Fatec Cruzeiro Prof. Waldomiro May
Revista Científica H-TEC Humanidades & Tecnologia

GET TOGETHER: ESTUDO E IMPLEMENTAÇÃO DE UMA APLICAÇÃO BLOCKCHAIN USANDO SMART CONTRACTS

Autores
Pedro Caetano Diniz Siqueira[1]
José Walmir Gonçalves Duque[2]

RESUMO
A evolução da tecnologia é cada vez mais rápida e tem impacto direto na sociedade - o modo como as pessoas veem o dinheiro mudou drasticamente e a tecnologia começou a afetar a economia com o nascimento do Bitcoin, a primeira Criptomoeda do mundo, que foi inicialmente proposta em 2008 e em 2018 inspirou este artigo. Em face ao cenário das Criptomoedas, este trabalho tem por objetivo desenvolver um protótipo de aplicação de Crowdfunding, fazendo uso da Blockchain e que possa ser capaz de processar Smart Contracts dentro da Ethereum Network, a fim de demonstrar a efetividade da aplicação de métodos, técnicas e ferramentas adequadas a esse contexto moderno de tecnologia. Para o desenvolvimento da solução, foi admitida a Criptomoeda Ethereum, totalmente digital e descentralizada. Fazendo uso de uma API disponibilizada pela Ethereum, a web3, foi possível escrever as transações na Blockchain e, para uma interface amigável, foi utilizada a biblioteca React.js. Em paralelo, para viabilizar a escrita dos contratos, foi utilizada a linguagem Solidity, baseada em Javascript. Como resultado do trabalho, obteve-se um sistema eletrônico de transação descentralizado que não necessita de um intermediário, que conta com assinaturas digitais que permitem forte controle sobre propriedade prevenção de gasto duplo, tudo isso por meio de uma rede peer-to-peer que utiliza prova de trabalho para criar um registro público, que é impraticável para fraudadores modificarem. Portanto, o artigo oferece uma visão atual sobre aplicações envolvendo Criptomoedas e mostra o quão eficazes são essas soluções modernas referentes a transações de capital.
Palavras-chave: 1. Blockchain; 2. Smart Contracts; 3. Crowdfunding; 4. Criptomoedas

GET TOGETHER: STUDY AND IMPLEMENTATION OF A BLOCKCHAIN APPLICATION USING SMART CONTRACTS

Abstract
The evolution of technology is increasingly rapid and has a direct impact on society - the way people view money has changed dramatically, and technology has begun to affect the economy with the birth of Bitcoin, the first Cryptomane in the world, which was initially proposed in 2008 and in 2018 inspired this article. This work aims to develop a Crowdfunding application prototype, making use of Blockchain and able to process Smart Contracts within the Ethereum Network, in order to demonstrate the effectiveness of the application of methods, techniques and tools appropriate to this modern technology context. For the development of the solution, the Criptomoeda Ethereum, totally digital and decentralized, was admitted. Using an API provided by Ethereum, web3, it was possible to write the transactions in Blockchain and, for a user-friendly interface, the React.js library was used. In parallel, to make viable the writing of

[1] Graduação em Ciência da Computação pelo Centro Universitário Salesiano São Paulo – Lorena. Email: pedro.cds@outlook.com
[2] Mestrado em Engenharia Eletrônica e Computação pelo ITA e docente na Fatec Prof. Waldomiro May. Email: walmir.duque@fatec.sp.gov.br

the contracts, the language Solidity, based on Javascript, was used. As a result of the work, a decentralized electronic transaction system that does not require an intermediary, which has digital signatures that allow strong control over property double expense prevention, is achieved through a peer-to-peer network that uses proof of work to create a public record, which is impractical for fraudsters to modify. Therefore, the article offers a current insight into applications involving Cryptomanes and shows how effective these modern solutions are for capital transactions.
Keywords: *1. Blockchain; 2. Smart Contracts; 3. Crowdfunding; 4. Criptomanes*

INTRODUÇÃO

O comércio na Internet passou a depender quase exclusivamente de instituições financeiras que servem como "terceiros confiáveis" para processar pagamentos eletrônicos. Enquanto o sistema funciona bem para a maioria das transações, ainda sofre das fraquezas inerentes do modelo baseado em confiança.

As instituições financeiras atuam como uma "contraparte" confiável para facilitar a transação, mas elas gastam tempo resolvendo disputas e lidando com transações fraudulentas. Isso, obviamente, aumenta o custo de se performar uma transação por meio da Internet e torna as transações relativamente caras.

Hoje existe uma versão "*Peer-to-peer*" de dinheiro eletrônico que permite pagamentos on-line enviados diretamente de uma parte para outra sem passar por uma instituição financeira.

Em um sistema *Peer-to-peer* as transações criptográficas serão computacionalmente impossíveis de serem revertidas, protegendo assim os usuários contra qualquer tipo de fraude nas transações. Este sistema de dinheiro (Criptomoeda) *Peer-to-peer* ainda é capaz de resolver um problema antigo, que é o "gasto duplo", ou seja, quando se performam duas transações online simultaneamente com uma mesma moeda.

O sistema dessas chamadas Criptomoedas funciona com uma cadeia de assinaturas digitais (*Blockchain*), que podem ser passadas de uma pessoa para outra, utilizando uma assinatura eletrônica (Hash). Durante esse processo, o remetente da moeda assina eletronicamente as transações passadas e também a chave pública do receptor para quem está enviando aquela moeda.

Analogamente, seria como assinar o recebimento de uma encomenda e, então, escrever um endereço para onde a encomenda deverá ser enviada, mantendo assim sempre validadas as transferências pelos próprios mantenedores das moedas. Esse registro histórico das transações

cria a Blockchain das Criptomoedas, que é essencialmente um livro contábil de todas as transações de Criptomoedas que ocorreram até então.

Visando contornar problemas com moeda e instituições no ambiente de Crowdfunding, este artigo mostra uma nova visão sobre os meios de pagamento e transações no mundo das Criptomoedas, como funcionam e onde podem ser aplicadas.

Em face do cenário supracitado das Criptomoedas, este trabalho tem por objetivo desenvolver um protótipo de aplicação *Crowdfunding* fazendo uso da *blockchain*, que possa ser capaz de processar *Smart Contracts* dentro da *Ethereum Network*, a fim de demonstrar a efetividade da aplicação de métodos, técnicas e ferramentas adequadas a esse contexto moderno de tecnologia.

2 CRIPTOMOEDAS E BLOCKCHAIN

A base teórica deste artigo consiste em Criptomoedas e Blockchain – técnicas e métodos de desenvolvimento serão explicitados e justificados na seção 2, metodologia, deste trabalho.

2.1 Criptomoedas

A evolução da tecnologia é cada vez mais rápida e tem impacto direto no mundo e em várias áreas da sociedade, visando sempre melhorá-la e/ou simplificá-la. O modo da sociedade de ver o dinheiro mudou drasticamente e a tecnologia começou a afetar diretamente a economia com o nascimento do Bitcoin, a primeira Criptomoeda descentralizada do mundo – Bitcoin foi inicialmente apresentada em 2008 na “The Cryptography Mailing List” (Um grupo de discussão sobre criptografia).

Um usuário conhecido somente pelo seu pseudônimo, Satoshi Nakamoto fez uma proposta no mínimo interessante, a criação de uma moeda virtual descentralizada. Segundo Satoshi:

> O que é preciso é um sistema de pagamentos eletrônicos baseado em provas criptográficas em vez de confiança, que permita que duas partes interessadas em fazer transações diretamente façam-nas sem a necessidade de um intermediário confiável. Transações que são computacionalmente impraticáveis de reverter podem proteger vendedores de fraude, e serviços de proteção poderiam ser facilmente implementados para proteger os compradores (algo como PagSeguro, Paypal ou MercadoPago fazem atualmente).” (SATOSHI, 2008, The Cryptography Mailing List)

Após o lançamento da moeda em 2009 e a declaração de que seu código seria *open-source*, outras moedas começaram a surgir e desenvolvedores começaram a estudar a tecnologia a fim de desenvolver aplicações capazes de realizar transações com criptomoedas. Atualmente existem mais de 1195 versões de Criptomoedas, de acordo com o site de empreendedores startse.com (fonte: coinmarketcap.com) e o mercado tende a crescer cada vez mais. A chave do sucesso das criptomoedas é a Blockchain, assunto a ser tratado na próxima sub-seção.

2.2 Blockchain

Blockchain trata de uma tecnologia que viabiliza as criptomoedas – é na *Blockchain* que são feitas, armazenadas e replicadas as transações. Essa foi a grande invenção por trás do sistema das moedas e o futuro da *Blockchain* aponta outros usos além do financeiro. Segundo Don Tapscott (Blockchain Revolution p.10) a *Blockchain* é conhecida por revolucionar a era digital:

> A tecnologia que, provavelmente, terá o maior impacto sobre o futuro da economia mundial chegou, e não são carros autodirigidos, energia solar ou inteligência artificial. Essa tecnologia é conhecida por Blockchain. A primeira geração da revolução digital nos trouxe a internet da informação. A segunda geração – impulsionada pela tecnologia do Blockchain – está nos trazendo a internet do valor: uma nova plataforma distribuída que pode nos ajudar a remodelar o mundo dos negócios e a transformar a velha ordem dos assuntos humanos para melhor.

Uma definição interessante do conceito na era 1.0 da Blockchain foi citada por Vitalik Buterin, co-fundador da Ethereum, capturando o sentido amplo do que é uma *Blockchain*:

> Uma blockchain é um computador mágico para o qual qualquer pessoa pode fazer upload de programas e deixar os programas auto-executáveis, onde o estado atual e todos os anteriores de cada programa são sempre publicamente visíveis, e que possui uma garantia criptoeconômica muito forte de que programas rodam em execução. A cadeia continuará a executar exatamente da maneira que o protocolo blockchain específica. (Buterin 2015, 1)

Pilkington (2015) argumenta que essa definição carece de rigor científico, pois "computador mágico" é um termo discutível - transmite a ideia de que as aplicações executadas em tal plataforma têm um alcance global: "sem fronteiras nacionais ou geopolíticas, e se estendem sem limites para o futuro" (Davidson, De Filippi en Potts 2016, 8). No entanto, essa definição é interessante para os recursos que ela omite.

O uso abstrato de tal definição permite que Buterin (2015) enfatize a ideia de que *blockchain* é "informacional e processual" (Pilkington, 2015). Além disso, a definição carece

de termos financeiramente carregados, tais como: razão, dinheiro, criptomoeda, transações e taxa de hash.

Buterin (2015) complementa sua própria definição dizendo "… eles são [Blockchains] sobre a liberdade de criar um novo mecanismo com um novo conjunto de regras extremamente rápido e empurrá-lo para fora. Eles são Lego Mindstorms para construir instituições econômicas e sociais".

O importante para a visão geral de Buterin (2015) é que as *Blockchains* não precisam se relacionar com uma esfera monetária. Como explica Pilkington (2015), os conceitos de "Criptoeconomia" e "finalização de pagamento" não definem a *Blockchain*, mas são características fundamentais das aplicações *Blockchain*. Consequentemente, a visão de Buterin (2015) prediz que *Blockchains* podem existir sem tokens subjacentes.

Há uma nuance, no entanto: "a moeda é necessária para fazer com que blocos de criptografia funcionem…". Mas a moeda está lá simplesmente como encanamento econômico para incentivar a participação consensual, manter depósitos e pagar taxas de transação, não como o ponto central da mania especulativa, interesse do consumidor e excitação" (Buterin, 2015).

Gideon Greenspan apoia a visão de Buterin, afirmando que:

> Se modificarmos nosso esquema de" banco de dados" para que cada linha possa representar vários ativos, em vez da moeda nativa do *Blockchain*, poderemos nos livrar dessa moeda por completo. Isso nos deixa com uma *Blockchain* como uma forma de alcançar consenso e segurança em um aplicativo financeiro peer-to-peer para qualquer classe de ativo. (GREENSPAN 2015).

De qualquer forma, nem todos os especialistas concordam com a definição do *Blockchain*. Muitos parecem argumentar que *Blockchains* sem Tokens subjacentes não podem existir. "A moeda é parte integrante do mecanismo de incentivo da rede para manter sua segurança; os dois têm uma relação simbiótica existencial" (Swanson 2015, 8). Da mesma forma, Jeremy Allaire diz que: "Tem de haver um valor subjacente ao Token usado para mover o valor ..." (Allaire 2015).

Embora o debate ainda não tenha sido encerrado, pode-se argumentar que o último autor está fechando o tópico e deixa pouco ou nenhum espaço para a expansão do *Blockchain* em aplicativos não relacionados a finanças. Essas definições que limitam os bloqueios a uma esfera monetária têm menos interesse pelas aplicações Blockchain 3.0.

No entanto, todos os autores parecem concordar que a moeda é um aspecto importante nas *Blockchains*, seja sua representatividade apenas "Um encanamento econômico para incentivar a participação de consenso" ou uma parte inseparável e fundamental do processo. Por uma questão de pesquisa e raciocínio intelectual, este documento considera a definição de Buterin (2015) como uma base para a tecnologia Blockchain, sem prejudicar a importância da moeda na propagação da tecnologia em aplicações não financeiras.

Quanto ao seu funcionamento, a Blockchain trabalha como um livro caixa de todas as transações realizadas com as moedas e as armazena na rede. Sobre sua confiabilidade e persistência Muhammad Mannir Ahmad Getso (THE BLOCKCHAIN REVOLUTION AND HIGHER EUCATION p.57), Mestre em Engenharia de Sistemas de Computação afirma:

> O blockchain é uma tecnologia relativamente nova usada para verificar e armazenar registros de transações de criptomoedas on-line, como o Bitcoin. O sistema é redundante e distribuído, dificultando que as transações sejam rescindidas, duplicadas ou falsificadas. Além de moedas on-line, o blockchain tem usos potenciais em saúde, educação e muitos outros campos.

A *Blockchain* realmente é muito poderosa e segura pelo fato de os dados serem replicados a todo momento e cada nó de sua cadeia possuir uma cópia completa de toda base de dados, sempre visando proteger as transações nela realizadas, um outro grande benefício dessa tecnologia é o chamado P2P, que elimina a necessidade de um intermediário nas transações. Muhammad Mannir Ahmad Getso (The Blockchain Revolution and Higher Eucation p. 58) diz que: "A Blockchain funciona como uma plataforma global, distribuída e altamente segura, um banco de dados onde poderíamos armazenar e trocar coisas de valor e onde poderíamos confiar uns nos outros sem intermediários no processo".

3 METODOLOGIA

3.1 Divisão das Tecnologias

O desenvolvimento do projeto e o uso de seus materiais e métodos foram divididos em dois setores: *Front-end* e *Back-end*. No setor Front-end foram dispostas tecnologias referentes a interface onde o usuário terá contato com o aplicativo, definindo estruturas visuais e construindo a navegação entre telas.

No setor do Back-end foi construída toda a lógica da aplicação, como a escrita do *Smart Contract* responsável pelas transações e a conexão da aplicação com a rede *Ethereum* e sua *Blockchain*. No setor do Front-end com foco em facilidade de acesso e performance, a aplicação foi desenvolvida com interface voltada totalmente para a web fazendo uso da biblioteca *React* para o Front-end, seguindo padrões modernos de UX e design, para que o usuário não se intimide com essa tecnologia complexa.

3.2 O Back-end

Para o desenvolvimento do Back-end da aplicação foi necessário um grande estudo sobre a arquitetura utilizada, pois trata-se de uma tecnologia completamente nova que se encontra no início de seu desenvolvimento.

Graças à Ethereum network e seu forte apreço por desenvolvedores, a API escrita em JavaScript Web3 foi escolhida para a interação com a rede e a Blockchain - por ser criada pela própria comunidade *Ethereum*, fornece uma base sólida de ferramentas de interação, envio e recebimento de dados por meio de chamadas RPC.

3.2.1 Web3

Quanto à API responsável por interagir com a Blockchain Ethereum, a melhor opção no mercado é o Web3.js, uma api desenvolvida pelos próprios criadores da *Ethereum Network*.

O Web3.js funciona com qualquer nó Ethereum, que expõe uma camada RPC. O Web3 também contém o objeto eth - web3.eth (especificamente para interações blockchain Ethereum) e o objeto shh - web3.shh (para interação Whisper). Para efetivar transações e realizar testes na aplicação foi utilizada uma sub-rede da Ethereum chamada de rinkeby, que facilita a obtenção da moeda.

3.2.2 Solidity

Como linguagem chave foi utilizada a *Solidity*, essencialmente uma linguagem de programação para escrever *Smart contracts*. Com o *Solidity*, é possível criar aplicativos que simulem uma campanha de financiamento coletivo, uma loteria, um empréstimo ou qualquer

outro tipo de instrumento financeiro. O *Solidity* é conhecido por ser bastante semelhante ao *Javascript* e excepcionalmente fácil de aprender para quem tem experiência anterior em JS.

Para interagir com a rede *Ethereum* foi utilizado um plugin do Chrome chamado *Metamask*, que funciona como uma espécie de carteira para armazenar *Ethereum*.

3.2.3 Web3 - Solidity

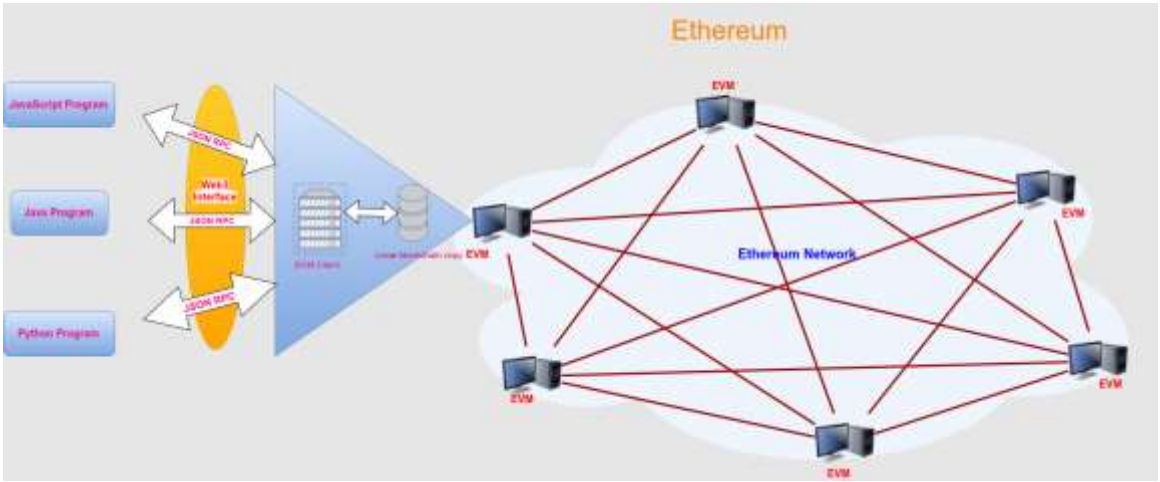
Existem aspectos diferentes a serem considerados no desenvolvimento de aplicações *Blockchain* com *Ethereum*, tais como, por exemplo:

- Desenvolvimento de contrato inteligente (*Smart Contract*) - código de escrita que é implantado no *Blockchain* com a linguagem de programação *Solidity*.
- Desenvolvimento de sites ou clientes que interagem com o *Blockchain* – escrita do código que lê e grava dados do *Blockchain* com contratos inteligentes.

O Web3.js permite cobrir a segunda responsabilidade citada anteriormente: desenvolver clientes que interagem com a *Etherem Blockchain*. O Web3.js é uma coleção de bibliotecas que permitem realizar ações como enviar Ether de uma conta para outra, ler e gravar dados de contratos inteligentes, criar contratos inteligentes e muito mais. Basicamente pode-se usar o Web3.js para ler e gravar na Ethereum Blockchain.

Para que isso fique mais claro, o entendimento do Web3.js interagir com o *Blockchain Ethereum*, a seguir apresenta-se a Figura 01 está um diagrama de como um cliente fala com *Ethereum*:

Figura 01 – Interação Web3.js e Ethereum



Fonte: Website Ethereum (2018)

Web3.js “fala” com a Blockchain Ethereum via JSON RPC, que significa "Remote Procedure Call" - trata-se de um protocolo para as chamadas da rede. Ethereum é uma rede Peer-to-peer de nós que armazena uma cópia de todos os dados e códigos no Blockchain. O Web3.js permite realizar solicitações a um nó Ethereum individual com JSON RPC para ler e gravar dados na rede.

Quanto à primeira responsabilidade citada acima é possível contar com o *SolidityJS* (Linguagem orientada a contratos), que nada mais é do que uma linguagem feita para escrever *Smart Contracts*. Pode-se pensar que é uma forma de controlar uma conta bancária com código. Totalmente baseada em Javascript, oferece uma facilidade de aprendizado para quem já teve contato com a linguagem.

A *Solidity* foi inicialmente proposta em agosto de 2014 por Gavin Wood. A linguagem foi posteriormente desenvolvida pela equipe de Solidity do projeto Ethereum, liderada por Christian Reitwiessner. É uma das quatro línguas (sendo as outras Serpente, Viper (experimental) e Mutan (depreciado) destinadas a atingir a Máquina Virtual Ethereum (EVM).

Atualmente, o Solidity é o idioma principal do Ethereum, bem como em outros Blockchains privados executados em plataformas que competem com o Ethereum, como o Monax e sua Blockchain Hyperledger Burrow, que usa o Tendermint para obter acesso.

3.2.4 Metamask

MetaMask é um plugin desenvolvido para ser utilizado no Google Chrome e FireFox que permite que um usuário rode *Ethereum Apps* diretamente no seu navegador sem executar um nó completo na *Ethereum Network*.

O *MetaMask* inclui um cofre de identidade seguro, fornecendo uma interface de usuário para gerenciar suas identidades em sites diferentes e assinar transações *Blockchain*.

O *MetaMask* desempenha um papel importantíssimo para a Criptomoeda *Ethereum* pois tem a missão de tornar o *Ethereum* mais fácil de usar para o maior número de pessoas possível.

3.2.5 Ethereum Network

A Ethereum Network: É uma plataforma descentralizada capaz de executar contratos inteligentes (*Smart contracts*) e aplicações descentralizadas, fazendo uso da tecnologia

Blockchain. São aplicações que funcionam exatamente como programadas, gerando assim confiabilidade nos sistemas, sem qualquer possibilidade de censura, fraude ou interferência de terceiros. Isso porque o contrato (*Smart contracts*) é imutável.

Em sua base possui uma máquina virtual descentralizada Turing completude, a chamada *Ethereum Virtual Machine* (EVM), que pode executar scripts usando uma rede internacional de nós públicos (Blockchain). Pode-se entender a Blockchain como uma tecnologia que é capaz de armazenar registros de transações em um arquivo que funciona como uma espécie de planilha pública distribuída e de segurança garantida por criptografia. As transações publicadas na Blockchain são verificadas e validadas pelos próprios usuários num processo conhecido como mineração.

A mineração ocorre via execução de códigos de natureza criptográfica, sendo assim, o sistema pode funcionar num protocolo distribuído recompensando seus usuários pelo poder computacional empregado por eles. Contratos inteligentes "assinados" no Blockchain do Ethereum e a mineração são pagos em Ether, o combustível da plataforma.

O Ethereum foi fundado por Vitalik Buterin em janeiro de 2014, e formalmente apresentado para a comunidade na forma de um White Paper (assim como o Bitcoin). A definição formal da Virtual Machine do Ethereum (EVM) foi escrita por Gavin Wood.

O ponto que torna o Ethereum diferente da moeda digital mais difundida do mundo (o bitcoin), é que o Ethereum visa levar a tecnologia do Blockchain e os contratos inteligentes para "tudo" que possa ser programado.

O princípio é que toda transação, execução de código e registro, assinatura de contrato digital, ou qualquer outra aplicação que seja executada na rede do Ethereum seja paga em Ether, sendo assim, o Ethereum pode ser considerado um grande computador onde os usuários pagam pela quantidade de recurso utilizado.

O Ether é uma moeda digital utilizada dentro da plataforma do Ethereum para rodar os contratos inteligentes, serviços computacionais dentro da rede e para pagar taxas aos mineradores. O Ether é negociado nas corretoras com o código ETH.

3.3 Front-End

O React JS, que surgiu em 2011, é o responsável por todo o setor do front-end. React foi desenvolvido por engenheiros de software do Facebook. A primeira implementação do React foi na timeline do próprio Facebook, no mesmo ano de 2011; um ano mais tarde seu uso

também foi implementado no feed do Instagram. O React é uma biblioteca open source, em JavaScript, usada para construção de interfaces.

Por ter um objetivo muito bem definido, ele é capaz de realizar essa tarefa com excelência, principalmente em relação a manipulação do DOM (Document Object Model), afinal, trata-se de uma biblioteca focada em construção de interfaces e uma de suas maiores qualidades deve ser manipular o DOM. É nesse quesito que o React se destaca e é por isso que ele é tão utilizado atualmente.

Um dos grandes diferenciais do React é o Virtual-DOM. O v-dom é uma técnica simples e complexa ao mesmo tempo. Simples no conceito e complexa na aplicação. Simples porque ela é apenas uma representação em JavaScript puro (memória) do DOM "real". A manipulação do dom não é algo "produtivo", é extremamente lento e causa vários problemas nas aplicações. Então com v-dom passamos a manipular esse objeto e não o DOM real. Quando o objeto v-dom é atualizado um algoritmo calcula a diferença entre o v-dom e o DOM real, alterando então partes do DOM. É muito mais produtivo alterar os elementos DOM no JavaScript, processa-los e "aplicar de uma vez" na Árvore DOM do navegador. React veio com o objetivo de facilitar isso.

Para entender melhor o motivo do React facilitar o desenvolvimento e ser aplicado nesse projeto, é necessário falar sobre web componentes. Trata-se de uma técnica que vem sendo discutida desde 2009. Componentes Web são um conjunto de normas atualmente sendo produzidas por engenheiros do Google que permitem a criação de componentes reutilizáveis em documentos e aplicações web. A intenção por trás deles é trazer a engenharia de software baseada em componentes para a web.

Um web component tem a capacidade de criar Custom Tags HML que encapsulam estrutura (HTML), estilo (CSS) e comportamento (JavaScript). Pode-se entender como trechos de HTML reaproveitáveis.

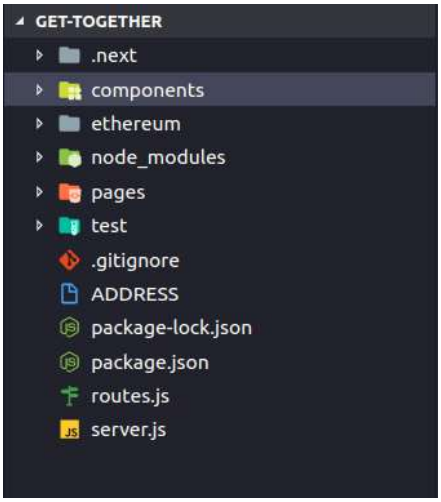
4 RESULTADOS E DISCUSSÃO

4.1. Resultados

Aplicando as ferramentas utilizadas e métodos apresentados o resultado do desenvolvimento foi uma interface simples, agradável e intuitiva para lidar com a aplicação. Quanto à estrutura do projeto, foram aplicadas as boas práticas de programação *Javascript*,

preconizadas pela biblioteca do React, resultando na árvore de pastas apresentada na Figura 02 a seguir:

Figura 02 – Árvore de Pastas do Projeto



Fonte: Os Autores (2018)

O ReactJS foi aplicado no design e nas rotas entre as páginas da aplicação, com transições suaves e um reaproveitamento de código baseado nos princípios dos Web Components. Um bom exemplo de componente reaproveitável no código da aplicação é visto na Figura 03 a seguir:

Figura 03 – Componente reaproveitável

```
render() {
  return (
    <Layout>
      <div>
        <h3>Campanhas em andamento</h3>

        <Link route="/campaigns/new">
          <a>
            <Button
              floated="right"
              content="Criar uma campanha"
              icon="add circle"
              primary
            />
          </a>
        </Link>

        {this.renderCampaigns()}
      </div>
    </Layout>
  );
}
}
```

Fonte: Os Autores (2018)

Uma vez apresentada a estrutura do projeto, serão mostradas as páginas implementadas do sistema. Em primeiro lugar, a Página inicial do sistema que contém todas as campanhas que foram cadastradas na plataforma, conforme visto na Figura 04 a seguir:

Figura 04 – Página inicial do sistema

Fonte: Os Autores (2018)

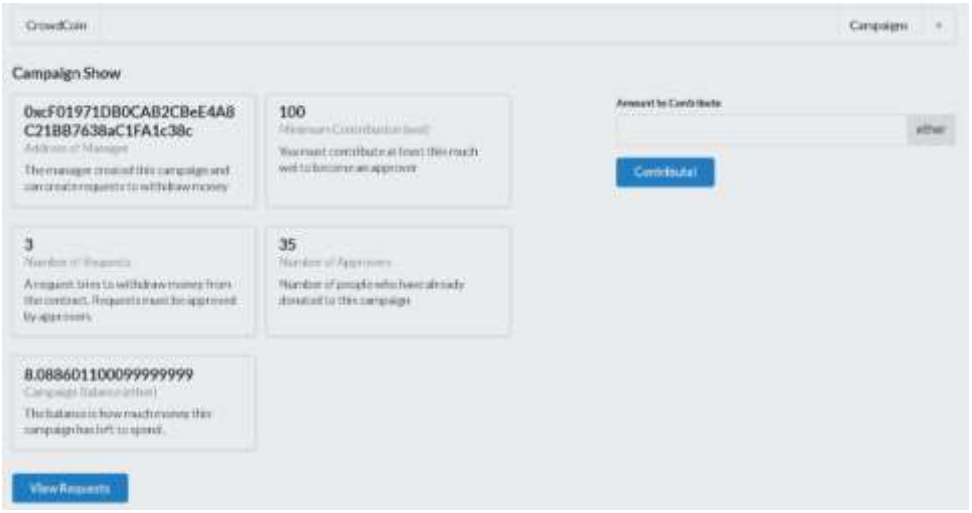
Em seguida, apresenta-se na Figura 05, a seguir, o Formulário de criação de campanha, em que o mantenedor deve definir um valor mínimo de contribuição para participar da campanha:

Figura 05 – Formulário de Criação de campanha

Fonte: Os Autores (2018)

Adiante, na Figura 06 é possível visualizar uma campanha - no primeiro campo pode-se ver informações sobre o mantenedor da campanha, no segundo campo pode-se ver informações sobre contribuição mínima para se tornar um aprovador de retiradas da campanha, no terceiro campo pode-se ver a quantidade de requisições de retirada existentes na campanha, no quarto campo pode-se ver o número de pessoas que realizaram doações para essa campanha e no quinto campo pode-se ver o valor em Ether que a campanha arrecadou até o momento. Para facilitar contribuições existe um campo na lateral direita da tela para que outros usuários possam contribuir com a campanha em questão com apenas um clique:

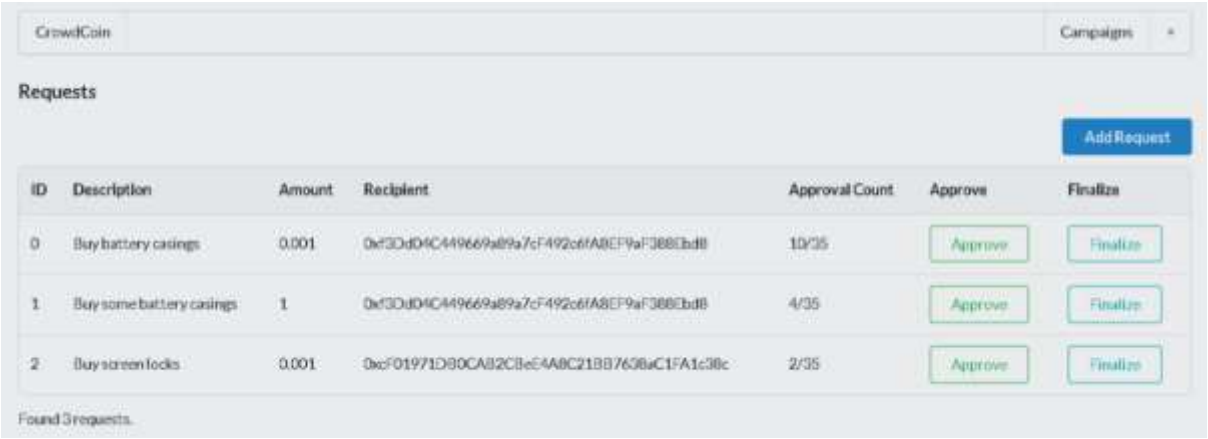
Figura 06 – Formulário de Visualização de campanha



Fonte: Os Autores (2018)

Uma nova tela, mostrada na Figura 07, permite que contribuintes com título de aprovadores possam localizar essa área no sistema – neste recurso pode-se ter acesso às requisições de retirada de fundo das campanhas que participam e podem decidir se concordam com as retiradas ou não:

Figura 07 – Consulta e Aprovação de Requisições de Retirada de Fundos



Fonte: Os Autores (2018)

Por fim, na Figura 08, é mostrada uma tela do sistema na qual o mantenedor poderá solicitar retiradas, preenchendo devidamente os campos solicitados e oferecendo uma breve descrição sobre o motivo de tal retirada:

Figura 08 – Criação de Requisição de Retirada de Fundos das Campanhas

Fonte: Os Autores (2018)

4.2. Discussão

Ao finalizar esse projeto, alguns resultados eram esperados como funcionalidades perceptíveis na aplicação implementada:

- Um sistema eletrônico de transação descentralizado que não necessita de um intermediário;
- Assinaturas digitais que permitem forte controle sobre propriedade e o gasto duplo é prevenido;
- Uma rede Peer-to-peer que utiliza prova de trabalho sendo usada para criar um registro público que é impraticável para fraudadores modificarem.

O esperado com o desenvolvimento da aplicação foi obter a possibilidade de passar adiante informações e conhecimento sobre este tema, que gera tanto interesse atualmente. Foi discutido que o desenvolvimento deste projeto é apenas um dos meios em que se pode aplicar soluções financeiras no atual mundo das Criptomoedas. Essa área tende a mudar muito a forma como o dinheiro e as transações financeiras serão tratadas daqui para a frente e isso causa um impacto enorme na vida das pessoas, tornando assim este assunto tão importante para todos.

Foi avaliado também que o resultado da aplicação foi muito positivo e confiável em relação ao uso das tecnologias citadas. Transações realizadas numa Blockchain se mostraram totalmente confiáveis e irreversíveis, economizando tempo e dinheiro e solucionando grandes problemas em relação ao modelo atual de transações (baseado em confiança), garantindo assim que as pessoas que fazem uso dessa tecnologia possam desfrutar de um padrão de segurança altíssimo.

CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo construir uma aplicação Blockchain usando Smart Contracts – para tal, foi usado um caso de *Crowdfunding* em que o doador pode participar mais nas decisões das campanhas, tornando, assim, um aplicativo mais confiável e atraente para esse público-alvo.

O trabalho também ofereceu uma visão atual sobre aplicações envolvendo Criptomoedas e mostrou que podem ser consideradas plausíveis essas modernas soluções referentes a transações e manipulação de capital. Percebeu-se, também, seu vasto espectro de aplicação como, por exemplo, loterias, bancos e até a área de logística, em uma transportadora, na qual aplicações devessem rastrear algum objeto ou carga.

As tecnologias empregadas na construção da solução demonstraram ser tecnicamente apropriadas e ofereceram um bom resultado ao permitir entregar, de fato, as funcionalidades requeridas pela aplicação: a prática integração de Web3 com *Blockchain* viabiliza a interação com Ethereum. Em consonância com a Web3, a Solidity facilitou a construção de Smart Contracts. Em termos de front-end, o React altamente direcionado a manipulação do DOM, mais especificamente V-DOM, viabiliza web components. Percebe-se, em todas essas tecnologias, a presença forte e crescente do "JavaScript" como um padrão, tanto no back quanto no front-end.

Por meio das tecnologias citadas, esse trabalho também apresentou a importância de se utilizar criptografia (por sua segurança e confiabilidade) e que os dados sejam de conhecimento público, diferentemente das instituições financeiras tradicionais: permite-se transparência e evita-se fraudes no mercado financeiro, ao se eliminar custos extras com transações e resolver problemas como o gasto duplo (uso de uma mesma moeda digital mais de uma vez).

REFERÊNCIAS

BUTERIN, V. (2015, Agosto 21). **An Introduction to Futarchy.** Acesso em: 15 abr 2018, Ethereum Blog: https://blog.ethereum.org/2014/08/21/introduction-futarchy/

BUTERIN, V. (2015, May 6).
DAOs, DACs, DAs and More: An Incomplete Terminology Guide. Acesso em: 15 abr 2018, Ethereum Blog: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-anincomplete-terminology-guide/

Bitcoin White paper. Disponível em: <https://bitcoin.org/bitcoin.pdf >. Acesso em: 23 mar 2018.

Conteúdo oficial relacionado ao Bitcoin. Disponível em: <https://bitcoin.org/pt_BR/ >. Acesso em: 24 mar 2018.
Conteúdo oficial relacionado ao Ethereum. Disponível em: <https://www.ethereum.org/>. Acesso em: 24 mar 2018.
Conteúdo oficial relacionado a react. Disponível em: <https://reactjs.org/>. Acesso em: 2 abr 2018.
Conteúdo oficial relacionado a web3js. Disponível em: <https://web3js.readthedocs.io/en/1.0/>. Acesso em: 8 abr 2018.
Conteúdo oficial e github relacionado a Solidity. Disponível em: <https://github.com/ethereum/solidity>. Acesso em: 12 abr 2018.
Conteúdo oficial relacionado a Metamask. Disponível em: <https://metamask.io/>. Acesso em: 15 abr 2018.
Ethereum White paper. Disponível em: <https://github.com/ethereum/wiki/wiki/White-Paper>. Acesso em: 26 mar 2018.
Github oficial React. Disponível em: < https://github.com/facebook/create-react-app>. Acesso em: 4 abr 2018.
Github oficial web3js. Disponível em: <https://github.com/ethereum/web3.js/>. Acesso em: 8 abr 2018.
Github oficial Metamask. Disponível em: < https://github.com/MetaMask>. Acesso em: 8 abr 2018.
LOMBA, ALEX **Ethereum: O Guia de Insider Completo Para Universo de Ethereum Abrangente Que, Desde Programação, Mineração Até Contratos Inteligentes, Investimento, Negociação E Tecnologia Blockchain.** 7 mar 2018.