓRGÃOS. ÓRGÃOS REGULADORES E INOVAÇÃO TECNOLÓGICA: A TRANSFORMAÇÃO DIGITAL DAS INSTITUIÇÕES FINANCEIRAS COMO

DESAFIO AO DIREITO. *Journal of Personality and Social Psychology*, v. 1, n. 1, p. 1188–1197, 2017. ISSN 0092-6566. <https://osf.io/nf5me%0Ahttp://dx.doi.org/10.1016/j.tree.2015.01.012%0Ahttps://ww

LUCENA, A. U.; HENRIQUES, M. A. A. Estudo de arquiteturas dos Blockchains de Bitcoin e Ethereum. *Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum*, v. 1, n. 1, p. 1–12, 2016.

MATIAS-PEREIRA, J. Custos da escassez no meio circulante do Brasil de moedas metálicas. *Observatorio de La Economía Latinoamericana*, n. January 2010, p. 35, 2010. ISSN 1696-8352. <http://www.eumed.net/cursecon/ecolat/br/10/jmp.htm>.

MESQUITA, P. L. Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gerência de Projetos em Tecnologia da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gerência de Projeto. n. 2001, 2017. <https://www.riuni.unisul.br/bitstream/handle/12345/3162/JORGE_WEISS_AD6_

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem. *Journal for General Philosophy of Science*, v. 39, n. 1, p. 53–67, 2008. ISSN 09254560.

Oliveira, Marina e Macena, Thaís . *Voltou de viagem com dinheiro estrangeiro? Veja opções e saiba o que fazer.* 2015. Disponível em : `https://viagem.uol.com.br/noticias/2015/02/03 voltou-de-viagem-com-dinheiro-estrangeiro-saiba-quais-sao-as-suas-opcoes.htm`. Acessado em 07/11/2018. <https://viagem.uol.com.br/noticias/2015/02/03/voltou-de-viagem-com-dinheiro-estrangeiro-saiba-quais-sao-as-suas-opcoes.htm>.

PALMA, L. M. et al. Blockchain and smart contracts for higher education registry in Brazil. *International Journal of Network Management*, n. October 2018, p. 1–21, 2019. ISSN 10991190.

POPOV, S. IOTA whitepaper v1.4.3. *New Yorker*, v. 81, n. 8, p. 1–28, 2018. ISSN 0028-792X. <https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92

SILVA, J. C. A Circulação de Moedas Metálicas no Brasil Palavras-chave Introdução. *Revista técnico-científica das faculdades atibaia*, p. 11–27, 2003.

TRINDADE,Rodrigo, 2019. *Golpistas criam falsos canais para roubar doações às vítimas de Brumadinho* . Disponível em : https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/01/28/ year = 2019, NOTE = "Acessado em 20/04/2019". <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/01/28/golpistas-criam-falsos-canais-para-roubar-doacoes-as-vitimas-de-brumadinho.htm>.