APLICAÇÃO DE CONTRATOS INTELIGENTES USANDO BLOCKCHAIN NO CONTEXTO DA SOCIEDADE

Ítalo Regis Rocha da Costa
Prof. Dr. Wellington Sousa Aguiar (Orientador)
Prof. Dr. Aminadabe Barbosa de Sousa
Prof. Me. Henrique Nogueira da Gama Mota

RESUMO

A era do digital, tão anunciada por muitos pesquisadores da área, também chamada de quarta revolução industrial por alguns escritores, chegou. A tecnologia está cada vez mais presente no nosso meio e estamos cada vez mais dependentes de suas vantagens. Cada vez mais pesquisadores e cientistas têm desenvolvido tecnologias mais seguras, mais performáticas e que consomem menos energia. Uma tecnologia, com pouco mais de 10 anos, tem revolucionado o mercado financeiro com a ideia de armazenamento de recursos monetários em carteiras digitais, com a possibilidade de realizar transferências sem precisar de um intermediador. Essa tecnologia é a Blockchain, motivador principal desta pesquisa, uma espécie de armazenamento de transações em bloco encadeados, transações essas que são seguras, rastreáveis, descentralizadas e irreversíveis. O objetivo desta pesquisa é demonstrar o conceito de *smart contracts*, definido por Nick Szabo, dentro do contexto da sociedade brasileira com o intuito de auxiliar os órgãos governamentais a ter ferramentas que lhe possibilitem combater as irregularidades. A metodologia utilizada nessa pesquisa foi a pesquisa aplicada, pois foi desenvolvido uma solução prática para demonstrar a viabilidade da solução, e a metodologia bibliográfica. A pesquisa teve a natureza de cunho qualitativo de acordo com as conclusões do próprio autor. Os resultados obtidos durante os testes foram satisfatórios quanto a funcionalidade. Os fatores de confiabilidade, usabilidade e eficiência também foram considerados e todos tiveram resultados conforme o esperado. Concluindo, após a realização dos testes, foi identificado necessidades de melhorias no processo de confidencialidade e performance, mas, no que tange ao conceito aqui discorrido, é viável e de suma importância para a sociedade.

Palavras-chave: Blockchain; Ethereum; Smart Contracts; INSS; Fraudes previdenciárias.

ABSTRACT

The digital age, so announced by many researchers in the field, also called the fourth industrial revolution by some writers, has arrived. Technology is increasingly present in our environment and we are increasingly dependent on its advantages. More and more researchers and scientists have developed technologies that are safer, more performance and use less energy. A technology, with little more than 10 years, has revolutionized the financial market with the idea of storing monetary resources in digital portfolios, with the possibility of making transfers without the need for an intermediary. That technology is Blockchain, the main motivator of this research, a kind of storage of chained block transactions, transactions that are secure, traceable, decentralized and irreversible. The objective of this research will be to demonstrate the concept of Smart Contracts, defined by Nick Szabo, within the context of Brazilian society in order to help government agencies to have tools that enable them to combat irregularities. The methodology used in this research was applied research, as a practical solution was developed to demonstrate the viability of the solution, and the bibliographic methodology. The research had a qualitative nature according to the author's own conclusions. The results obtained during the tests were satisfactory in terms of functionality. The factors of reliability, usability and efficiency were also considered and all had results as expected. In conclusion, after the tests have been carried out, improvements in the process of confidentiality and performance will be necessary, but the concept discussed here is viable and is of paramount importance to society.

Keywords: Blockchain; Ethereum; Smart Contracts; INSS; Social security fraud.

INTRODUÇÃO

A previdência social brasileira é constituída de muitos fatores históricos, fatores esses que contribuíram para constituir um programa social que movimenta valores que representam mais de 8% do PIB anual desde o ano de 2014.

A atual legislação previdenciária brasileira está estabelecida na Constituição Federal de 1988 (CF/1988), que recebeu quatro emendas desde então. Além disto, três leis recentes a complementam. Ressalta-se que os direitos relativos à previdência social podem ser considerados direitos sociais fundamentais que têm adquirido uma força normativa crescente e atingiram o seu mais alto grau nessa Constituição. (NOLASCO, 2012)

A Lei Eloy Chaves, de 1923, é considerada o marco zero do atual sistema previdenciário brasileiro para os trabalhadores do setor privado. Foi responsável pela criação de caixas de aposentadorias e pensões por morte para os trabalhadores ferroviários. Cobria uma pequena parcela da população trabalhadora e seus dependentes. Após essa lei, inúmeras caixas de aposentadoria foram criadas, beneficiando várias categorias de trabalhadores, como portuários, servidores públicos, mineradores etc. Quase todas as caixas de aposentadoria e pensão previam a forma de custeio da previdência da respectiva categoria, além dos benefícios a serem concedidos. Operavam sob o regime de capitalização, e a vinculação era por empresas. (OLIVEIRA E BELTRÃO, 2000; CAMARANO, 2002; NOLASCO, 2012)

A previdência brasileira é constituída por três regimes. O maior deles, o Regime Geral de Previdência Social (RGPS), cobre os trabalhadores do setor privado. Os servidores públicos titulares de cargos efetivos são cobertos pelo Regime Próprio de Previdência Social (RPPS). Cada unidade federada possui o seu próprio regime. Ambos os regimes são públicos e de filiação compulsória. O terceiro regime é privado, de adesão facultativa, representado pela previdência complementar. (CAETANO, 2014)

A previdência social tem por fim assegurar, aos seus beneficiários, meios indispensáveis de manutenção, por motivo de incapacidade, idade avançada, tempo de serviço, desemprego involuntário, encargos de família, reclusão ou morte daquele de quem dependiam economicamente. (BRONDI, 2007)

O INSS foi criado em 27 de junho de 1990, durante a gestão do então presidente Fernando Collor de Melo, por meio do Decreto nº 99.350, a partir da fusão do IAPAS com o INPS. Hoje o instituto caracteriza-se como uma organização pública prestadora de serviços previdenciários para a sociedade brasileira e conta com uma quantidade de 76.386 servidores.

A Dataprev é uma empresa pública, que fornece soluções de tecnologia da informação e comunicação para a previdência social. A empresa é vinculada ao ministério da economia possui patrimônio próprio e autonomia administrativa e financeira. Hoje a empresa tem um quadro de 3.300 servidores.

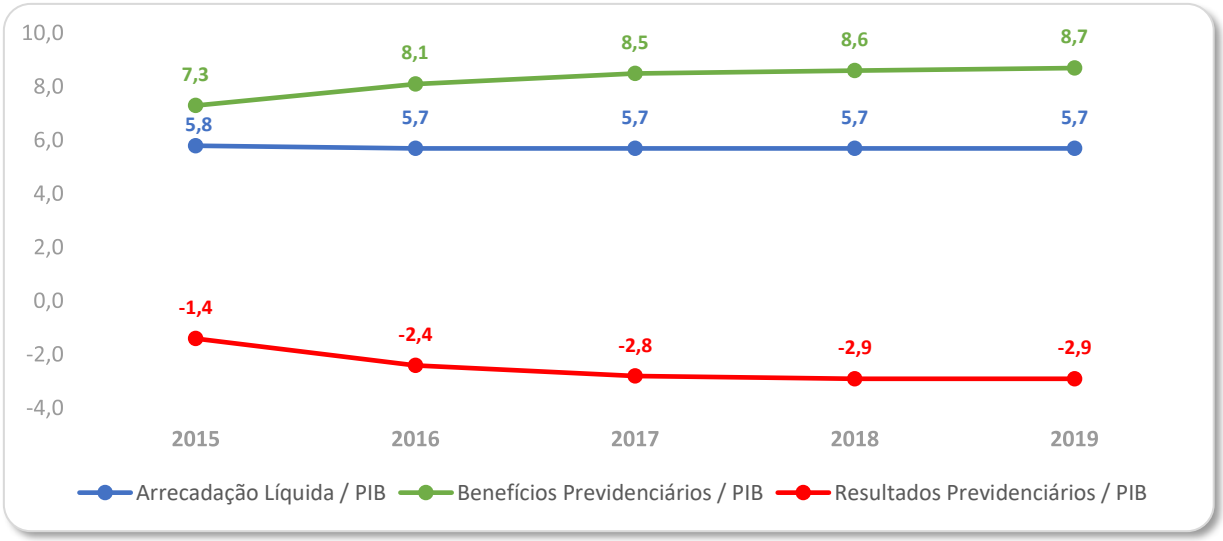
Segundo INSS, 2020, um cidadão pode se colocar na posição de beneficiário da previdência social quando atende as prerrogativas de um dos seguintes benefícios.

- Aposentadoria por idade
- Aposentadoria por invalidez
- Aposentadoria por tempo de contribuição
- Aposentadoria especial por tempo de contribuição

- Aposentadoria da pessoa com deficiência por idade
- Aposentadoria da pessoa com deficiência por tempo de contribuição
- Aposentadoria por tempo de contribuição do professor
- Auxílio doença
- Auxílio acidente
- Auxílio reclusão
- Pensão por morte
- Salário maternidade
- Salário família

O governo federal tem tentado ao longo dos anos, entre seus representantes de grau maior, buscar alternativas que tornem o sistema previdenciário sustentável. O Gráfico 1, abaixo, demonstra a grande representação do programa previdenciário dentro do PIB brasileiro. Além disso, podemos observar que nos últimos anos o déficit da relação arrecadação e benefício tem ficado cada vez maior.

Gráfico 1 – Arrecadação Líquida, Despesa com Benefícios e Resultado Previdenciário em relação ao PIB (Em %) de 2015 a 2019.



Fonte: Previdência Social

A Tabela 1 abaixo, nos mostra a relação da população brasileira com o mesmo programa. Um fator importante é que o número de beneficiários tem crescido exponencialmente ano a ano e isso tem aumentado a tensão no governo por medidas emergências.

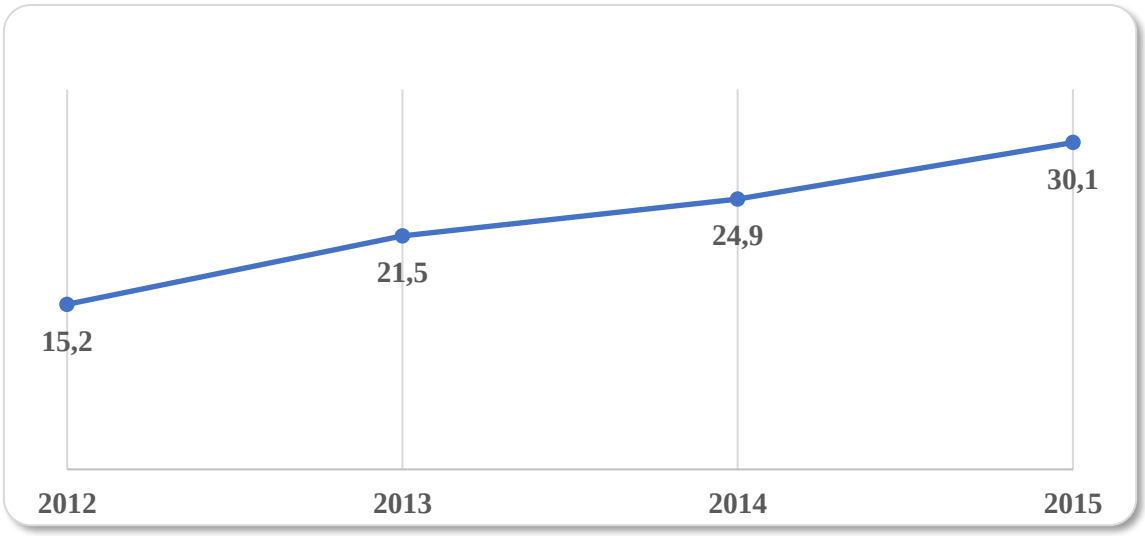
Tabela 1 – Quantidade de beneficiários ativos por ano, por número de benefícios e a proporção com a população.

ANO	POPULAÇÃO	BENEFICIÁRIOS ATIVOS					% POPULAÇÃO
		TOTAL	Quantidade de Benefícios				
			1	2	3	4	
2016	**206.081.432**	**31.585.996**	29.593.902	1.973.625	18.198	271	**15,32%**
2017	**207.660.929**	**32.396.511**	30.516.035	1.863.210	17.009	257	**15,60%**
2018	**208.494.900**	**33.095.484**	31.314.085	1.765.205	15.949	245	**15,87%**

Fonte: Previdência Social e IBGE, Adaptado.

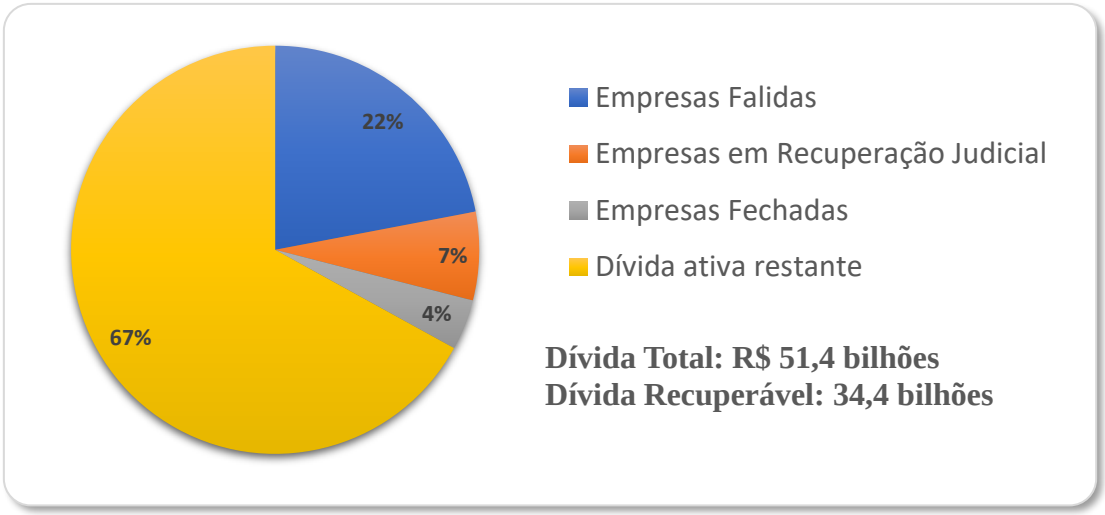
O cenário atual, visualizado abaixo nos gráficos 2 e 3, não nos traz uma boa retrospectiva da saúde previdenciária brasileira. As receitas, que deveriam vir do repasse das empresas como contribuição do trabalhador, estão sendo cada vez mais retidas por fraudes e sonegações das pessoas jurídicas.

Gráfico 2 – Valores que as empresas não repassam ao governo referentes à contribuição previdenciária do trabalhador (em R$ bilhões).



Fonte: SINAIT (Sindicato Nacional dos Auditores Fiscais do Trabalho)

Gráfico 3 – Dívida ativa previdenciária, 2017 (250 maiores devedores, em R$ bilhões).



Fonte: PGFN (Procuradoria-Geral da Fazenda Nacional)

Há uma grande necessidade de equilíbrio em sistemas previdenciários, como o brasileiro, na qual taxativamente demonstra que déficits públicos previdenciários crescentes ameaçam o equilíbrio dos sistemas, assim como a sustentabilidade das contas públicas (MEDICI, 2009).

Segundo Félix, Ribeiro e Tostes (2008) existe uma relação entre os déficits previdenciários e as ocorrências de fraudes ou suspeitas de irregularidades. Reis, Fernandes e Antunes apresentam levantamentos de bilhões de reais em ações de apuração de fraudes previdenciárias contatos a partir do final da década de 1980.

As fraudes são o resultado de oportunidades, quer por um controle interno frágil, quer por excesso de comando. A previdência social brasileira vem sofrendo com um número cada vez maior de fraudes em seus benefícios (PERERA, FREITAS E IMONI-ANA, 2014).

A falsificação de RG e registro civil, certidão de nascimento ou casamento, atingiu proporções preocupantes. Não há, hoje, um método seguro de identificação do cidadão, como biometria, por parte do poder público, afirmou Marcelo Henrique de Ávila, coordenador-geral da COINP (UOL, 2019).

As fraudes previdenciárias acontecem, na sua maioria, pela falta de integração entre sistemas de informações do INSS com os dos demais interessados. Para exemplificar esse cenário vamos citar o caso dos cartórios, onde eles precisam enviar periodicamente para o instituto algumas informações como a relação dos nascimentos e dos óbitos. Essas informações precisavam ser submetidas para a instituição até o dia 10 do mês subsequente aos registros, porém o Art. 68 da Lei nº 13.486, de 18 junho de 2019, estabeleceu que, O Titular do Cartório de Registro Civil de Pessoas Naturais remeterá ao INSS, em até 1 (um) dia útil, pelo SIRC ou por outro meio que venha a substituí-lo, a relação dos nascimentos, dos natimortos, dos casamentos, dos óbitos, das averbações, das anotações e das retificações registradas na serventia. Com a nova diretriz em andamento, houve grandes contestações por parte dos tabeliões que questionavam a falta de estrutura própria e do INSS para conseguir cumprir o prazo.

OBJETIVOS

Criar uma base centralizada com informações dos cidadãos brasileiros necessárias para se ter uma identidade digital que seja inviolável, descentralizada e segura. Essa base de

informações será o insumo necessário para que possamos implementar medidas tecnológicas nos demais fluxo onerosos e burocráticos que temos no setor público ou privado. A base de dados gerada será basicamente a relação pessoa por registro na Blockchain.

Podemos ressaltar como objetivos secundários, mas que trarão valor a solução proposta:

- Mitigar fraudes nos programas do governo federal.
- Realizar estudos sobre os comportamentos da população tomando como base no rastreio das movimentações realizadas pela vida digital do cidadão.
- Evitar sonegações de impostos, pois teremos de forma acessível ao governo toda transação financeira de compra e venda de bens e de rendas pessoais.
- Criar uma integração entre os sistemas públicos e privados.
- Criar uma prova de conceito para o uso de Blockchain, além das criptomoedas, na sociedade.

REFERENCIAL TEÓRICO

BLOCKCHAIN

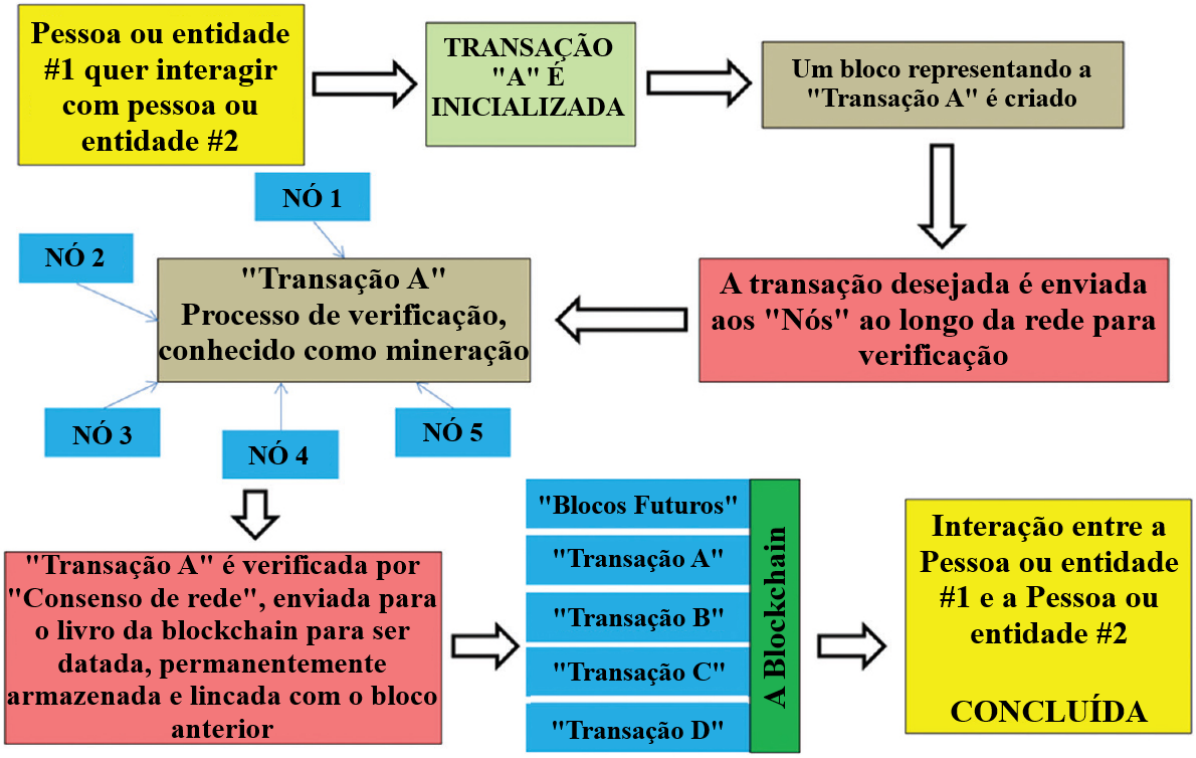
A Blockchain pode ser definida como uma base de dados distribuída que realiza o encadeamento de todos os registros dos elementos da rede, como também de registros de criação de novos elementos e modificação deles. Seu funcionamento se baseia em princípios como: funções *Hash* que não permitem decodificação, registro do tempo de criação ou modificação do arquivo, assinatura digital do autor responsável pela ação e rede descentralizada. As funções que não permitem decodificação nos asseguram que é praticamente improvável realizar a adulteração dos elementos. Já o registro de todos os momentos em que ocorre alguma intervenção nos elementos tem o benefício de impedir que fraudes temporais sejam possíveis. As assinaturas digitais visam garantir que toda e qualquer alteração em algum elemento pertencente a um determinado nó da rede Blockchain seja realizada pelo proprietário do par de chaves pública e privada daquele nó. A rede descentralizada é crucial para o sucesso da tecnologia, desta forma todas as alterações podem ser validadas em vários pontos da rede, e caso haja alguma inconsistência a própria rede irá invalidar a mesma (LUCENA; HENRIQUES, 2016).

As características apresentadas pela blockchain são benéficas para empresas que realizam autenticidade dos dados, como por exemplo, o caso dos cartórios de registros e entidades emissoras de documentos pessoais. Podendo ser utilizado com a finalidade de prova de identidade, pois não só armazena dados que podem ser usados para identificar alguém ou algo, como também provê conceitos básicos de segurança para identificação e autenticação (DRESCHER, 2018).

O surgimento desta tecnologia disruptiva chamada blockchain está proporcionando a criação de novos serviços, aplicativos, e soluções para mercado financeiro, e em outras áreas, como por exemplo, as empresas notariais (CROSBY et al., 2016). Esta tecnologia vem realizando uma verdadeira transformação de diversos setores econômicos. Do mercado financeiro ao naval, de votações de projetos de leis a fluxos comerciais, de registro de terras à identificação da veracidade de documentos, a possibilidade de sua utilização como protocolo tem gerado debates, preocupações e, por que não oportunidades para variados segmentos (LUIZARI, 2017).

A figura 1 abaixo, representa um modelo conceitual e explicativo de como um determinado usuário pode interagir com outro ponto na rede, um outro usuário ou um contrato, seja com uma transferência de recurso ou com a autenticação de um termo.

Figura 1 – Representação conceitual do paradigma da Blockchain

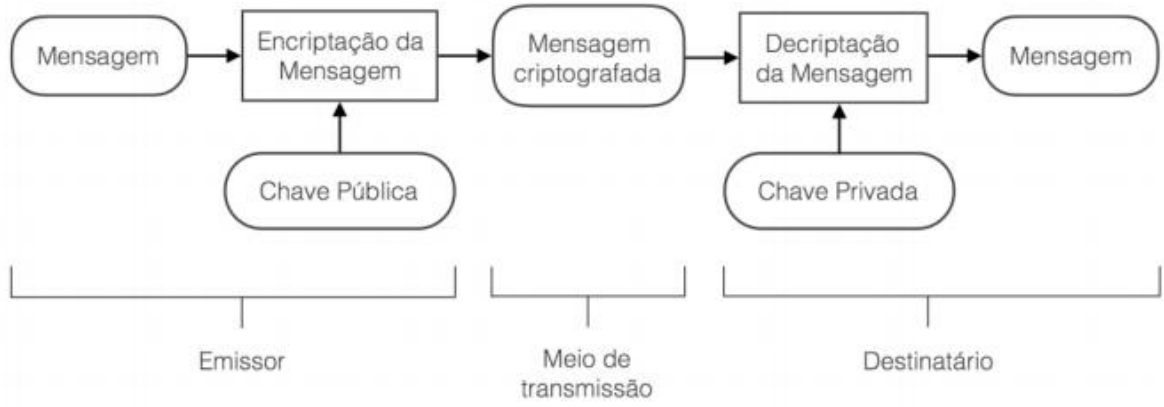


Fonte: STAWICKI; FIRSTENBERG; PAPADIMOS, Adaptado.

CRIPTOGRAFIA ASSIMÉTRICA

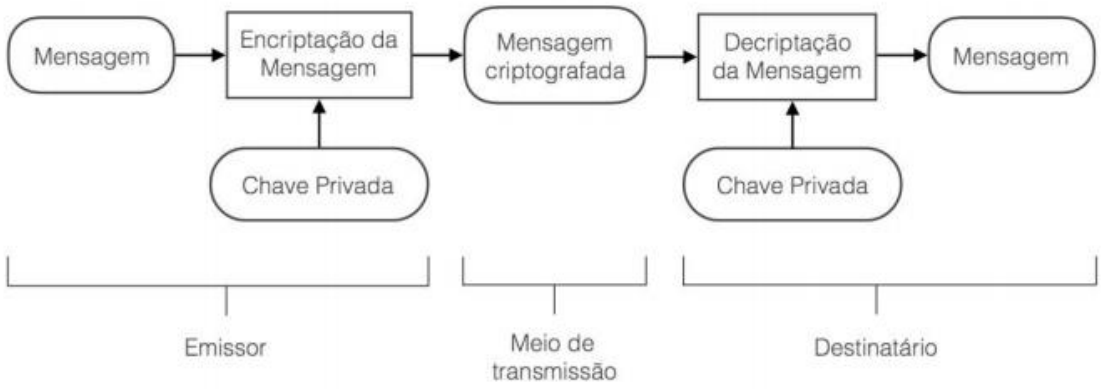
As interações realizadas na rede Blockchain são possíveis através de uma criptografia denominada de criptografia assimétrica ou criptografia de chave pública e privada. Como o próprio nome deixa evidente, esse tipo de criptografia faz uso de duas chaves (Funções *Hash*), onde a pública é usada para criptografar a informação, e a privada é usada para descriptografar os dados, conforme figura 2 abaixo. Somente com a posse da chave pública um usuário, não autorizado, não consegue visualizar as informações protegidas. Existe um outro fluxo, conforme figura 3 abaixo, que realiza a criptografia e a descriptografia com a chave privada. A única diferença nesse caso é que a criptografia será realizada pela própria chave privada e, além da confiabilidade que já é atestado no fluxo anterior, é possível também validar a confidencialidade já que a chave privada não é conhecida publicamente.

Figura 2 – Fluxo de criptografia assimétrica utilizando a chave pública para criptografar



Fonte: SALOMAA, adaptado.

Figura 3 – Fluxo de criptografia assimétrica utilizando a chave privada para criptografar



Fonte: SALOMAA, adaptado.

BITCOIN

No ano de 2009, em um fórum especializado em criptografia, um documento foi compartilhado com a ideia de ser uma *White Paper* de um sistema financeiro baseado em blocos criptografados. Esse documento, com a autoria de Satoshi Nakamoto, seria a primeira vez que o mundo veria a ideia do que hoje nós chamamos de Bitcoin.

Bitcoin é uma versão de dinheiro eletrônico puramente ponto-a-ponto que permite pagamentos online sejam enviados diretamente de uma pessoa para outra sem a necessidade de passar por uma instituição financeira, como bancos, por exemplo. As assinaturas digitais oferecem uma parte da solução, mas os principais benefícios são perdidos quando um intermediário confiável ainda é necessário (NAKAMOTO, 2008).

> "O que se torna necessário é um sistema de pagamentos eletrônicos baseado em provas criptográficas ao invés de confiança, permitindo que duas partes dispostas a negociar diretamente entre si possam o fazer sem a necessidade de um terceiro confiável. Transações que são computacionalmente impraticáveis de serem revertidas protegem os vendedores de caírem em alguma fraude. Além disso, mecanismos de rotina

> de depósitos poderiam ser facilmente implementados para proteger os compradores.” (NAKAMOTO, 2008).

O surgimento do Bitcoin tem sido aclamado desde 2009, ano do seu surgimento, como a tecnologia que veio para revolucionar o dinheiro e a moeda, sendo o primeiro exemplo de ativo digital que simultaneamente não possui nenhum lastro e valor intrínseco e nenhum emissor ou controlador centralizado (BUTERIN, 2014).

ETHEREUM

O Bitcoin revolucionou o mercado financeiro com a ideia de ser um ativo criptográfico, mas foi em 2014 quando Buterin percebeu que o motor do Bitcoin, a Blockchain, poderia ter infinitas possibilidades de uso a ponto de não revolucionar somente o mercado financeiro, mas sim todo e qualquer negócio existente no planeta que faça uso de acordos, contratos e registros, e necessite de rastreabilidade, autenticidade, controle de autorização e que seja programável a ponto de imitar o mundo real.

O que o projeto Ethereum pretende prover é uma Blockchain que seja programável, por uma linguagem de programação que seja *Turing Complete*, ou seja, que tenha as funcionalidades da máquina de Turing como recursos de linguagem condicionantes, laços de repetições etc. Com esses recursos programáveis as possibilidades de sua utilização sai de simplesmente realizar autenticação de transações financeiras, no caso do Bitcoin, para um leque de infinita possibilidade de uso (BUTERIN, 2014).

SMART CONTRACTS

Smart contracts, em português contratos inteligentes, são os produtos gerados a partir do desenvolvimento de programas realizado na blockchain, no nosso caso de estudo, blockchain Ethereum. Esses programas ficam armazenados na blockchain e são referenciados por endereço público. Neste contrato ou programa está incluído uma lógica que irá executar tarefas quando um endereço válido lhe sensibilizar, ou quando houver interações através de oráculos que ficam consultando dados do mundo real.

Segundo Szabo, os *smart contracts* podem ser vistos como uma máquina de refrigerante, que quando inserimos dinheiro nos é retornado o refrigerante no sabor que pedimos e, caso seja necessário, o troco. A máquina de refrigerante não precisou de uma intervenção humana para tomar uma decisão e nem de um mediador para conferir os valores, pois estava programada para realizar essa função. Os *smart contracts* vão além dessa máquina de vender ao propor a incorporação de contratos em todos os tipos de bens valiosos e controlados por meios digitais. Os contratos inteligentes referenciam esse bem de uma forma dinâmica, geralmente aplicada de maneira proativa e fornecem uma observação e verificação muito melhores, onde medidas proativas devem ficar aquém.

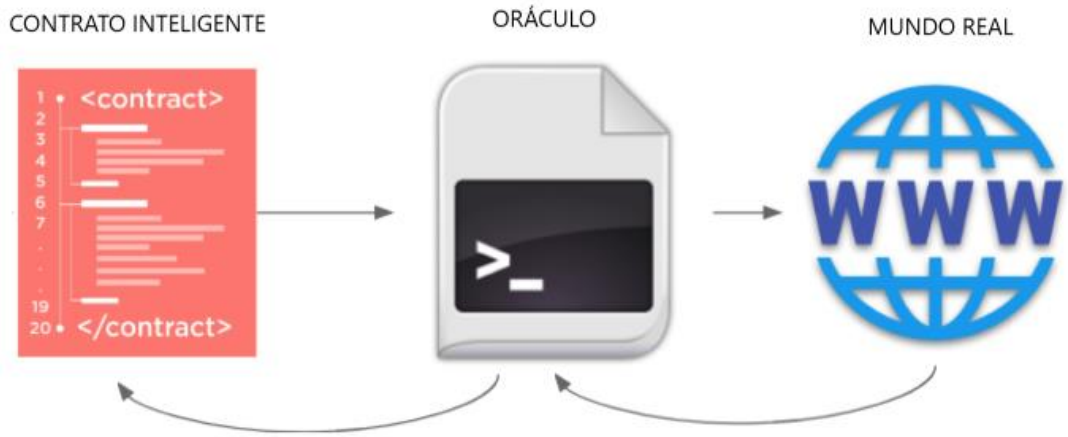
> “A Ethereum faz isso construindo o que é essencialmente a última camada fundamental abstrata: uma blockchain com uma linguagem de programação Turing completa, permitindo que qualquer pessoa escreva contratos inteligentes e aplicativos descentralizados, onde possam criar suas próprias regras arbitrárias para propriedade, formatos de transação e funções de transição de estado” (BUTERIN, 2014).

ORÁCULOS

Muitas das vezes os *smart contracts* necessitam de informações que são alheias ao próprio contrato e às partes. Nesses momentos é necessário desenvolver uma comunicação informatizada entre o *smart contract* e a fonte confiável detentora desta informação. Essa ligação é feita através do que chamamos de oráculos.

Segundo Malaquias e Dias, os dados dos oráculos podem ter fontes e ser acedidos de maneiras distintas, seja através de uma API, de input humano dado através de determinado front-end, de dispositivos como *wearables* ou outros que se encontram conectados a pessoas ou coisas (IoT), entre outras. Na figura 4, abaixo, podemos visualizar o fluxo de análise que será executado quando um contrato inteligente implementa a funcionalidade de um oráculo que está escutando dados do mundo real.

Figura 4 – Fluxo de informações entre um contrato inteligente e o mundo real.



Fonte: Elaborado pelo Autor.

SOLIDITY

Solidity é uma linguagem de programação de alto nível, orientada a contrato e desenvolvida para rodar em cima da Máquina Virtual Ethereum. Sua sintaxe é parecida com JavaScript, tem suporte a herança, bibliotecas e tipos complexos definidos pelo usuário. Esta linguagem obedece às funcionalidades de uma linguagem de programação de Turing (SOLIDITY, 2017).

A linguagem Solidity é usada para escrever contratos inteligentes e hospedá-los na blockchain Ethereum. Para a realizar o desenvolvimento existe uma IDE padrão chamada de Remix, esta é uma IDE baseada navegador com compilador integrado. Existe também *plugins* para as IDE's mais utilizadas no mercado como Intellij, Visual Studio e outras.

METODOLOGIA

Este projeto tem características de uma pesquisa aplicada, em que os conceitos estudados são desenvolvidos visando a utilização no mundo real. Pesquisa aplicada é voltada à absolvição de conhecimentos com o uso da aplicação proposta numa situação específica (GIL, 2010).

Pesquisa aplicada tem como objetivo provocar conhecimento para a aplicação prática conduzidos à resolução de problemas específicos relaciona verdades e interesses locais (SILVA, 2001).

A natureza desta pesquisa é de cunho qualitativo. Na visão de Martinelli (1999), um ponto a ressaltar é que a pesquisa qualitativa traz à tona a importância do que os participantes pensam a respeito do que está sendo pesquisado.

Para os interpretacionistas a pesquisa qualitativa é importante pois ela se dedica ao estudo da experiência humana, entendendo que as pessoas interagem, interpretam, e constroem sentidos. Para Moreira 2002, "[...] com grande dificuldade, a pesquisa qualitativa vai abrindo seus próprios caminhos".

O projeto utilizou também a pesquisa bibliográfica por meio de livros, artigos, teses, dissertações, visando criar um conteúdo completo e seguro sobre o assunto estudado.

Na concepção de Gil 2002, "[...] a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos". A principal vantagem da pesquisa bibliográfica está no fato de permitir ao pesquisador a cobertura de uma gama de fenômenos muito mais abrangente do que aquela que poderia pesquisar diretamente.

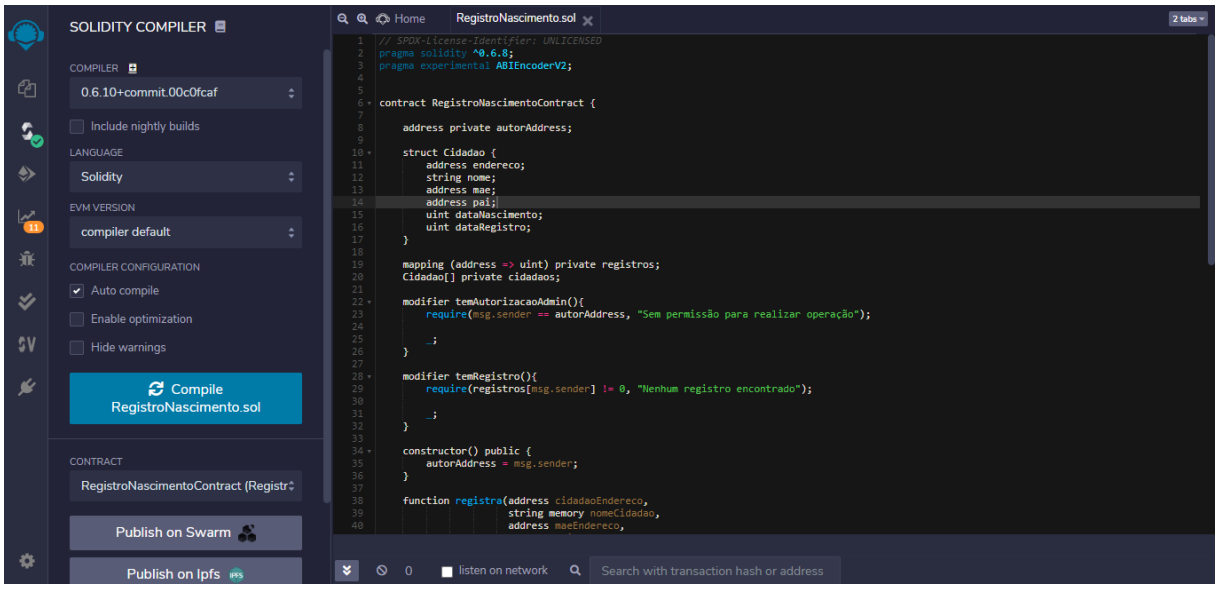
Para elaboração desta pesquisa foi desenvolvido uma API (*Application Programming Interface*) *RESTful* protótipo para simulação de um registro de nascimento utilizando os recursos e benefícios oferecidos pela Blockchain Ethereum.

LEVANTAMENTO DOS DADOS E RESULTADOS

DESENVOLVIMENTO

Para o desenvolvimento do *Smart Contract* foi utilizado a IDE Remix, conforme Figura 5, abaixo. Esta IDE tem o benefício de realizar a auto compilação do código enquanto acontece o desenvolvimento, para isto, ela faz uso de uma máquina virtual da *Ethereum* desenvolvida em Java Script.

Figura 5 – IDE Remix

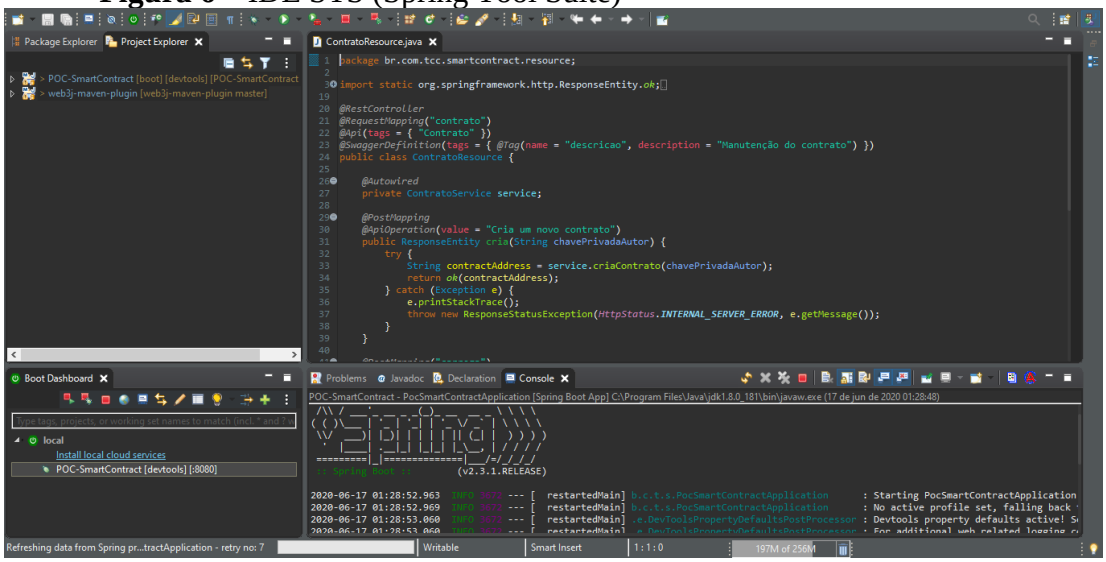


Fonte: Elaborado pelo Autor.

Para o desenvolvimento da API foi utilizada a IDE STS (Spring Tool Suite), descrita na Figura 6, a linguagem de programação Java e como framework de *bootloader*, o Spring

Boot. A IDE STS é um *fork* da tradicional IDE Eclipse, o grande benefício do STS em relação ao Eclipse está nas configurações pré-definidas que facilitam a integração com o *framework* Sprint Boot. O Spring Boot tem se tornado um padrão para desenvolvimento de softwares na plataforma Java, seus benefícios são inúmeros, como herança de dependências, configuração facilitadas por anotações e arquivos de propriedades usando reflexão, além da principal, que é trazer o servidor de aplicações Tomcat embarcado.

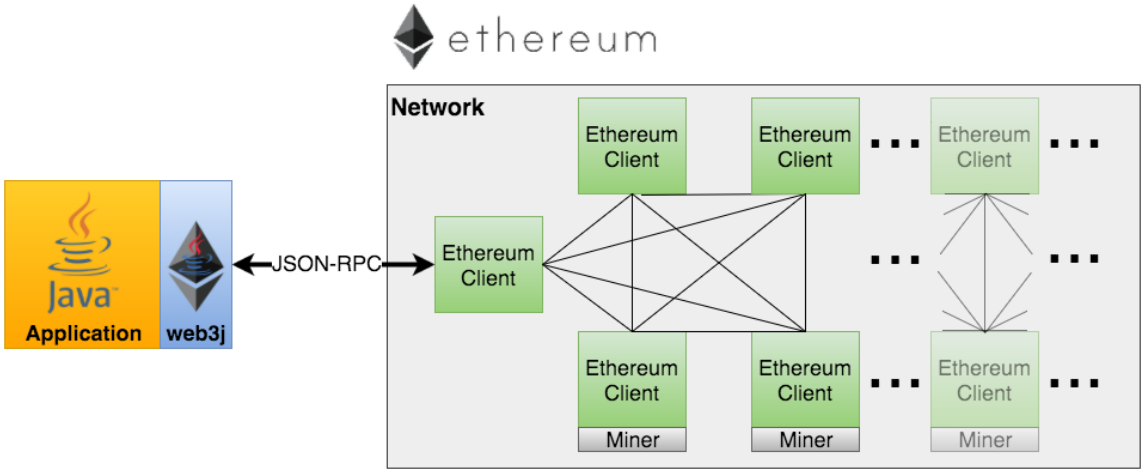
Figura 6 – IDE STS (Spring Tool Suite)



Fonte: Elaborado pelo Autor.

O projeto web3j foi usado para realizar o interfaceamento entre a API desenvolvida e a as funcionalidades do *smart contract*. Com a biblioteca web3j é possível interagir com o *smart contract*, já publicado na blockchain. Esta biblioteca contém um plugin (web3j-maven-plugin) que gera classes Java (*Wrappers*) para representar o contrato dentro do projeto e facilitar a interação com ele. A imagem 7, abaixo, demonstra o interfaceamento relatado acima.

Figura 7 – Biblioteca web3j

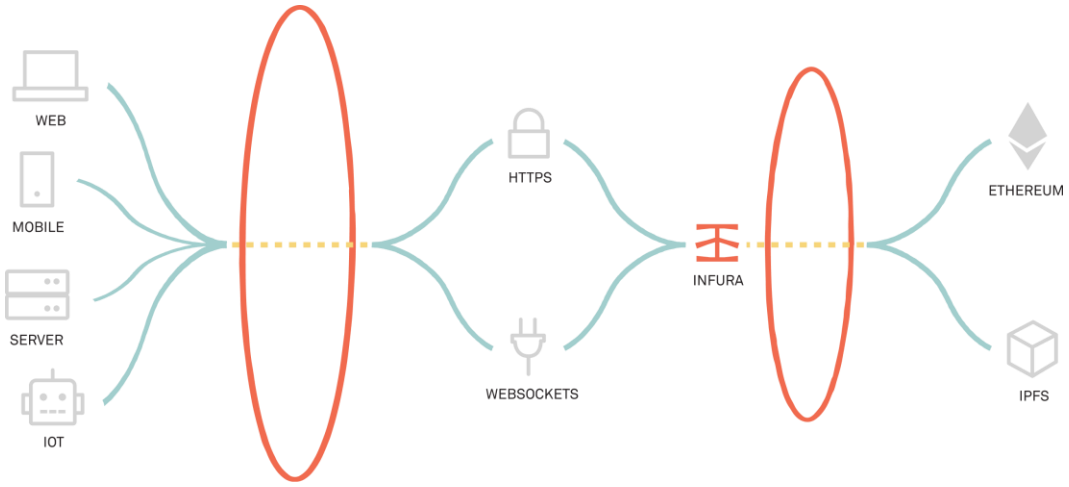


Fonte: WEB3J

A biblioteca web3j necessita de um serviço de gerenciador de nós para se comunicar fisicamente com a blockchain da Ethereum. Para não precisar configurar um gerenciador de nós no computador de desenvolvimento e agilizar os cenários de teste, se atendo mais fortemente as regras de negócio, foi utilizado os recursos da Infura que é uma plataforma

que facilita a interação com a blockchain da Ethereum através de serviços. Na figura 8, abaixo, é possível entender melhor a responsabilidade dessa plataforma nos cenários de teste.

Figura 8 – Infura

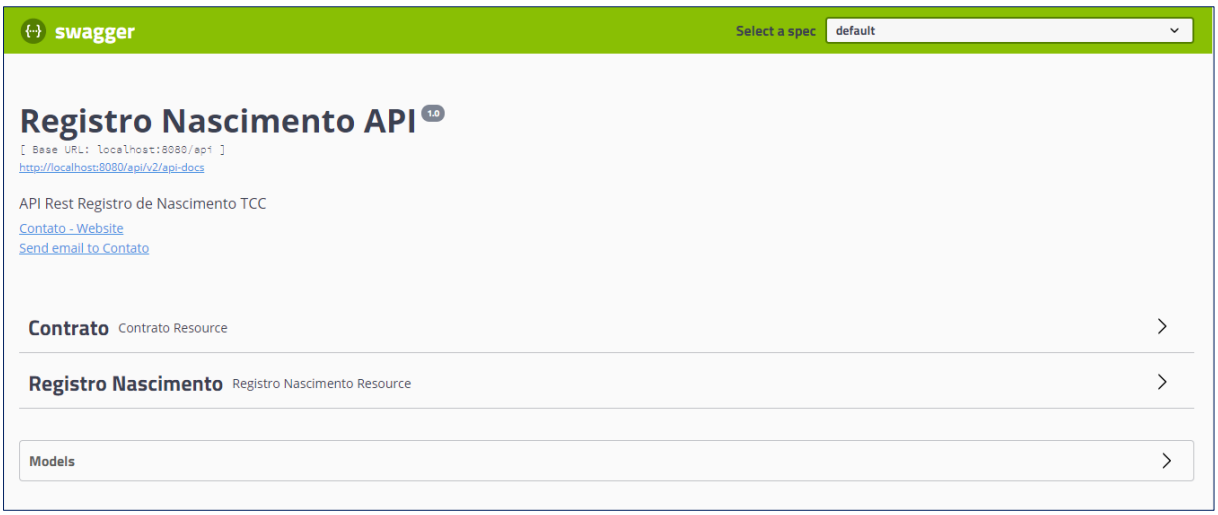


Fonte: INFURA

O projeto Ethereum disponibiliza uma blockchain de produção, chamada de *Mainnet*, e algumas outras para testes, chamadas de *Testnet*. Uma alternativa para testes seria hospedar a própria blockchain na máquina de desenvolvimento, criando assim o que chamamos de blockchain privada. Usaremos para hospedar o *smart contract* desenvolvido a *Testnet Ropsten*.

Para realizar as requisições para a API desenvolvida foi utilizado o padrão *OpenAPI* através do *Swagger*. Este padrão tem a responsabilidade de especificar modelos de requisições de uma API *Restful* de forma legível. Na figura 9, abaixo, podemos visualizar o Swagger da API desenvolvida nessa pesquisa.

Figura 9 – Especificação Swagger para a API desenvolvida na pesquisa



Fonte: Elaborado pelo Autor.

Com o objetivo de coletar resultados que medissem a funcionalidade, confiabilidade, usabilidade e eficiência foi realizado cenários de testes simulando um fluxo de cadastro e pesquisa de dados.

RESULTADOS

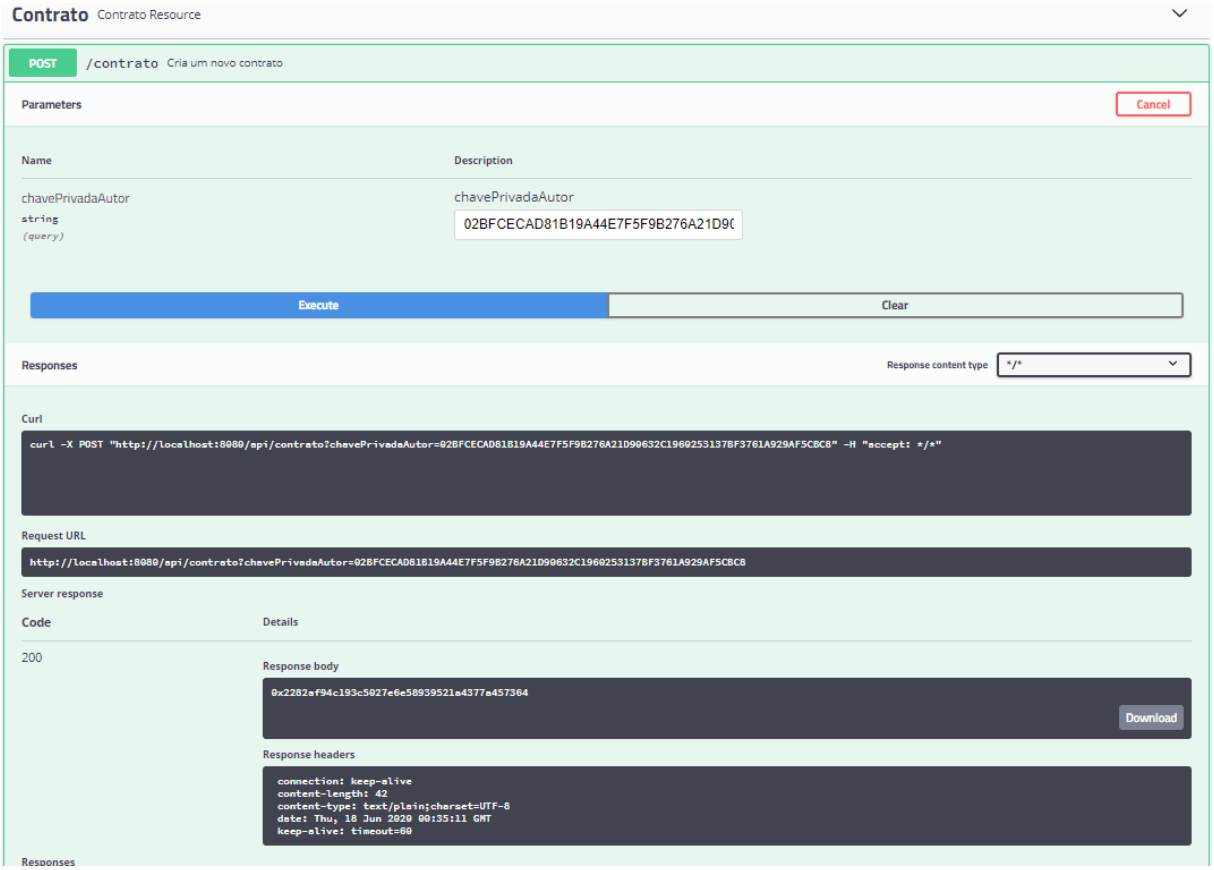
Quando interagimos com uma *smart contract* através da chamada de suas funções podemos ter nossas requisições classificadas como transações ou chamadas. A primeira é assim denominada por alterar o estado do contrato, ou seja, realiza a alteração dos valores das variáveis globais existentes no contrato. A interação denominada de chamada realiza apenas consulta nas variáveis do contrato ou faz cálculos em memória.

Para realizar interações do tipo transação, será preciso custear as taxas de rede que em uma blockchain do tipo PoW (*Proof of Work*) contém e são consideradas como recompensas para os minerados de plantão. Essas recompensas são basicamente o "salário" pago aos minerados por disponibilizar o seu poder computacional para validar os cálculos exigidos por minha transação. No caso da blockchain da Ethereum essa taxa é calculada em *Ether* que é a maior unidade monetária da blockchain.

Publicação do *Smart Contract*

Para disponibilizar o contrato na blockchain da Ethereum é necessário realizar uma requisição com verbo POST na rota '/contrato', conforme figura 10, abaixo. Essa requisição tem a primícias de já existir uma *wallet* que será chamada de autor do contrato. Deverá ser enviado junto requisição a chave privada da *wallet* do autor. Essa requisição será considerada uma transação que, apesar de não alterar o estado do contrato, está criando o mesmo. Essa operação levou o tempo de 17 segundos para ser minerada e autorizada e teve um custo de taxa de aproximadamente 0.026105971 *Ether*.

Figura 10 – Chamada para a publicação do *smart contract* .

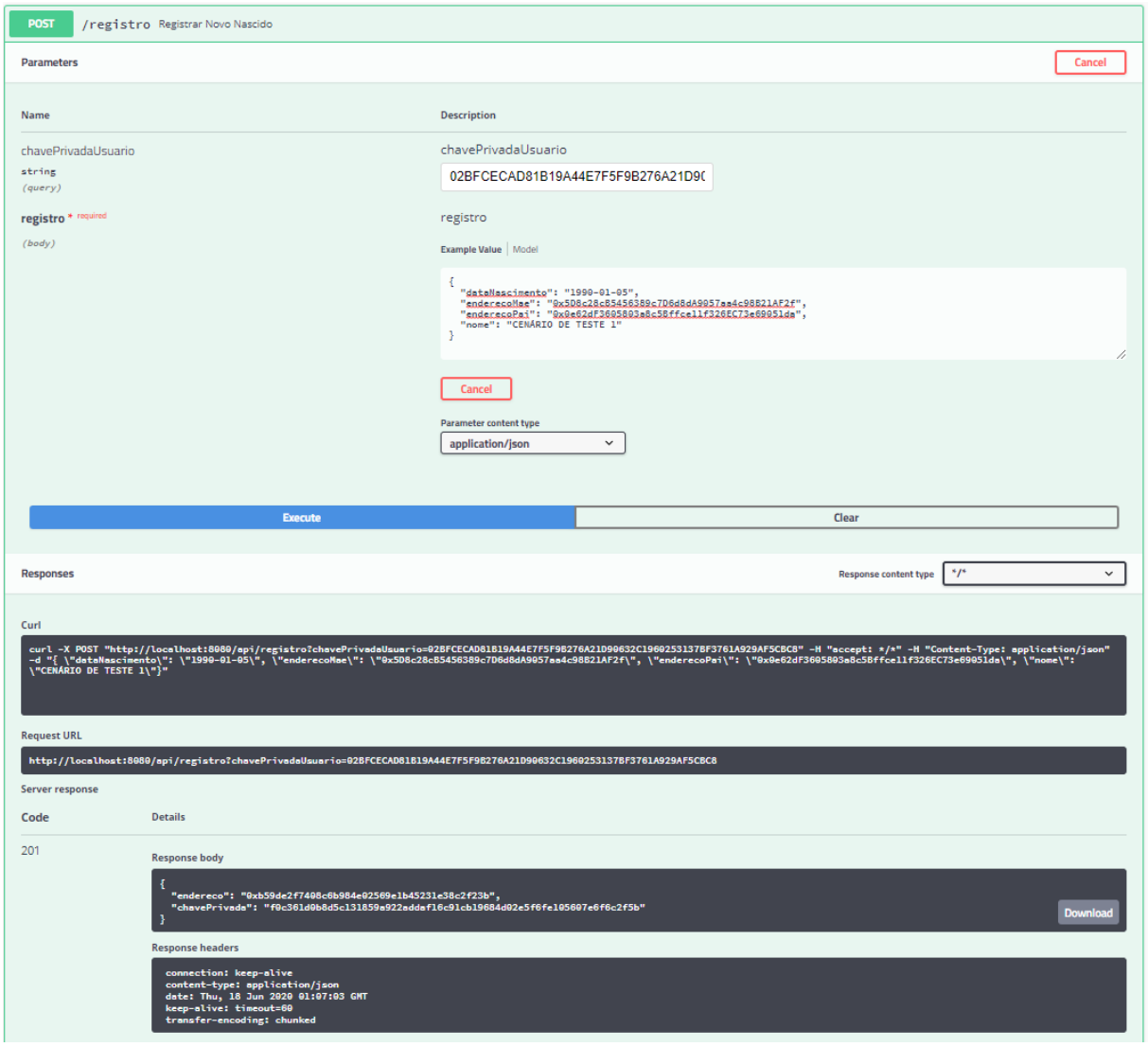


Fonte: Elaborado pelo Autor.

Registro de Nascimento

Para registrar um recém-nascido será necessário realizar uma requisição com o verbo POST na rota ‘/registro’, conforme figura 11, abaixo. Nessa requisição será necessário informar o nome do novo nascido, a data de nascimento e as chaves públicas do pai e da mãe. Será retornado um objeto contento a chave pública e privada do recém-nascido. Nesta operação do tipo transação tivemos um tempo de espera de mineração e validação de 15 segundos e um custo de 0.007808573 Ether de taxas.

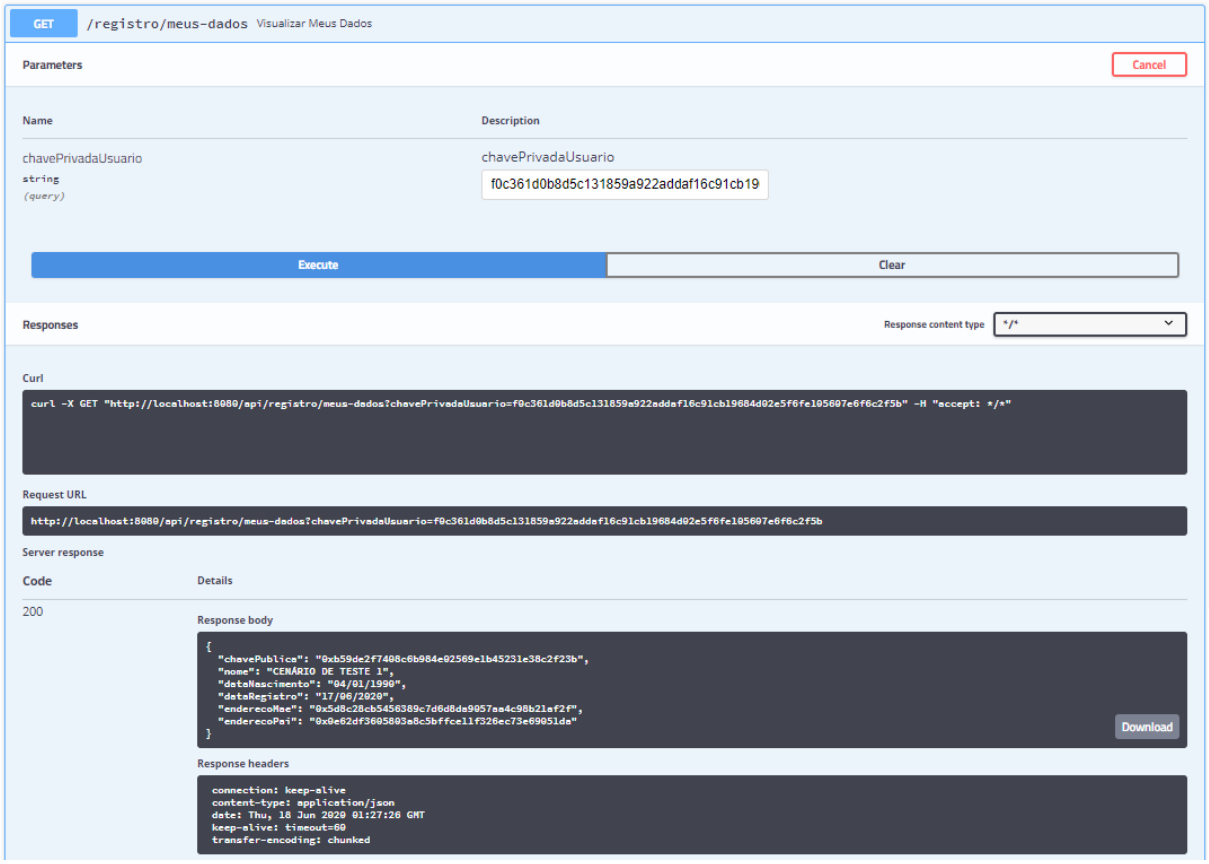
Figura 11 – Registro de um recém-nascido no *smart contract*



Fonte: Elaborado pelo Autor.

Uma importante funcionalidade é permitir o próprio registrado consultar suas próprias informações, e isso vai ser possível realizando uma requisição GET na rota ‘/registro/meus-dados’, conforme figura 12, abaixo. O registrado deve informar sua chave privada para a verificação da sua identidade. Nessa requisição do tipo chamada não teremos nenhum custo de *Ether* e o retorno aconteceu em um tempo de 214 milissegundos.

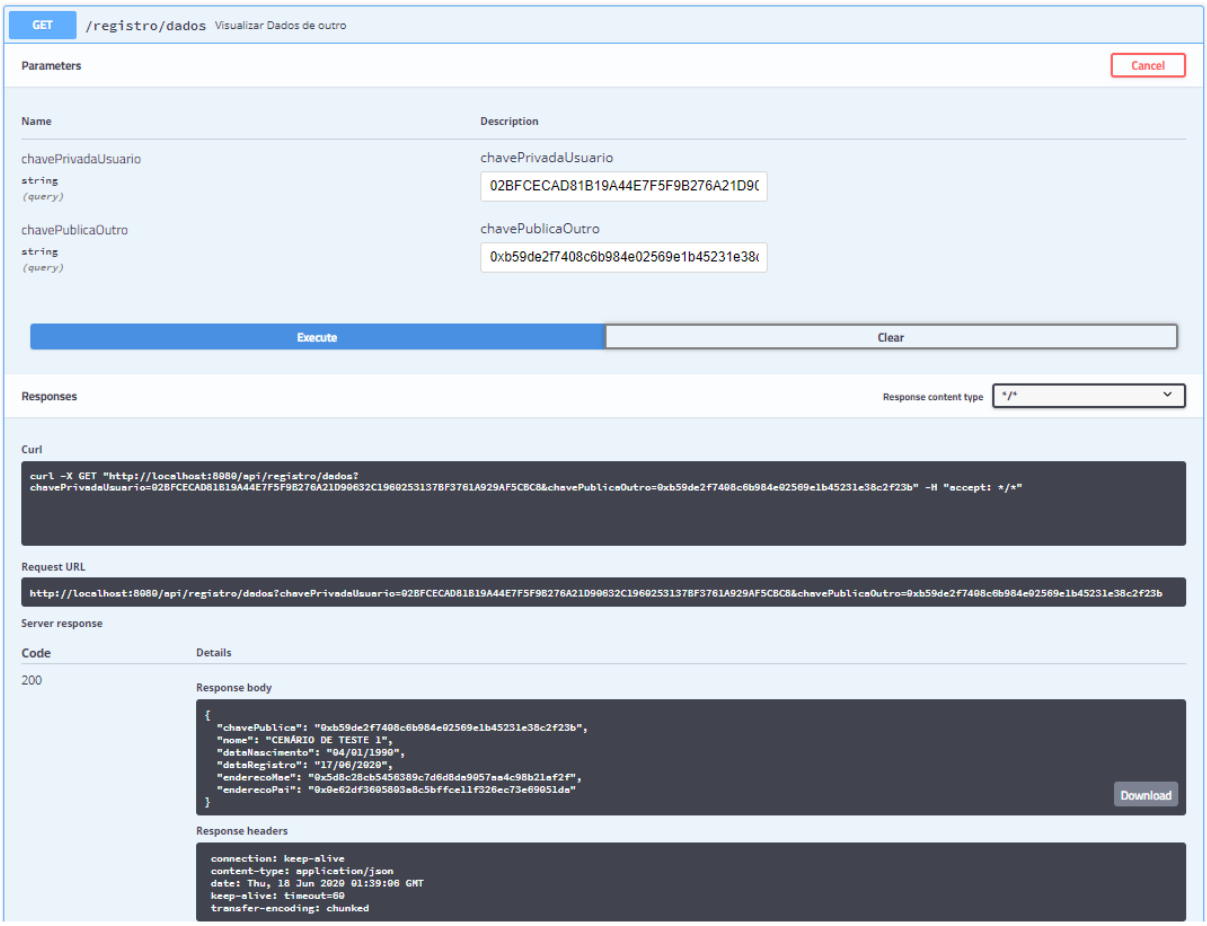
Figura 12 – Consulta de registro pelo próprio registrado



Fonte: Elaborado pelo Autor.

Uma outra funcionalidade que será permitida somente ao autor do contrato será a consulta do registro de qualquer registrado, conforme figura 13, abaixo. Para realizar a consulta de um registrado diferente do requisitante deve ser informado a chave privada do autor do contrato e a chave pública do registrado que se deseja consultar através de uma requisição GET na rota ‘/registros/dados’. Essa interação é do tipo chamada, por isso não tem custo de Ether, e levou 315 milissegundos para ser processada.

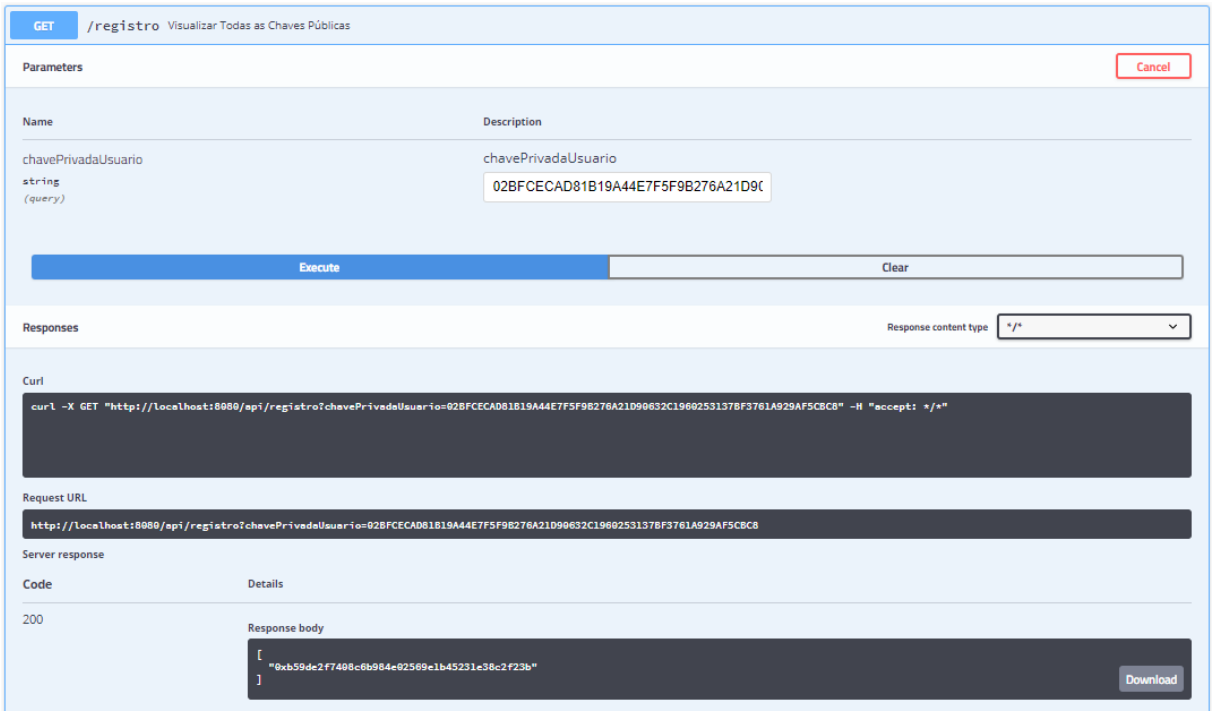
Figura 13 – Consulta de qualquer registrado realizada pelo autor do *smart contract*



Fonte: Elaborado pelo Autor.

Por último e não menos importante, o autor também terá permissão, e somente o autor, de consultar a lista de todos os registrados no contrato. Para tal, o autor do contrato deverá realizar uma requisição GET na rota ‘/registro’ informando sua chave privada, conforme figura 14, abaixo. Essa operação foi do tipo chamada e não teve custo de taxa em *Ether* e foi processada em 216 milissegundos.

Figura 14 – Consulta de todos os registrados realizada pelo autor do *smart contract*



Fonte: Elaborado pelo Autor.

CONCLUSÕES

Para a concepção do projeto foi necessário conhecimento de desenvolvimento de software na plataforma Java, seguindo o paradigma de orientação a objeto, e o padrão de desenvolvimento de API's *Restful*, usando a convenção Open API. Podemos ressaltar a grande importância do conhecimento voltado a tecnologia blockchain onde foi necessário recorrer a cursos externos e vários artigos científicos para aprofundar a sapiência na área. Deste modo, afirma-se que foi de extrema importância os diversos aprendizados teórico e tecnológico recebidos no curso de Sistemas de Informação.

O objetivo principal da pesquisa foi alcançado de modo satisfatório, podendo considerar que a funcionalidade dos recursos disponibilizados e a confiabilidade das informações atenderam o pressuposto de criar uma base unificada de identificação de pessoas na blockchain da Ethereum. Quanto a performance, no fator de eficiência, deve ser realizado melhorias no fluxo pensando em um contexto de comunicação assíncrona. Espera-se que o conceito aqui discorrido possa ser amadurecido quanto a confidenciabilidade das informações em relação a forma de distribuição da chave privada. Quanto a sua aplicação em um cenário de produção, será necessário realizar uma análise de viabilidade de custo para uma blockchain pública ou um possível uso de uma blockchain privada sem perder a confiabilidade.

Conclui-se que diante das melhorias a serem aferidas no processo, o conceito de se ter uma base de identificação dos cidadãos armazenadas em uma blockchain é de possível alcance e irá trazer inúmeros benefícios para a sociedade como um todo.

REFERÊNCIAS BIBLIOGRÁFICAS

BELTRÃO, K.; OLIVEIRA, F. O idoso e a previdência rural. In: CAMARANO, A. A. (Org.). Muito além dos 60: os novos idosos brasileiros. Rio de Janeiro: Ipea, 1999. p. 307-318.

BRONDI, Benjamin; BERMÚDEZ, René Raúl Zambrana. Departamento pessoal modelo. 4 ed. São Paulo: IOB, 2007. 806 p.

BUTERIN, V. Um contrato inteligente de próxima geração e plataforma de aplicativos descentralizada, white paper , 2014.

CAMARANO, A. A. Brazilian population ageing: differences in well-being by rural and urban areas. Rio de Janeiro: Ipea, 2002. (Texto para Discussão, n. 113).

CAETANO, M. A dinâmica fiscal da previdência social brasileira. In: CAMARANO, A. A. (Org.). Novo regime demográfico: uma nova relação entre população e desenvolvimento econômico? Rio de Janeiro: Ipea, 2014. p. 571-585.

CERVO, Amado L.; SILVA, Roberto da; BERVIAN, Pedro A. Metodologia Científica. 6ª ed. São Paulo: Ed. Pearson Prentice Hall, 2007.

CROSBY, M.; PATTANAYAK, P.; VERMA, S.; KALYANARAMAN, V. Blockchain Technology: Beyond Bitcoin. Applied Innovation, v. 2, p. 6-10, 2016.

FÉLIX, Claudia Lima; RIBEIRO, Heliton José; TOSTES, Fernando P. Uma contribuição à análise de fatores que influenciam o equilíbrio do sistema previdenciário. 10(39), 2008.

GIL, A. C. Como Elaborar Projetos de Pesquisa. Atlas, 2002. v. 4ª ed.

GIL, A. C. Como Elaborar Projetos de Pesquisa. Atlas, 2010. v. 5ª ed.

INFURA, 2020. https://infura.io/, acessado em 17/06/2020.

INSS, https://www.inss.gov.br, acessado em 19/05/2020.

LUCENA, A. U. de; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum, 2016.

LUIZARI, L. Blockchain Chega à atividade Notarial e Registral Brasileira. Cartórios com Você, 7. ed., ano 1, p. 12-30, mar/abr., 2017.

MALAQUIAS, Pedro Ferreira; DIAS, Luis Alves. Smart Contracts: Alguns Contributos Teóricos e Práticos, 2019.

MARTINELLI, Maria Lúcia. Pesquisa Qualitativa: um instigante desafio. São Paulo: Veras, 1999.

MEDICI, Andre: Reassembling social security: a survey of pensions and health carere forms in Latin America, 2009.

MOREIRA, Daniel Augusto. O método fenomenológico na pesquisa. São Paulo: Pioneira Thomson, 2002.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

NOLASCO, L. Evolução histórica da previdência social no Brasil e no mundo. Revista Âmbito Jurídico, ano 18, n. 98, 2012.

PERERA, Luiz Carlos Jacob; FREITAS, Eduardo Costa de; IMONI-ANA, Joshua Onome. Avaliação do sistema de combate às fraudes corporativas no Brasil. Agosto 2014.

REIS, Jose Milton dos; FERNANDES, Marcos; ANTUNES, Olavo Varajão. A Polícia, o Ministério Público e a Investigação Criminal, 2008.

SALOMAA, Arto. Public Key Cryptography, 1996. Ed. Springer 2a Ed. ISBN 978-3-642-08254-2. 55-71.

SILVA, Edna Lúcia; MENEZES, Estera Muszkat. Metodologia da pesquisa e elaboração de dissertação. 3. ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001. 121p.

STAWICKI S. P., FIRSTENBERG M. S., PAPADIMOS T. J. What's new in academic medicine? Blockchain technology in health-care: Bigger, better, fairer, faster, and leaner. Int J Acad Med, 2018.

SZABO, N. Formalizing and Securing Relationships on Public Networks. First Monday, v. 2, n. 9, 1 Sep. 1997.

UOL, Fraudadores do INSS ganham aposentadoria com RG e certidão falsos, 2019. https://economia.uol.com.br/noticias/redacao/2019/01/24/principais-fraudes-contra-previdencia-falsificacao-documentos.htm, acessado em 26/05/2020.

WEB3J, 2019. https://docs.web3j.io/ , acessado em 17/06/2020.