Blockchain para dispositivos móveis: Implementação de um aplicativo peer-to-peer em rede local para negociação de criptomoeda

Leonardo Amorim de Oliveira[1], Dr. Antonio Luiz Basile[1]

[1]Faculdade de Computação e Informática (FCI) – Universidade Presbiteriana Mackenzie – São Paulo, SP – Brasil

leonardoamorim.oliveira@mackenzista.com.br, albasile2@gmail.com

Abstract. *It is believed that cryptocurrencies will lead into a new economic and technological evolution, thanks to its base technology: the Blockchain. The technology, which can be described as a distributed ledger, is still poorly known by the comom population and even by cryptocurrencies users and investors. This article presents the result of a research about the technology and proposes to develop a Blockchain driven cryptocurrency trading app for iOS mobile devices connected in a local network, aiming to bring the end user closer to the technology's procedures. Although limited by the local peer-to-peer network, Blockchain implementation on mobile devices is possible and scalable.*

Resumo. *As criptomoedas apresentam-se como uma nova evolução econômica e tecnológica, graças a sua tecnologia base: o Blockchain. A tecnologia, que pode ser descrita como um livro razão distribuído, ainda é pouco conhecida pela população e até mesmo pelos usuários e investidores de criptomoedas. Este artigo apresenta uma pesquisa a cerca da tecnologia e se propõe a desenvolver um aplicativo de negociação de criptomoeda para dispositivos móveis iOS em rede local com a tecnologia Blockchain, a fim de aproximar o usuário final aos processos da tecnologia. Mesmo que limitada por conta da rede peer-to-peer local, a implementação em dispositivos móveis é viável e escalável.*

1. Introdução

1.1. Contextualização e Relevância do Tema

Tradicionalmente, moedas são controladas por governos e transações eletrônicas são realizadas por intermédio das instituições financeiras. O economista e vencedor do prêmio Nobel, Douglass North (1920-2015) discorreu em sua tese que instituições são agentes de confiança para reduzir incertezas, a fim de conectar partes e permitir a troca de valor [Warburg 2016].

As criptomoedas tornaram-se uma das principais promessas na revolução tecnológica e econômica do século XXI. Pela primeira vez na história, é possível reduzir incertezas em transações monetárias apenas com tecnologia, sem a necessidade de instituições políticas e financeiras [Warburg 2016]. As criptomoedas surgem a fim de

eliminar o intermédio de instituições em transações, permitindo a transferência direta entre dois indivíduos. Isso é possível graças a sua tecnologia inovadora: o Blockchain.

De modo breve, o Blockchain pode ser descrito como um grande livro-razão descentralizado, em que os dados registrados são auditáveis, legítimos e transparentes para todos. A tecnologia foi pioneiramente proposta por Satoshi Nakamoto (2008) em um artigo que introduz o Bitcoin ao mundo, juntamente com explicações sobre a composição de blocos, a construção de um histórico de dados com base em prova de trabalho computacional e validação de legitimidade com assinaturas digitais.

De acordo com o relatório "Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics", realizado pela crypto.com e liderado por Kevin Wang, o número global de usuários de criptomoedas atingiu 221 milhões em julho de 2021. Esse número representa aproximadamente 8 milhões de pessoas a mais que a população brasileira no último censo (213,3 milhões de habitantes), publicado pelo IBGE (Instituto Brasileiro de Geografia e Estatística) em agosto de 2021.

Além da impressionante quantidade de usuários, destaca-se a velocidade na qual as criptomoedas estão sendo adotadas. Foram necessários apenas quatro meses para dobrar a quantia global de usuários de criptomoedas de 100 milhões para 200 milhões, enquanto demoraram nove meses para crescer de 65 milhões para 100 milhões de usuários [Wang 2021].

Apesar dos holofotes na mídia e do grande número de usuários e investidores de criptomoedas, para muitas pessoas o conhecimento sobre o seu funcionamento e a sua tecnologia base, o Blockchain, é defasado ou inexistente. De acordo com uma pesquisa conduzida pela Crypto Literacy em 2021, 98% das pessoas não entendem conceitos básicos de criptomoedas.

Tendo em vista que a tecnologia base do Blockchain é muito distante do usuário final, que apenas utiliza, especula e negocia criptomoedas, expor o seu funcionamento pode ajudar na educação e conscientização de seus conceitos básicos. O uso do Blockchain em dispositivos móveis surge como alternativa para apresentar os seus processos em um nível próximo, dada a grande presença destes dispositivos no cotidiano e a sua fácil usabilidade e mobilidade. O Blockchain prova-se capaz de ser implementados em diferentes cenários técnicos, todavia é necessário estudá-lo para dispositivos móveis.

1.2. Objeto de Pesquisa

1.2.1. Contextualização do Problema de Pesquisa

A presença de dispositivos móveis no cotidiano não é novidade. Conforme relatado na PNAD Contínua TIC (Pesquisa Nacional por Amostra de Domicílios Contínua - Tecnologia da Informação e Comunicação) em 2018, 79,3% dos brasileiros com 10 anos ou mais têm aparelhos celulares para uso pessoal e 98,1% deste mesmo grupo acessam internet pelo celular. Dada estas estatísticas, introduzir o Blockchain em dispositivos móveis é uma oportunidade de promover a tecnologia e expor o seu funcionamento ao usuário final.

Entretanto, entender os conceitos que compõe o Blockchain e implementá-lo não é uma tarefa trivial. Existem vários processos complexos de criptografia, comunicação

entre pares e descentralização que tornam a compreensão e implementação desafiadores [Yaga et al. 2018]. Ademais, existem poucas referências teóricas e, principalmente, artigos acadêmicos sobre a implementação da tecnologia em dispositivos móveis com comunicação peer-to-peer para negociação de criptomoedas.

Do ponto de vista técnico, além da complexidade dos processos envolvidos no Blockchain, o desenvolvimento de aplicativos para dispositivos móveis possui um maior número de limitações do que outras plataformas, como computadores e websites, dada as peculiaridades do ambiente. Apesar do grande poder computacional que dispositivos móveis possuem atualmente, os processos do Blockchain podem ser complexos demais para estes dispositivos caso não sejam devidamente adaptados para o seu contexto.

Diante do cenário apresentado, as perguntas que serão respondidas nessa pesquisa são: quais as estruturas e os processos que compõe a tecnologia e como implementar o Blockchain em dispositivos móveis com comunicação entre pares para a negociação de criptomoeda?

1.2.2. Hipótese

Sabe-se que o Blockchain não passa de estruturas e processos com uma finalidade, como diversas outras tecnologias e teorias presentes no campo da ciência da computação. Do ponto de vista da plataforma, linguagem de programação Swift (voltada para dispositivos móveis que suportam o sistema operacional iOS) possui bibliotecas de criptografia (CryptoKit) e de comunicação ponto-a-ponto (MultipeerConnectivity) que viabilizam diversos processos complexos. Ademais, existem implementações da tecnologia em outras plataformas. Portanto, acredita-se ser possível implementar o Blockchain em dispositivos móveis com comunicação ponto-a-ponto para a negociação de criptomoeda.

1.3. Objetivos do Estudo

1.3.1. Objetivo Geral

O objetivo principal deste projeto é compreender a tecnologia Blockchain, estudando as suas estruturas e processos, e desenvolver um aplicativo de negociação de criptomoeda para dispositivos móveis iOS em rede local com a tecnologia Blockchain. O aplicativo será publicado em repositório público, permitindo o compartilhamento de conhecimento.

1.3.1. Objetivos Específicos

O projeto visa compreender as estruturas e processos da tecnologia Blockchain e estudar as adaptações necessárias ao modelo de Nakamoto para a sua implementação em dispositivos móveis.

Por fim, propõe-se que o Blockchain seja implementado em um aplicativo para dispositivos móveis (que suportem o sistema operacional iOS) para a negociação de uma criptomoeda fictícia, de maneira que o usuário final seja apresentado aos processos da tecnologia e à composição das suas estruturas. No caso deste presente trabalho, a comunicação ponto-a-ponto será exclusiva à rede local, uma vez que o foco está no Blockchain, ao invés do desenvolvimento da tecnologia ponto-a-ponto.

1.4. Justificativa

O uso e investimento em criptomoedas é inevitável e a tecnologia Blockchain apresenta-se como uma evolução na maneira na qual se transaciona valores, a ponto de existirem previsões que ela transformará o sistema econômico de maneira radical. Dado a presença massiva de dispositivos móveis na sociedade civil, é uma estratégia interessante aproveitar-se do seu alcance para apresentar e difundir o Blockchain. Portanto, é importante estudar o funcionamento do Blockchain ao desenvolver um aplicativo que ofereça a interações com uma criptomoeda, como negociação e visibilidade das estruturas.

Do ponto de vista acadêmico, este artigo contribui no estudo de Blockchain e sua implementação para dispositivos móveis. O tema por si só é limitado a uma quantidade pequena de artigos, e esta limitação é ainda maior no contexto brasileiro (baixo número de dissertações em português), e quando o assunto é implementação para dispositivos iOS.

1.5. Delimitação do Estudo

- Delimitação por Sistema Operacional: Este estudo limita-se a usuários de dispositivos móveis (celulares) que utilizem o sistema operacional iOS, da Apple Inc.
- Delimitação por Rede: Este estudo limita-se a comunicação ponto-a-ponto em rede local (wi-fi ou bluetooth).

2. Referencial Teórico

No sistema econômico atual, transações são necessariamente intermediadas por uma terceira parte. O intermediário tem como objetivo validar e garantir os valores transacionados, agindo como um agente de confiança e reduzindo as incertezas ao redor da negociação [Warburg 2016]. Porém, as ferramentas críticas e as burocracias ao redor dos processos efetuados por essas instituições terceiras limitam a agilidade e benefícios da transformação digital da economia [Iansiti e Lakhani 2017].

O artigo “Bitcoin: A Peer-to-Peer Electronic Cash System”, publicado pelo pseudônimo Satoshi Nakamoto em 2008, introduziu os conceitos de Blockchain e moeda criptografada (origem do termo criptomoeda) [Ribeiro e Mendizabal 2019]. Nele, foi proposto a criptomoeda Bitcoin em um sistema de pagamento eletrônico baseado em prova criptográfica, ao invés de uma terceira parte de confiança, permitindo que duas partes negociem diretamente entre si [Nakamoto 2008].

O Blockchain pode ser definido como um banco de dados distribuído, ou livro-razão público, de todos os eventos digitais (transações, por exemplo) executados e compartilhados entre as partes em questão [Crosby et al. 2016]. Autoridades centrais, como instituições políticas ou financeiras, não desempenham nenhum papel [Davis 2011].

O Blockchain é uma tecnologia complexa e ainda extremamente jovem. No entanto, ela possui cinco princípios muito bem fundamentados: distribuição dos dados, comunicação descentralizada, transparência, imutabilidade e validação por prova de trabalho criptográfico. Estes tópicos serão explorados em meio as definições de estruturas e processos, nas subseções a seguir.

2.1. Corrente de Blocos

A definição técnica e arquitetura do Blockchain é descrita em seu próprio nome, de maneira literal: uma corrente de blocos. Ele é um arquivo digital constantemente atualizado e disponível para todos os participantes [Ribeiro e Mendizabal 2019].

Para um dado ser armazenado, é criado um bloco. Este, por sua vez, passa por uma prova de trabalho criptográfico (processo o qual será aprofundado na subseção 2.5) e, em seguida, é validado por todos os participantes da rede [Chaves 2021]. Por fim, caso a validação ocorra com sucesso, o bloco é inserido ao final da corrente. Uma vez que o bloco é adicionado na corrente, ele passa a fazer parte do sistema [Ribeiro e Mendizabal 2019]. Além do mais, destaca-se que o primeiro bloco do Blockchain é chamado de Gênesis e nenhum bloco o precede [Singh e Kumar 2021].

2.2. Blocos

O bloco é a estrutura que armazena um dado ou um conjunto de dados, como uma série de transações, por exemplo. Cada bloco possui um hash, criado a partir de todas as propriedades que compõe o bloco [Ribeiro e Mendizabal 2019].

Dado um Blockchain de criptomoeda (como o do Bitcoin, por exemplo), as informações que constituem um bloco são: o conjunto de transações, uma estampa temporal, um nonce (número resultante da prova criptográfica, que será aprofundado na subseção 2.5) e o hash do bloco anterior [Nakamoto 2008]. Uma vez que cada bloco possui o hash do bloco anterior, cria-se um elo entre os blocos, resultando na corrente (o Blockchain) [Lyra 2019]. Ainda, caso seja realizada qualquer alteração no bloco, o seu hash será alterado, e, consequentemente, o hash do bloco sucessor também. Por este motivo, o Blockchain é praticamente imutável.

2.3. Transações

As transações são processos em que ocorre a mudança intencional de posse de uma ou um conjunto criptomoedas. Essas moedas criptográficas, por sua vez, são uma corrente de assinaturas digitais [Nakamoto 2008]. As partes envolvidas em uma transação utilizam assinaturas digitais, com chaves públicas e privadas, para assinar digitalmente e realizar a operação de maneira segura [Yaga et al. 2018]. Ademais, a implementação de chaves públicas e privadas possibilita a validação e auditoria da transação por outros participantes da rede.

Dada a sua origem e a crescente popularidade das criptomoedas, o Blockchain é comumente relacionada a este fim. Entretanto, a sua aplicação estende-se a outros registros de finanças, dados de saúde, gerenciamento de cadeia de suprimentos, monitoramento de mercado, energia inteligente, proteção de direitos autorais etc. [Xu, Chen e Kou 2019].

2.4. Rede Peer-to-Peer

O Blockchain é uma tecnologia distribuída, ou seja, não é centralizada em um único computador. Os seus registros são regulados e mantidos por uma rede de computadores, onde cada um dos seus participantes (nós da rede) possui uma cópia de todos os registros [Deloitte 2016]. Destaca-se que não há um único nó com controle total e não é possível alterar ou deletar os seus dados [Sarmah 2018]. Desta forma, é construído um

histórico imutável e descentralizado [Arruñada e Garicano 2018], além de passível de verificação e auditoria por qualquer participante, demonstrando a sua transparência [Ribeiro e Mendizabal 2019].

A comunicação também procede maneira descentralizada, sendo efetuada diretamente entre os pares, ao invés de através de um nó central [Ribeiro e Mendizabal 2019]. Essa comunicação ocorre em uma rede ponto a ponto (peer-to-peer, em inglês), a fim de transmitir novas transações efetuadas, blocos a serem minerados (conceito que será explorado na subseção 2.5), novos blocos adicionados ao Blockchain etc. [Nakamoto 2008].

2.5. Prova de trabalho criptográfico

Como dissertado anteriormente, em transações de moedas reais as instituições intermediárias (terceira parte) têm como objetivo reduzir as incertezas ao redor da operação. Elas reduzem as incertezas ao se apresentarem como uma parte de confiança, que irá garantir e validar os valores transacionados entre duas partes [Warburg 2016].

Com o objetivo de eliminar o intermediário, o Blockchain substitui o fator confiança por uma prova de trabalho criptográfico. Esta prova é um procedimento que consiste em procurar um hash com um determinado número de zeros no seu início para um bloco a ser adicionado na corrente [Nakamoto 2008]. Só será possível obter diferentes hashes para um mesmo bloco se, e somente se, um de seus valores seja diferente. Deste modo, o valor da propriedade nonce do bloco (citada na subseção 2.2) é iterado [Nakamoto 2008]. Isso resultará em um hash diferente a cada iteração, que pode ser realizada aleatoriamente ou crescentemente. Ao final, será produzido um hash com o número de bits em zero desejado [Ribeiro e Mendizabal 2019] e, caso as iterações sejam em ordem crescente iniciando em zero, o nonce representará o número de iterações realizadas para produzi-lo. O esforço computacional necessário é exponencial ao número zero necessários [Nakamoto 2008].

O processo descrito é popularmente conhecido como “mineração” e é responsável por validar as transações por meio de poder computacional, a fim encontrar blocos válidos [European Central Bank 2012]. Como este trabalho criptográfico exige tempo de processamento de CPU, eletricidade e outros fatores, o Blockchain concede um incentivo (também conhecido pelo termo recompensa) para os nós da rede que executarem essa tarefa [Nakamoto 2008]. Além da ajuda de custos, o incentivo motiva o rápido processamento de transações e evita ações maliciosas, uma vez que estas não compensam [Ebrahimi, Routledge e Zetlin-Jones 2019].

2.6. Comunidade

Além da perspectiva técnica do Blockchain, deve-se buscar entender o papel das partes envolvidas. Existe uma “comunidade” ao redor da tecnologia, que interage direta e indiretamente com ela. São eles: os desenvolvedores, responsáveis por lançar e manter a iniciativa; os mineradores, que são donos de computadores (pares na rede) que validam transações em troca de recompensas; os investidores, que financiam o desenvolvimento de projetos de Blockchain; e, por fim, os usuários, aqueles que se utilizam do produto (por exemplo, da compra criptomoedas para transacionar ou especular valores) [Arruñada e Garicano 2018].

3. Metodologia da Pesquisa

A respeito da metodologia utilizada neste presente trabalho, o processo iniciou-se com uma revisão do referencial teórico, uma coletânea de literaturas com temas que envolvem a tecnologia de Blockchain e a negociação de criptomoedas. O foco esteve em compreender o que é o Blockchain, quais os seus processos e as suas finalidades.

A base teórica foi construída em um processo de pesquisa em bibliografias e documentos. Essa etapa teve como objetivo levantar as características de cada estrutura que compõe o Blockchain, entender como elas interagem entre si e quais os processos realizados na negociação de criptomoeda. Isso contribuiu com a etapa seguinte de desenvolvimento do aplicativo que implementa Blockchain para o sistema iOS.

Para o processo de desenvolvimento do aplicativo, primeiramente foi realizado um levantamento dos requisitos do sistema e, em seguida, a prototipagem das telas. A partir dos dados apurados e do conteúdo criado, foram decidas as tecnologias utilizadas para o desenvolvimento do aplicativo proposto e foi documentada a arquitetura do sistema. A seguir, o software foi desenvolvido com o intuito de possibilitar a negociação de criptomoeda com Blockchain entre dispositivos iOS conectados em uma mesma rede local. Por fim, o aplicativo resultante é apresentado e as conclusões da pesquisa relatadas.

Portanto, a pesquisa descrita neste artigo divide-se nas etapas a seguir:

1. Estudo da tecnologia Blockchain (composição e processos), com base no referencial teórico;
2. Planejamento e prototipagem do aplicativo proposto;
3. Desenvolvimento de um aplicativo de negociação de criptomoeda para dispositivos móveis iOS conectados em rede local que implementa a tecnologia Blockchain;
4. Preparação do artigo.

4. Desenvolvimento

O aplicativo proposto adapta o modelo de Nakamoto (2008) e os princípios da tecnologia (apresentados na seção 2) para dispositivos móveis. Portanto, o aplicativo realiza todas as operações base do Blockchain em uma abordagem própria, conforme apresentado na Figura 1.

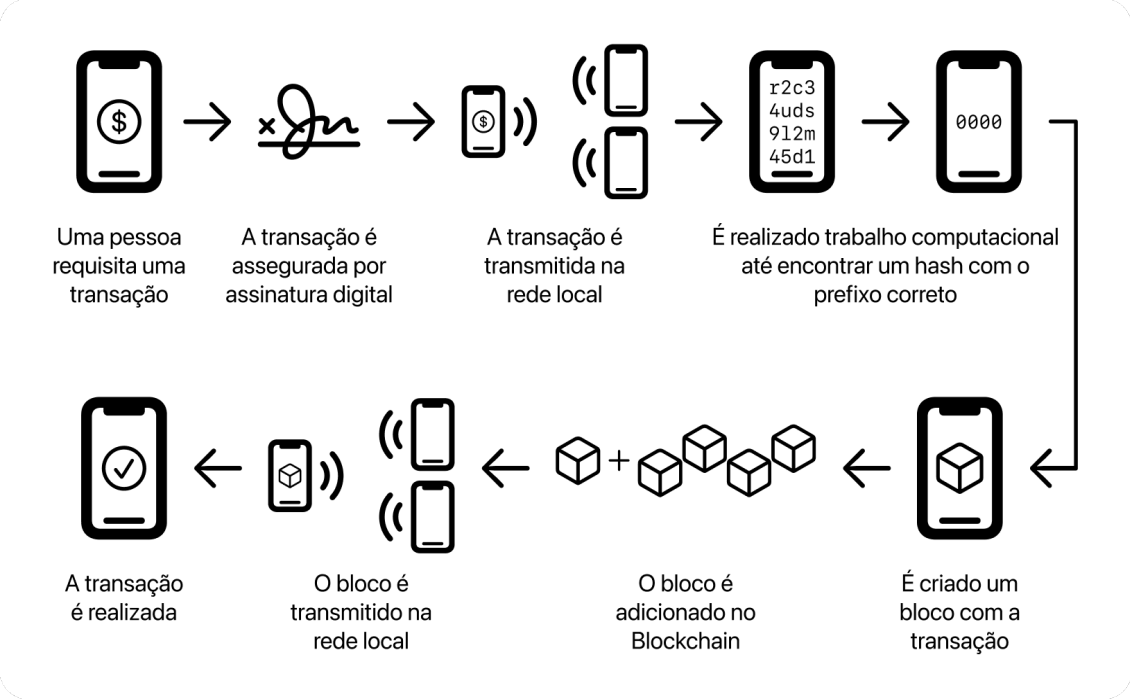

Figura 1. Funcionamento do Blockchain em rede local para dispositivos móveis iOS, implementado no aplicativo desenvolvido (figura do autor)

4.1. Requisitos do Sistema

A primeira etapa do desenvolvimento consiste no levantamento dos requisitos do sistema. De acordo com a Cedro Technologies, "trata-se do processo de compreensão e identificação das necessidades que o cliente espera ser solucionado pelo sistema que será desenvolvido, definindo o que o software vai fazer".

4.1.1. Requisitos Funcionais

As funcionalidades que o aplicativo deve possuir são:

1. Escolher o nome do participante, identificando o usuário na rede da maneira que o este desejar;
2. Criar ou ingressar em uma rede peer-to-peer local, viabilizando as interações entre pares que o Blockchain necessita;
3. Iniciar o Blockchain por meio da mineração do bloco gênesis, processo em que se cria o primeiro bloco e permite que os pares conectados criem blocos que armazenam negociações de criptomoeda;
4. Consultar o saldo de criptomoedas, possibilitando a gerência deste pelo usuário;
5. Transacionar quantias da criptomoeda fictícia para os participantes da rede, essência do Blockchain proposto nesta pesquisa;
6. Auditar as informações da sessão, como número de blocos na corrente, blocos minerados, transações recebidas e transações enviadas pelo usuário, com o objetivo de dar visibilidade as ações dos usuários e aproximá-los da tecnologia;

7. Auditar as informações do Blockchain, como os dados que compõe cada bloco, cumprindo o princípio de transparência da tecnologia;
8. Habilitar e desabilitar a elegibilidade para minerar blocos, permitindo que o usuário escolha conscientemente o papel que deseja desempenhar no Blockchain;
9. Minerar blocos próprios e de outros participantes, atendendo o princípio de validação por prova de trabalho criptográfico;
10. Exibir as iterações do hash durante o processo de mineração de um bloco, apresentando ao usuário de maneira transparente os processos do Blockchain.

4.1.2. Requisitos Não-funcionais

As características que o aplicativo deve possuir são:

1. Todas as transações devem ser autenticadas com assinaturas digitais, processo fundamental do Blockchain que assegura ambas as partes de uma transação, reduzindo as incertezas e permitindo a auditoria;
2. O processo de mineração não deve se estender por mais de 1 minuto, pois, dado o fim didático do projeto, preza-se por uma breve e clara exposição dos procedimentos da tecnologia;
3. A prova de trabalho criptográfico deve buscar por pelo menos dois números zeros iniciais no hash, permitindo um processo minimamente desafiador e duradouro de mineração;
4. Apenas um participante pode criar e minerar o bloco gênesis, porque este é um bloco de caráter único que inicializa o Blockchain;
5. Todos os participantes conectados podem transacionar a criptomoeda e auditar o Blockchain, praticando os princípios de distribuição dos dados e comunicação descentralizada;
6. Apenas transações com valores maior que zero e com destinatário podem ser efetuadas, tendo em vista que essas são exigências universais para qualquer tipo de negociação;
7. Mineradores receberão 5 moedas de incentivo por bloco minerado, cumprindo uma agenda de incentivo para a realização de trabalho criptográfico.

4.2. Prototipagem de Telas

A fim de levantar os requisitos do sistema e guiar o desenvolvimento do aplicativo e de sua interface, foi construído um protótipo no software Figma. Todas as telas foram prototipadas utilizando textos remetentes ao tema, com o objetivo de retratar a realidade o mais próximo possível. Em relação ao tema da interface, o protótipo abrange apenas telas em modo escuro (dark mode, em inglês), uma vez que o processo é demorado e um modo de tela é o suficiente para o levantamento de requisitos e para guiar o desenvolvimento.

Primeiramente foi prototipado a introdução, que apresenta o aplicativo e a sua proposta. Nela, o usuário deve inserir um nome para identificá-lo e, em seguida, definir

o seu papel na sessão. As ações cumprem os requisitos funcionais 1 e 2, respectivamente.

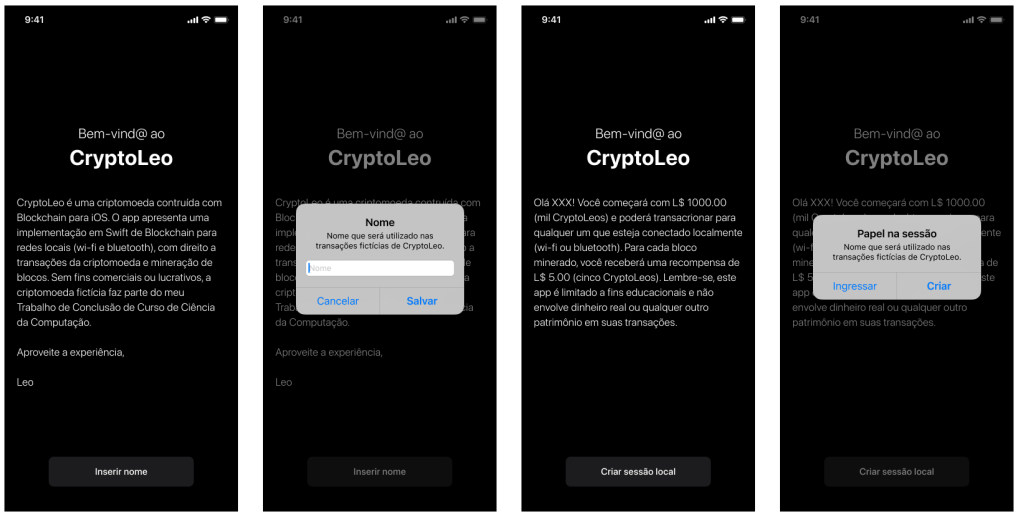

Figura 2. Protótipo das telas de introdução (figura do autor)

O protótipo da tela principal tem como objetivo centralizar a experiência do usuário, apresentando as informações principais e iniciando fluxos de transação e auditoria. Na tela é possível visualizar o saldo de criptomoedas, os dados da sessão do em andamento e controlar a elegibilidade do usuário para minerar blocos, atendendo os requisitos funcionais 4, 6 e 8, respectivamente. A tela de mineração de bloco, por sua vez, exerce os requisitos 9 e 10 ao apresentar o processo de mineração com a iteração do hash.

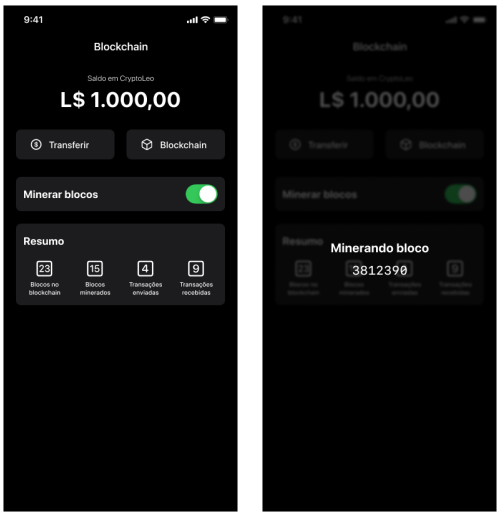

Figura 3. Protótipo das telas principal e de mineração, respectivamente (figura do autor)

Além do mais, a tela de transação foi prototipada visando negociações de forma simples, em que usuário insere o valor e o destinatário. Seu protótipo foi concebido com o requisito funcional 5 e com os requisitos não funcionais 5 e 6 em mente. Por fim, o protótipo da tela de auditoria apresenta todos os dados no Blockchain, ou seja, os detalhes de cada bloco, cumprindo o requisito funcional 7 e o requisito não-funcional 5.

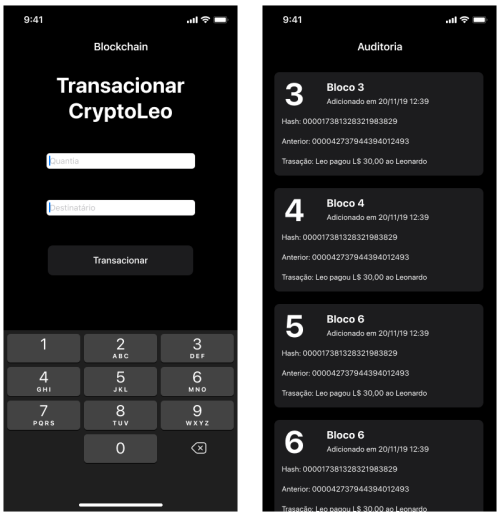

Figura 4. Protótipo das telas de transação e auditoria, respectivamente (figura do autor)

4.3. Arquitetura do Sistema

4.3.1. Objetos

A arquitetura do projeto é composta por quatro principais objetos, que serão descritos na sequência: Transacionador, Delegado de Sessão, Comunicador e Controlador. As suas interações são descritas na figura 5.

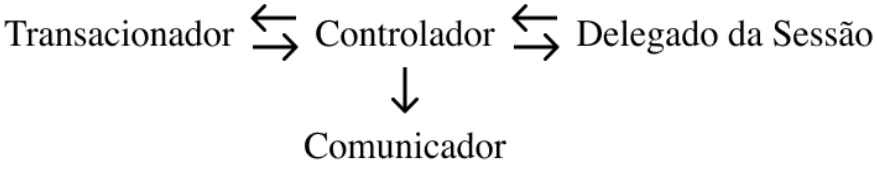

Figura 5. Arquitetura do projeto (figura do autor)

O Transacionador (referido no código como “BlockchainTransactor”) é o objeto responsável por gerenciar as operações do Blockchain, efetuando transações e criando e minerando blocos. Ele se comunica diretamente com o Controlador, objeto que será detalhado mais adiante.

O Delegado da Sessão (referido no código como “BlockchainSessionDelegate”) é o objeto responsável por receber e manipular eventos relacionados à sessão local. Basicamente, ele lida com dois principais cenários da comunicação peer-to-peer do Blockchain: acompanhar o status de conexão dos participantes na sessão, que representam possíveis transacionadores e mineradores de criptomoeda; e receber informações de outros participantes, como uma nova transação a ser inserida em um bloco ou um bloco recém minerado a ser adicionado ao Blockchain. Esse objeto se comunica diretamente com o Controlador.

O Comunicador (referido no código como “BlockchainBroadcaster”) é o objeto responsável por transmitir eventos relacionados ao Blockchain para todos os pares conectados na rede local, como novas transações ou blocos recém minerados prontos para serem adicionados à corrente. Ele recebe informações diretamente do Controlador, porém não se comunica de volta com ele.

Por fim, o Controlador (referido no código como “BlockchainViewController”) é o objeto responsável por controlar todos os objetos que compõe o Blockchain e a interface, direcionando dados e ações e delegando cada tarefa para o objeto encarregado de executá-la.

4.3.2. Estruturas

A arquitetura do projeto é composta por cinco principais estruturas de dados: Participante, Transação, Recompensa, Bloco e Corrente de Blocos.

O Participante (referido no código como “Peer”) é a estrutura que representa o nó na rede do Blockchain. Ela é utilizada para moldar um usuário, que será capaz de transferir criptomoedas ou minerar blocos e ser recompensado. A estrutura possui as seguintes propriedades:

- Nome do participante: nome do usuário, que será apresentado na interface;
- UUID: identificador único e exclusivo associado ao participante;
- Chave pública: código público utilizado para verificar as transações assinadas por este usuário.

A Transação (referida no código como “Transaction”) é a estrutura que representa a transação de criptomoeda entre dois participantes. A estrutura possui as seguintes propriedades:

- Remetente: participante que realizou a transação;
- Destinatário: participante que recebeu a transação;
- Quantidade: valor a ser transacionado;
- Estampa temporal: texto como data e hora da operação;
- Mensagem: descrição da transação;
- Assinatura digital: criptografia única do remetente para essa transação.

A Recompensa (referida no código como “Reward”) é a estrutura que representa a recompensa em criptomoeda concedida a um participante por minerar um bloco. A estrutura possui as seguintes propriedades:

- Minerador: participante que realizou a prova de trabalho criptográfico;
- Quantidade: valor em criptomoeda recebido como incentivo;
- Estampa temporal: texto como data e hora da recompensa;
- Mensagem: descrição da recompensa.

O Bloco (referido no código como “Block”) é a estrutura que representa um bloco do Blockchain. A estrutura possui as seguintes propriedades:

- Índice: posição do bloco na corrente;
- Hash: valor único gerado pelo algoritmo SHA256 que identifica o bloco e a prova de trabalho criptográfico inserida nele;
- Transação: estrutura especificada na subseção 4.3.2;

- Recompensa: estrutura especificada na subseção 4.3.2;
- Nonce: número que representa a prova de trabalho, que deve ser incrementada até que seja encontrado um valor que forneça ao hash do bloco os bits zeros necessários;
- Chave: um valor único com todas as informações do bloco, composta por índice, hash anterior, transação, recompensa e nonce.

A Corrente de Blocos (referida no código como "Blockchain") é a estrutura que representa o próprio Blockchain. A estrutura possui uma única propriedade: uma lista de Blocos, estrutura especificada na subseção 4.3.2.

4.4. Tecnologia

Como apresentado anteriormente, o presente projeto tem como objetivo desenvolver um aplicativo de negociação de criptomoeda para dispositivos móveis iOS em rede local com a tecnologia Blockchain. Para o desenvolvimento em tal plataforma, foi utilizado o software Xcode com a linguagem de programação Swift. Ademais, foram utilizadas as seguintes bibliotecas: Foundation, para tipos e operações base; UIKit, para elementos de interface; CryptoKit, para operações de criptografia, como geração de hash e assinaturas digitais com chaves públicas e privadas; e MultipeerConnectivity, para a comunicação peer-to-peer em rede local (wi-fi ou bluetooth).

4.5. Implementação

No processo de implementação do Blockchain, três procedimentos destacam-se dos demais, dadas a sua importância e alta complexidade: transação de criptomoeda, mineração de bloco e adição de bloco à corrente.

A operação de transação foi implementada no Transacionador, onde cria-se uma estrutura de Transação com as informações fornecidas pela interface, via Controlador. Para que isso seja possível, primeiro o método cria a mensagem da transação, descrevendo a quantidade de criptomoeda, os participantes envolvidos e a estampa temporal. Em seguida, a mensagem é assinada pelo remetente da transação utilizando a sua chave privada e é validada por meio de sua chave pública.

Com todas as informações necessárias e com a transação devidamente assinada criptograficamente, a Transação é criada. A seguir, deve-se criar um Bloco para armazenar a transação e minerá-lo para adicioná-lo no Blockchain. Essa operação poderá ser efetuada pelo próprio remetente ou por outro nó na rede. Caso o usuário opte pela segunda opção, o Transacionador encaminhará a Transação para o Controlador, que por sua vez encaminhará para o Comunicador.

O método de mineração de bloco (também presente no Transacionador) é responsável por encontrar um hash com quatro números zeros em seu início, por meio iterações do seu nonce. Devido ao intenso processamento, as interações do nonce são executadas em uma thread em segundo plano. Quando o trabalho de mineração é concluído, um Bloco é criado com as informações e com o hash resultante. Por fim, este é adicionado ao Blockchain e enviado para todos os outros nós, via o Comunicador.

Minerado o bloco, este deve ser adicionado à corrente. Para tal, o método de adição ao Blockchain, também localizado no Transacionador, realiza três validações essenciais:

- Validação da existência de uma Transação no Bloco recebido;
- Validação da veracidade da assinatura digital da Transação, utilizando a chave pública do remetente;
- Validação do hash do bloco, assegurando que este possui o número de zeros necessários (quatro neste projeto) e, consequentemente, se passou pela prova de trabalho criptográfico (mineração).

Caso ocorra algum erro em qualquer uma das validações, o Bloco não é adicionado ao Blockchain e o erro é encaminhado para o Controlador, que ordenará a interface a apresentar um indicativo visual.

A implementação do Blockchain proposta nesta presente pesquisa pode ser conferido no repositório público do projeto [Oliveira 2021].

5. Resultados

Finalizado o desenvolvimento, apresenta-se o aplicativo intitulado CryptoLeo, que implementa Blockchain em dispositivos móveis iOS, possibilitando a negociação e auditoria da criptomoeda fictícia que dá o nome ao aplicativo. O app é adaptado para light e dark mode (modos claros e escuros de interface). As figuras nesta seção apresentam as telas do aplicativo em light mode.

Ao iniciar o aplicativo, é apresentado o fluxo introdutório. Nessa sequência de telas são exibidas a proposta do aplicativo e o seu funcionamento. Ainda, nesse fluxo, o usuário deve se identificar e escolher se deseja iniciar o Blockchain ou ingressar em um existente na rede local que está conectado.

Figura 6. Telas de início, identificação, introdução e seleção de sessão, respectivamente (figura do autor)

Selecionada a opção de sessão, é apresentado o lobby. Esta tela é responsável por exibir os usuários conectados na sessão antes de iniciá-la. Uma vez que há pelo menos 2 pares conectados na sessão, o botão “Começar” torna-se visível.

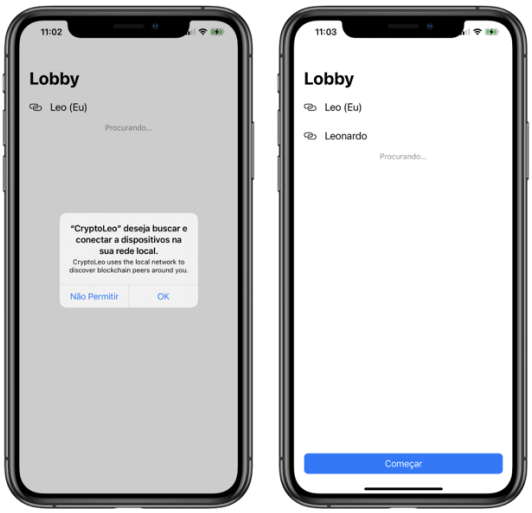

Figura 7. Tela de lobby da sessão local, em que é requisitada permissão para se conectar na rede local (figura do autor)

Uma vez que a sessão é iniciada, apresenta-se a tela principal do aplicativo. Ela consiste na exibição do saldo de criptomoeda e do resumo da sessão (informações de blocos no Blockchain, transações enviadas, transações recebidas e blocos minerados pelo usuário). Ademais, a tela possui um interruptor de elegibilidade de mineração de blocos e botões para iniciar os fluxos de transação e auditoria. Na tela de transação, são apresentados os campos de quantia e destinatário, que quando preenchidos fazem com que o botão “Transferir” se torne visível, possibilitando a negociação. A tela de auditoria, por sua vez, apresenta todos os blocos do Blockchain detalhadamente. Para cada bloco, são exibidas: posição na corrente, hash, hash do bloco anterior, descrição da transação, descrição da mineração e o nonce (prova de trabalho criptográfico).

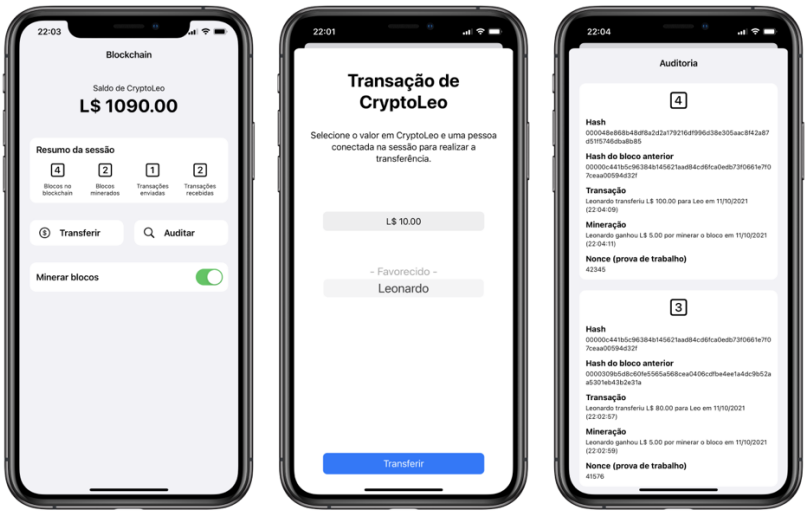

Figura 8. Telas principal, de transação e de auditoria, respectivamente (figura do autor)

Como descrito anteriormente no artigo, para que uma negociação seja concretizada e registrada no Blockchain, é preciso que um bloco seja minerado. Desta maneira, quando uma negociação é realizada (pelo usuário ou por outro par conectado na rede) e o interruptor de elegibilidade de mineração está ativado, o usuário recebe um alerta indicando a necessidade de minerar um bloco. Caso o usuário seja o remetente da negociação e não esteja elegível para mineração de blocos, é apresentado um alerta indicando que outro usuário irá minerar o bloco.

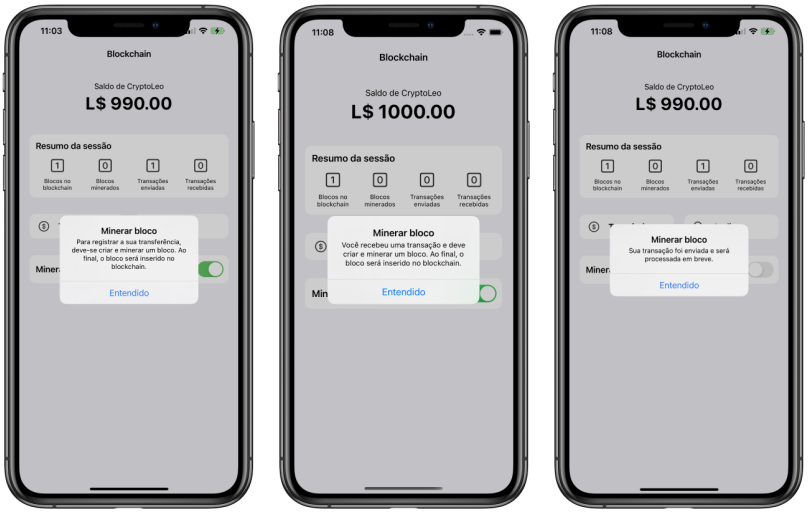

Figura 9. Avisos de comunicação na rede peer-to-peer: mineração própria de bloco, mineração de bloco recebido e transmissão de bloco a ser minerado por outro usuário, respectivamente (figura do autor)

Durante a mineração, a tela principal do aplicativo é desfocada e é apresentada a iteração hash em busca dos quatro zeros necessários para validar criptograficamente o bloco. Uma vez encontrados os zeros, é exibido o número de iterações que foram necessárias até atingir o resultado esperado.

Figura 10. Telas de mineração do bloco gênesis, de mineração de bloco comum e de sucesso no processo de mineração, respectivamente (figura do autor)

6. Conclusões e Recomendações

Apesar das incertezas e de sua volatilidade nas bolsas de valores, as criptomoedas e, principalmente, o Blockchain, devem se consolidar no decorrer do século XXI. O Blockchain não se trata apenas de uma evolução econômica e política, mas também de uma evolução no campo da ciência da computação [Warburg 2016]. A tecnologia apresenta uma maneira segura, distribuída e auditável de armazenar informações, sejam ela de qualquer tipo, desde criptomoedas até dados de saúde.

Em relação ao aplicativo desenvolvido, a implementação para rede peer-to-peer local prova-se limitada, uma vez que não há uma continuidade de conexão (é encerrada caso os participantes deixem a sessão) e baixo limite de participantes (8 pares conectados simultaneamente). Por essa razão, os processos de transmissão e recebimento de informações foram limitados e simplificados.

Todavia, a implementação do Blockchain em dispositivos móveis demonstra ser viável, concluindo o objetivo deste presente projeto de pesquisa e desenvolvimento. Ao realizar todos os procedimentos localmente no dispositivo móvel, eles são necessariamente apresentados ao usuário. Isso o aproxima da tecnologia e o torna mais participativos em seus processos, com destaque à procedimentos como transação, envio de transação para ser armazenado em bloco, mineração de bloco, adição de bloco a corrente e auditoria dos dados da corrente e de seus blocos.

Além do mais, o Blockchain desenvolvido é escalável, apresentando inúmeras possibilidades de melhorias e extensões, como: comunicação em redes remotas peer-to-peer, contratos inteligentes [Iansiti e Lakhani 2017], redução armazenamento com Árvores de Merkle [Nakamoto 2008], verificação da maior corrente de prova criptográfica [Nakamoto 2008], transparência com pseudonimidade [Iansiti e Lakhani 2017] etc.

7. Referências

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 31 ago. 2021.

WARBURG, Bettina. Palestra proferida no TEDSummit, jun. 2016. Disponível em: <https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy?language=pt-br>. Acesso em: 5 set. 2021.

IANSITI, Marco; LAKHANI, Karim R. The Truth About Blockchain: It will take years to transform business, but the journey begins now. Harvard Business Review, p. 118–127, jan./fev. 2017. Disponível em: <https://hbr.org/2017/01/the-truth-about-blockchain>. Acesso em: 23 set. 2021.

RIBEIRO, Lucas; MENDIZABAL, Odorico. Introdução à Blockchain e Contratos Inteligentes: Apostila para Iniciante. Universidade Federal de Santa Catarina, Departamento de Informática e Estatística, 2021. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/221495/RT-INE2021-1.pdf?sequence=1>. Acesso em: 23 set. 2021.

CROSBY, Micahel et al. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review, Berkeley, n. 2, p. 6-19, jun. 2016. Disponível em: <https://j2-

capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>. Acesso em: 23 set. 2021.

DAVIS, Joshua. The crypto-currency: Bitcoin and its mysterious inventor. The New Yorker, p. 62-70, 10 out. 2011. Disponível em: <https://cryptome.org/0005/bitcoin-who.pdf>. Acesso em: 23 set. 2021.

SARMAH, Simanta Shekhar. Understanding Blockchain Technology. Computer Science and Engineering, v. 8, n. 2, p. 23-29, ago. 2018. Disponível em: <https://www.researchgate.net/profile/Simanta-Sarmah/publication/336130918_Understanding_Blockchain_Technology/links/5d913eb9a6fdcc2554a69c7c/Understanding-Blockchain-Technology.pdf>. Acesso em: 23 set. 2021.

YAGA, Dylan et al. Blockchain Technology Overview. National Institute of Standards and Technology, n. 8202, out. 2018. Disponível em: <https://arxiv.org/pdf/1906.11078.pdf>. Acesso em: 25 set. 2021.

EUROPEAN CENTRAL BANK. Virtual Currency Schemes. Frankfurt, out. 2012. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em: 25 set. 2021.

ARRUÑADA, Benito; GARICANO, Luis. Blockchain: The Birth of Decentralized Governance, 11 abr. 2018. Disponível em: <https://poseidon01.ssrn.com/delivery.php?ID=713094097085071088030119002065074069000039039014031001095005102028031087091006093071118026012125037127020069118072096120001100023054032039051011086122096077122006080086123106000100092090005118103094098126097081029072065124066064103090122003124098&EXT=pdf&INDEX=TRUE>. Acesso em: 26 set. 2021.

EBRAHIMI, Zahra; ROUTLEDGE, Bryan; ZETLIN-JONES, Ariel. Getting Blockchain Incentives Right, dec. 2019. Disponível em: <https://econ.ntu.edu.tw/uploads/asset/data/5f0beefd48b8a1027b003383/HKBU_1090714.pdf>. Acesso em: 27 set. 2021.

DELOITTE. Blockchain Enigma Paradox Opportunity, Londres, 2016. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf>. Acesso em: 27 set. 2021.

WANG, Kevin. Measuring Global Crypto Users. Crypto.com, 2021. Disponível em: <https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf>. Acesso em: 3 out. 2021.

CEDRO TECHNOLOGIES. Levantamento de Requisitos – O ponto de partida do projeto de software. Disponível em: <https://blog.cedrotech.com/levantamento-de-requisitos-o-ponto-de-partida-do-projeto-de-software>. Acesso em: 4 set. 2021.

SINGH, Sunil Kumar; KUMAR, Sumit. Blockchain Technology: Introduction, Integration and Security Issues with IoT, 2021. Disponível em: <https://arxiv.org/pdf/2101.10921.pdf>. Acesso em: 22 out. 2021.

STRACK, Ben. Survey Says Most People Still Don't Understand Crypto, Blockworks, 1 nov. 2021. Disponível em: <https://blockworks.co/survey-says-most-people-still-dont-understand-crypto>. Acesso em: 10 nov. 2021.

GOVERNO DO BRASIL. População brasileira chega a 213,3 milhões de habitantes, estima IBGE. 27 ago. 2021. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/08/populacao-brasileira-chega-a-213-3-milhoes-de-habitantes-estima-ibge>. Acesso em: 12 nov. 2021.

TOKARNIA, Mariana. Celular é o principal meio de acesso à internet no país, Agência Brasil, 29 abr. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/celular-e-o-principal-meio-de-acesso-internet-no-pais>. Acesso em: 12 nov. 2021.

CHAVES, Iara. Blockchain e criptomoedas: Biblioteca Virtual, 2021. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/194850>. Acesso em: 20 nov. 2021.

LYRA, João Guilherme. Blockchain e Organizações Descentralizadas: Biblioteca Virtual, 2019. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/169379>. Acesso em: 20 nov. 2021.

OLIVEIRA, Leonardo Amorim de. CryptoLeo, 2021. Disponível em: <https://github.com/LeoAOliveira/CryptoLeo>. Acesso em: 4 dez. 2021.