UNISINOS

Programa de Pós-Graduação em

Computação Aplicada

Mestrado Acadêmico

Christopher de Paula Gomes

USO DE NFT NO RECEITUÁRIO DIGITAL: UM MECANISMO DE SEGURANÇA MÉDICA E FARMACÊUTICA NO SISTEMA DE SAÚDE PÚBLICA

São Leopoldo, 2022

G633u GOMES, Christopher de Paula
Uso de NFT no receituário digital: um mecanismo de segurança médica e farmacêutica no sistema de saúde pública / Christopher de Paula Gomes. – 2022.
52 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Computação Aplicada, 2022.
"Orientador: Prof. Dr. Rodolfo Stoffel Antunes."

1. NFT (*non-fungible tokens)*. 2. Receiturário digital. 3. Segurança farmacêutica. 4. Saúde pública. I. Título.

CDU: 004

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecário: Henrique da Cruz Monteiro – CRB 1/2950)

RESUMO

A adoção de criptoativos é crescente e novas utilidades para eles vêm surgindo a cada dia. Algumas redes de criptoativos permitem alta escalabilidade, provêm privacidade a seus usuários e registro confiável de objetos virtuais e transações. Criptoativos podem ser tokens não fungíveis (NFTs), os quais são gerados por um contrato específico, mas que são distintos entre si. Os NFTs podem representar objetos do mundo real e provêm garantias de rastreabilidade que são compatíveis com osrequisitos de um mecanismo para controle de venda de medicamentos. Dado este contexto, este trabalho teve como objetivo analisar a aplicação de NFTs na representaçãode permissões de compras para medicamentos restritos. Foi desenvolvido um modelo dearquitetura baseado em Blockchains e NTFs que permite o armazenamento de prescrições médicas e das respectivas permissões para aquisições de medicamentos controlados. Este modelo foi implementado e testado utilizando a segunda camada da Ethereum voltada para testes, chamada Mumbai. Nesta rede foi constatado que o custo das solicitações de criação de NFT são menores do que R$0,01 e que o tempo das transações são menores que 15 segundos, o que torna a implementação viável. Esses resultados mostram que é possível implementar um sistema de receitas médicas através de uma rede escalável, barata e confiável.

Palavras-chave: NFT; Rede Polygon; Rede Ethereum; receita médica

ABSTRACT

The adoption of crypto assets is increasing and new uses for them are emerging every day. Crypto asset networks enable high scalability, provide privacy to their users, and offer reliable registration of virtual objects and transactions. Crypto assets can be non-fungible tokens (NFTs) generated by a specific contract, but which are distinct from each other. NFTs can represent real-world objects and provide traceability guarantees that are compatible with the requirements of a drug sales control mechanism. Given this context, this work analyzes the application of NFTs in the representation of purchase permits for restricted drugs. It proposes an architectural model based on Blockchains and NTFs to allows the storage of medical prescriptions and the respective permissions for the acquisition of controlled drugs. This model was implemented and evaluated using Ethereum's second layer for testing, called Mumbai. In this network, the cost of NFT creation requests is less than R$0.01 and the transaction time is less than 15 seconds, which makes the implementation viable. These results show that it is possible to implement a medical prescription system througha scalable, cheap, and reliable network.

Keywords: NFT; Polygon network; Ethereum network; Medical prescription

SUMÁRIO

Lista de Figuras

Lista de Tabelas

1 INTRODUÇÃO

Atualmente as prescrições para medicamentos controlados são feitas de acordo com a Lei 9.965/2000, juntamente com regras e resoluções do Conselho Federal de Medicina. O processo é manual e, embora exija informações como o número do CRM domédico, carimbo e assinatura, é um procedimento sujeito a falsificações que levam a compra e venda ilegal de medicamentos (LOPES, 2019). Consequentemente, pode haver prejuízos a saúde de algumas pessoas e ao meio social onde está irregularidadeocorra.

Novos mecanismos para o gerenciamento de medicações controladas são importantes para se evitar irregularidades que podem gerar consequências negativas paraa sociedade. Novas ferramentas computacionais têm surgido, contudo, muitas delas podem levar a abusos derivados da falta de rastreabilidade das operações, principalmenteem um cenário onde agências governamentais e grandes organizações privadas têm cadavez menos confiança por parte da população, conforme é possível verificar por exemplo em Roumeliotis (2019). Neste sentido, é necessário que se implemente um sistema que ao mesmo tempo promovam a rastreabilidade de medicações controladas e protejam a privacidade dos indivíduos através de processos simples e confiáveis.

Particularmente, no que se refere a receituário médico, existem tentativas de implementação. Por exemplo, o SUS possui alguns trabalhos neste sentido conforme podemos ver em Silva (2019). Porém não há tentativas de se implementar soluções utilizando a tecnologia NFT. Esta solução podemitigar a dificuldade de se ter uma solução escalável, transparente e que ao mesmo tempo suporte a privacidade dos usuários. A dificuldade de se implementar algo neste sentido está muitas vezes relacionada a falta de confiabilidade e medo de sofrer ataques ou manipulações dos dados que estão em uma rede de computadores. Em um cenário onde o paciente sai de uma consulta que lhe foi receitado variados tipos de remédios com regrasde tempo e dias para os consumir, esta mesma receita leva um carimbo do médico contendo seus dados médicos e sua assinatura junto a uma data para validação e assim opaciente pode levá-la a uma farmácia para realizar a compra destes medicamentos. A farmácia, caso desconfie da receita, pode realizar a validação através de uma checagem com o hospital ou consultório, o que passa por um processo lento e burocrático. Além disso, hoje é possível realizar verificação automática através do uso de recursos digitais, como contratos inteligentes, conforme apresentado ao longo deste trabalho.

Atualmente, devido a pandemia da COVID-19, o Manual de Orientação ao Farmacêutico para Prescrição Eletrônica, elaborado pelo Conselho Regional de Farmáciado Estado de São Paulo, fundamentou a prescrição médica digital, através da Medida Provisória (MP) nº 2.200-2, de 24 de agosto de 2001 (alterada pela Lei nº 14.063/2020), legislação específica para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica.

A partir da receita digital, o paciente consegue realizar a compra de medicamentosde uso comum sem precisar levar ou enviar a receita em papel, mas ela não é permitida para remédios de uso controlado. O que não traz grandes avanços ou benefícios ao setor,que tem a falsificação de receitas como um de seus maiores problemas, além do uso descontrolado de medicamentos. Devido a processos demorados e com grande possibilidade de ocorrência de falhas, há grande potencial de prejuízos financeiros tanto ao paciente quanto a órgãos

como o SUS, os quais não conseguem realizar o uso ou controle apropriados de medicamentos.

Novos mecanismos para o gerenciamento de medicações controladas são importantes para se evitar irregularidades que podem gerar consequências negativas paraa sociedade. Novas ferramentas computacionais têm surgido, contudo, muitas delas podem levar a abusos derivados da falta de confidencialidade, principalmente em um cenário onde agências governamentais e grandes organizações privadas têm cada vez menos confiança por parte da população. É necessário que se implemente um sistema queao mesmo tempo promovam o controle de medicação controlada e proteja a privacidade dos indivíduos através de processos simples e confiáveis.

Contratos inteligentes são uma tecnologia recente que visa garantir a autenticidadede transações para os usuários sem a necessidade de uma terceira parte confiável. Uma função recente dos contratos inteligentes é a criação de tokens não fungíveis (*non- fungible tokens* ou NFTs), que podem representar objetos do mundo real. Em particular, NFTs permitem representar receitas médicas ou permissões de compras para medicamentos controlados. Entretanto, tal possibilidade ainda não é amplamente explorada pela literatura. Neste contexto, o presente trabalho explora a seguinte questão de pesquisa: *Qual seria o modelo de uma arquitetura para o gerenciamento da venda demedicamentos controlados baseada no conceito de tokens não fungíveis?*

Dada a popularidade de fraudes realizadas com receitas médicas, a aplicação da tecnologia de NFTs permite mitigar sua ocorrência. Portanto, este trabalho tem como objetivo apresentar o modelo para um sistema de receitas baseado em permissões de compra de medicamento emitidos através de NFTs. Além disso, ele apresenta a implementação de um contrato inteligente que emite NFTs que representam permissões de venda para medicamentos restritos, utilizada para avaliar sua funcionalidade e escalabilidade. Nesse sentido, as principais contribuições deste trabalho são as seguintes:

- Apresentar uma solução para a emissão de permissões de compra que evite fraudede forma transparente e que ao mesmo tempo respeite a privacidade dos pacientesque movimentam as permissões de compra na rede;
- Discriminar os processos que o sistema deve estabelecer para fazer as transações entre os atores que usam a rede;
- Validar a viabilidade da proposta através de uma prova de conceito em uma rede Blockchain real, considerando ferramentas como o framework Brownie e o OpenEHR.

O restante desta dissertação está organizado da seguinte maneira. O Capítulo 2 introduz os principais conceitos relacionados ao trabalho desenvolvido. O Capítulo 3 descreve os trabalhos relacionados ao uso de Blockchains para o gerenciamento de prontuários eletrônicos. O Capítulo 4 introduz a arquitetura baseada em NFTs para o gerenciamento da permissão de compra de medicamentos. O Capítulo 5 discute a prova de conceito desenvolvida e os resultados obtidos com sua avaliação. Por fim, o Capítulo6 apresenta a conclusão do trabalho e suas direções futuras.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como objetivo esclarecer e pontuar os principais conceitos que servirão de base para o desenvolvimento deste trabalho. Tais conceitos incluem atecnologia Blockchain, incluindo sua descentralização, usabilidade, segurança e variadaspossibilidades de uso principalmente no campo da saúde com receituários eletrônicos e levando a tentativa de uso em receituário médico.

2.1 BLOCKCHAIN E APLICAÇÕES

O Blockchain é um meio que garante o desenvolvimento de arquiteturas para a execução de transações entre duas ou mais partes de forma confiável, sem que seja necessária uma autoridade central que valide ou estabeleça uma maior confiança entre elas. Esse conceito excluiu uma camada inteira, que anteriormente era preciso para transacionar ou ainda executar qualquer instrução. (WANG, et al, 2019).

A tecnologia da Blockchain pode ser utilizada para autenticar, autorizar ou ainda auditar os dados criados através de dispositivos. Com isso, por conta de sua natureza descentralizada, é excluída a necessidade de confiança por meio de terceiros e não tem um único ponto se quer de falha. (CHICARINO et. al, 2017).

O Blockchain realiza de maneira descentralizada, onde há uma cópia dos dados eé encontrada através de cada nó e, sendo assim, qualquer novo nó pode ser modificado apartir da rede. Ultimamente, o Blockchain ajudou diversas extensões no mercado, principalmente as que envolvem finanças, saúde eletrônica, serviços públicos, gestão de ativos, regulamentações governamentais, negócios imobiliários, logística, entre outros. (ZHENG et al, 2017). Com isso, observe-se que houve um grande sucesso por conta de sua capacidade de trabalhar de forma ampla, segura, sem que seja preciso que uma autoridade de confiança autorizar.

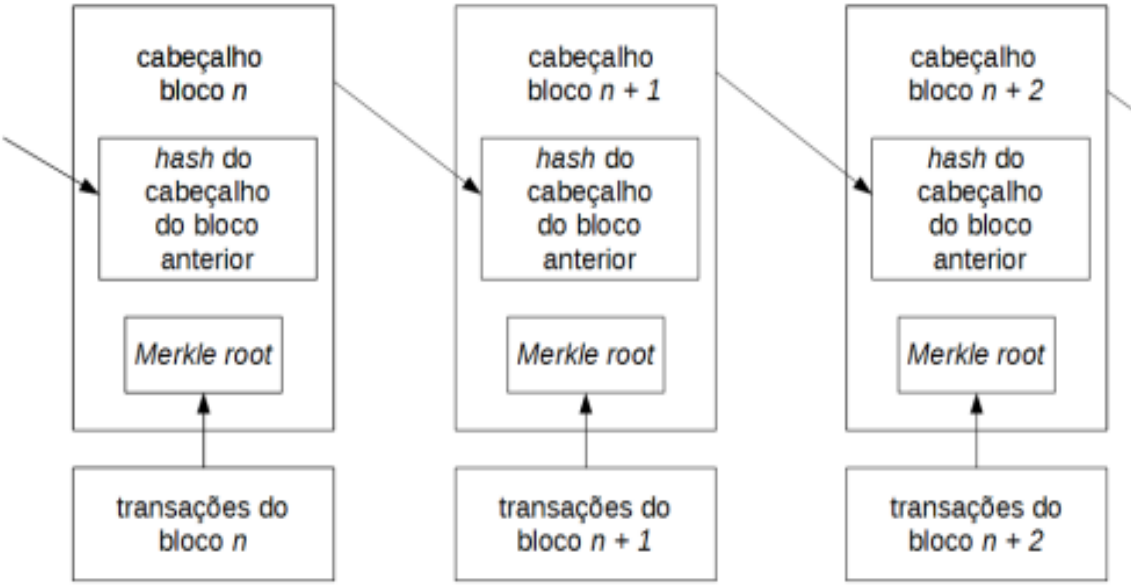
O Blockchain é na verdade uma rede distribuída em que possa realizar transações sem que seja preciso depender de intermediários, sendo assim, as validações realizadas por meio de uma transação são realizadas através da rede de computadores que usam o compartilhamento entre si que ela tem. Os computadores chamados de “nós” são os encarregados por reconhecerem as transações para que assim tornem válidas sem usar a instituição central de verificação. Um exemplo disso é o cartão de crédito que por meio de uma transação passa por uma operadora da máquina para autenticar a operação, que através da operadora do cartão que faz validação e, só com isso, o banco recebe a informação necessária para também autenticar/validar. Com isso é possível ver que há defato uma burocracia desnecessária nessas organizações, além de ter que haver umintermediário.

Não há como falar que ao utilizar o Blockchain não haverá mais fraudes, porém, não existe sistema que possa garantir algo assim, nenhum possui uma segurança total. Noentanto, é possível dizer que o Blockchain demonstra um nível eficiente em relação à segurança, já que ele trata os dados de forma imutável por meio dos blocos (Figura 1). Assim, é possível observar que isso é bastante complicado de ocorrer, já que não é fácil mudar o sistema, já que sua programação necessita da conclusão da rede em si, e como é um consenso distribuído, se uma informação for alterada de maneira indevida, ou mesmo

que uma pessoa se arrisque em fazer algo desse tipo, será muito fácil descobrir de quem se trata.

O banco de dados possui uma descentralização que não permite que fraudes ocorram por meio de mudanças de informações. Para que essa fraude ocorra, é preciso que a fraude ocorra em todos os bancos de dados do sistema, o que é obviamente impossível de acontecer. O Blockchain é uma rede peer-to-peer e seu nome tem relação ao fato de que ele é realizado por meio de uma cadeia de diversos blocos, onde eles precisam ser aprovados no consenso da rede para que assim sejam colocados. Esses blocos necessitam um do outro e eles tem um resumo, que é um tipo de Hash, assim, precisam aguardar em uma fila para serem colocados de acordo com a medida que chegam na rede. Essa Hash precisa se harmonizar com o Hash do bloco processador, já que é isso que faz com que os blocos sejam mutualmente dependentes. (MARTINS, 2019).

Figura 1- Cadeia de blocos de uma Blockchain



Fonte: Lucena e Henrique (2016)

Para fazer com que os blocos sejam formados e tenham as transações e os minerados, é necessário fazer uma quantidade elevada de cálculos de frequência avançada. Esses cálculos visam encontrar o Hash correto para o bloco a ser inserido na cadeia de blockchain. O poder computacional preciso para estes cálculos é considerável e aumenta com o passar do tempo. Por exemplo, o Bitcoin possui um poder computacional que impede que sua mineração ocorra em casa. (SEOK; PARK; PARK, 2019).

O Blockchain pode ser feito por meio de um banco de dados descentralizado semque seja necessária uma autoridade central. Dessa forma, ele pode servir como um centrode trocas de confiança entre diversas entidades sem que algumas tenham que confiar umana outra, nem mesmo como intermediários, por isso, é possível criar moedas financeiras altamente confiáveis. Isso demonstra que há de fato uma revolução, pois os sistemas de câmbio, onde, historicamente existe a necessidade de um intermediário que seja realmente confiável diante de todas as partes.

Um exemplo que pode ser usado é quando uma pessoa compra um objeto que é utilizado em alguma plataforma on-line, sendo responsável por analisar, ao trocar uma porcentagem, que a transação foi feita com sucesso e meio que compensa as partes caso ocorra alguma fraude. Do mesmo modo, quando um banco concorda em oferecer um empréstimo para uma empresa, através de um acordo explícito por meio de um contrato juridicamente vinculativo com o Estado, com seus poderes abusivos, é o que faz com quea obrigação estabelecida no contrato seja cumprida corretamente. Porém, é importante mencionar que isso não é preciso quando se trata da Blockchain. (MIRAZ; ALI, 2018).

Quando há moedas clássicas, automaticamente há também uma autoridade monetária, chamada de Bancos Centrais. Esses bancos possuem capacidade de dar mais unidades monetárias: Eles possuem poder para estabelecer o preço base para dar de crédito e eles decidem isso de acordo com a política macroeconômica, como por exemplo, a estabilidade em longo prazo, metas de inflação, taxa de importação e exportação, entre outros requisitos. (MIRAZ; ALI, 2018).

Sobre as criptomoedas, pode-se dizer que elas se baseiam em Blockchains, o que exclui a necessidade de haver uma autoridade central, o que é visivelmente mais vantajoso. Os requisitos para realizar novas unidades monetárias são estipulados previamente. Pode-se usar novamente a Bitcoin como exemplo, pois ela é uma nova moeda que toda vez que é emitida, um bloco é extraído (e isso ocorre a cada 10 minutos)o que é colocado na posse do nó que o extraiu. O valor cai em média a cada quatro anos e o sistema foi criado para chegar a uma totalidade de cerca de 21 milhões de Bitcoins noano de 2040. A incerteza política diante desse tipo de decisão praticamente some, mas ela também exclui por completo a possibilidade dos Estados usarem os bancos centrais paraconseguir alguma vantagem nos setores desejados ou ainda prejudicar certos setores.

Há diversas criptomoedas e elas compartilham suas utilidades como se fossem um tipo de sistema de pagamento. Algumas utilizam sua própria Blockchain, já outros trabalhar de acordo com a Blockchain do Bitcoin. Sua operação é consideravelmente heterogênea e todos eles procuram estabelecer melhorias em relação ao Bitcoin.

É provável que a alternativa mais eficiente seja o Ethereum, que é a segunda criptomoeda com capitalização bastante elevada. A Ethereum tem seu próprio Blockchain, o que difere do Bitcoin, sendo também baseado no PoW (acrônimo para prova de trabalho). Além de ser uma criptomoeda, a principal contribuição de contratos Ethereum são os chamados Contratos Inteligentes. (BUTERIN, 2014).

Os contratos inteligentes são scripts (códigos pequenos) residente auto executávelno Blockchain que procuram automatizar processos comerciais de um jeito seguro e evidente para os participantes. (MIRAZ; ALI, 2018).

Conforme a IBM, um Smart Contract (Contratos inteligentes) possui algoritmos em seus blockchains, por isso, quando é preciso impor requisitos previamente estabelecidos, eles são mais facilmente atendidos. Esses contratos são executados para realizar acordos estabelecidos inicialmente, com isso não há a necessidade da existência de intermediários para que haja confiabilidade no sistema.

Os contratos inteligentes são protocolos diretos entre dois ou até mais computadores implementados por meio de algoritmos. Eles procuram transmitir ativos por meio da Blockchain quando ações específicas são colocadas. Os algoritmos são feitossem que haja interferência de atores durante o processo. Há com isso a caracterização daausência de terceiros por meio de disputas. (IBM, 2021).

2.2 AS REDES BITCOIN E ETHEREUM

2.2.1 Primeira Blockchain – a rede do Bitcoin

Inicialmente é importante mencionar que o primeiro Mainstream Blockchain, sendo ainda considerado o mais conhecido no mundo, é o Bitcoin. Ele possui sua própriamoeda, chamada de BTC, onde os usuários conseguem comprar, vender e negociar entreas pessoas. Enviar e receber o BTC com outros peers na rede é o que estabelece como astransações funcionarão nos blocos do Bitcoin. Porém, como as informações financeiras confidenciais desse tipo são guardadas entre os pares e compartilhadas, é necessário ter uma forma de analisar se as informações armazenadas e posteriormente divulgadas serãocolocadas entre outros pares e assim não forem mudadas de forma prejudicial.

Nisso, é preciso pensar nos mineradores, isso porque, os mineradores são os verificadores de diversos Blockchains. Ao analisar essa verificação é computada por meiode cada minerador e isso é feito por um tipo de processo onde diversas transações em bloco são hash separadamente e cada hash possui uma entrada para outro hash criando assim uma estrutura de hashes em formato de árvore, conhecido como Merkle Tree. Um hash raiz é feito por mineradores que entendem dessa operação. Esses mineradores que usam a hash raiz possui uma pequena fração matematicamente estabelecida por meio de outros mineradores na rede tendo seu bloco imortalizado no livro-razão e colocado em uma cadeia de blocos analisados (a origem dos Blockchain possui seu próprio nome). Esse processo é feito para evitar que os mineradores enganem em relação ao número de transações e o conteúdo que foi criado dentro de cada uma das transações em um determinado bloco.

2.2.2 Contratos inteligentes Ethereum: um tipo diferente de blockchain

O Ethereum é uma criação parecida, porém única, de Blockchain, da mesma forma como o Bitcoin, ele possui sua moeda própria, conhecida como ETH. Porém, a rede Ethereum é uma Blockchain própria, já que, diferente do Bitcoin, tem uma máquina virtual própria chamada Ethereum (EVM) big-endian que se baseia em pilha. O EVM é parecido com à Java Virtual Machine (JVM) e é utilizado para fazer funcionar programascomo o Smart Contracts, que possuem instruções EVM de nível byte. Desse modo, comoa JVM, há opções que garantem que um programa faça cálculos e estabeleça a máquina de estado para frente, como ADD, SHL, LT entre outras. De forma parecida à linguagemJava e a linguagem JVM possuem requisitos em nível de byte, sendo criadas compilando uma linguagem específica de programação, conhecido como Solidity, para instruções de bytecode compatíveis com EVM, lugar que esses contratos conseguem ser criados.

Ainda que os contratos possuam características próprias comparado com outros programas que possuem linguagens assim, quando há um contrato, ele costuma ser encaminhado para a rede onde há instruções EVM podendo ser executadas através dos membros dessa rede, esse ato de encaminhamento é conhecido como implantação de contrato.

Durante a realização de implantação, o construtor de um contrato é chamado somente uma vez e o bytecode menos o código do construtor é colocado no Blockchain imutável, nele seu bytecode não pode ser mudado. A única forma de um programa não estar mais disponível é no caso do seu bytecode ser danificado por meio do uso de uma função programada que faz com que a instrução de autodestruição EVM seja ativada. Essa função é colocada para que o desenvolvedor a inclua ou não ao redigir o contrato, portanto, é opcional.

Os contratos possuem características parecidas com os programas regulares que são usados de diversas maneiras. Diante disso, outros programas, como os contratos Ethereum possuem um nome. Visto que são encaminhados para implantação na rede Ethereum, os contratos possuem um tipo de endereço hexadecimal próprio de cerca de 42 caracteres, compostos por diversos números e letras maiúsculas e também minúsculas (como o, 0x12a34C55...). Isso garante que os usuários consigam pesquisar as transaçõesno livro-razão onde os endereços estavam envolvidos através de um site online que rastreia o livro-razão. Também é possível que usuários e outros contratos usem funções dentro do programa, mas é necessário que eles possuam informações próprias sobre o contrato. (Ver sobre isso na seção 1.3 da ABI).

Os contratos precisam possuir o estado, o que faz com que um contrato tenha o ETH, sendo a forma mais importante de moeda do Ethereum. O contrato pode ser carregado com ETH durante a implantação, porém, também pode ser enviado ETH, ondedeverá ser colocado o endereço (o nome) de quem pertence o contrato. O contrato tambémpode enviar ETH para outros contratos, ou ainda, encaminhar ETH para os usuários diretos onde eles possuem seus endereços pessoais conhecidos como endereços decarteira, o que depende da lógica de negócio do contrato.

Diante da tecnologia para executar programas desse tipo e acompanhar a entradae saída de dinheiro, um contrato consegue realizar diversas coisas que, de outra maneira, acabaria com toda atenção e esforço colocados por meio de um agente humano, como trabalhar como um intercessor de duas partes. Um ótimo exemplo que pode ser usado, é que ao comprar uma casa, uma pessoa consegue colocar dinheiro em um contrato e passara escritura eletronicamente. Ao configurar um fundo fiduciário, um contrato consegue liberar fundos de em uma data estabelecida. Há ainda diversos casos onde é possível investir, fazer outras blockchains, jogar, entre várias outras funções.

2.2.3 Smart Contract

Smart Contracts (ou em português, Contratos Inteligentes) são programas de computador auto executáveis baseados na tecnologia blockchain que executam funções automaticamente após a ocorrência de um evento desencadeador (SWAN 2015; MATTILA, 2016). Tais contratos existem apenas em formato digital e podem incluir duas ou mais partes participantes. Como a estrutura blockchain não permite alteração de suas propriedades uma vez que o código foi programado, os contratos inteligentes também não. Isso significa que os termos de qualquer contrato desse tipo são lineares e serão executados automaticamente uma vez acordados (SWAN, 2015). Por exemplo, se um contrato inteligente for estabelecido entre um comprador alemão e um vendedor americano, que inclua o pagamento de 20% dos fundos, uma vez que as mercadorias sejam desembaraçadas pela alfândega, o contrato liberará automaticamente os fundos após a confirmação entrou no blockchain que a estância aduaneira liberou as mercadorias. Não há necessidade – nem possibilidade – de participantes ou

intermediários verificarem o pagamento ou alterarem as condições do contrato (CHRISTIDIS; DEVETSIKIOTIS, 2016).

A estrutura teórica dos contratos inteligentes pode ser atribuída ao cientista da computação e jurídico americano Nick Szabo. Ele mencionou o termo pela primeira vez em um artigo em 1994 que o descreve da seguinte forma:

> Um contrato inteligente é um protocolo de transação computadorizado que executa os termos de um contrato. Os objetivos gerais do design de contrato inteligente são satisfazer condições contratuais comuns (como termos de pagamento, garantias, confidencialidade e até mesmo aplicação), minimizar exceções maliciosas e acidentais e minimizar a necessidade de intermediários confiáveis.

Tais transações podem incluir transações simples de compra/venda ou também podem ter instruções mais extensas embutidas nelas. Semelhante aos contratos no sentido tradicional, os contratos inteligentes envolvem um acordo entre diferentes partes para fazer ou não fazer algo em troca de outra coisa (Swan 2015a, 17). Enquanto os contratos tradicionais exigem que cada parte confie na outra parte para cumprir suas obrigações, os contratos inteligentes eliminam a necessidade desse tipo de confiança entre os participantes (CAPGEMINI CONSULTING, 2016). Isso se deve ao fato de que qualquer contrato inteligente executará seu código de programa automaticamente e sem discrição. Todos os contratos inteligentes são essencialmente baseados no princípio de "condições se-isso-então-aquilo", o que significa que, se determinados critérios forem atendidos, uma resposta automática será acionada pelo programa (Mattila 2016, 16). Sua tecnologia depende de lógica inteligível e inequívoca, bem como de informações completas e precisas para total operacionalidade. Isso não deixa espaço para interpretação, pois o programa é sempre executado exatamente como foi programado antecipadamente. Como os contratos inteligentes são armazenados - e finalmente processados - no blockchain, a intervenção humana não é mais necessária e até impossível após a fase de programação (SWAN, 2015).

Outro exemplo comum usado para demonstrar isso é uma máquina de venda automática simples. Semelhante a um código de programa, uma máquina de venda automática se comporta de forma algorítmica, o que significa que o mesmo conjunto de instruções será seguido todas as vezes em todos os casos (SWAN, 2015). Assim que alguém deposita dinheiro na máquina e faz uma seleção, o item é entregue. Desde que a máquina esteja funcionando corretamente, ela não tem a capacidade nem a possibilidade de não cumprir as condições contratuais. Da mesma forma, um contrato inteligente é vinculado por seu design binário para executar o código pré especificado. Portanto, o código do programa define os direitos e obrigações decorrentes do contrato ao invés da legislação contemporânea (SWAN, 2015).

2.2.4 Gerenciamento de ativos por meio de contratos inteligentes

Outra característica importante dos contratos inteligentes modernos é sua capacidade de enviar, receber e transferir ativos para outras partes que participam do contrato (CHRISTIDIS; DEVETSIKIOTIS, 2016). Isso significa que os contratos inteligentes têm a capacidade de receber não apenas informações, mas também ativos como parte das transações e ainda manter e gerenciar os respectivos ativos no sentido de um administrador de acordo com os termos do contrato e suas condições predefinidas. Nesse contexto, Swan (2015) identifica três elementos distintivos dos contratos inteligentes: autonomia, autossuficiência e descentralização. Autonomia descreve a falta de necessidade de monitorar o contrato depois de acordado e lançado. Os agentes participantes não precisam agir manualmente. Qualquer ativo que possa ser digitalizado ou representado em formato digital (por exemplo, através de um certificado de propriedade) será transferido automaticamente.

Além disso, os contratos inteligentes são autossuficientes em sua capacidade de gerenciar recursos. Isso inclui, por exemplo, levantar capital através da emissão de capital e gastar esse capital em recursos necessários, como armazenamento ou poder de processamento. Por fim, os contratos inteligentes são descentralizados, pois são baseados na tecnologia blockchain e não precisam de um intermediário para a transação.

2.2.5 Inscrição Interface Binária (ABI)

Mesmo que um contrato esteja localizado na Ethereum blockchain, de maneira padronizada, nem todas conseguem utilizar o bytecode no blockchain. Cada contrato possui um tipo de mecanismo que se chama despachante de contrato (conhecido tambémcomo seletor de função) que precisa ser informado sobre qual função é chamada por umcontrato ou por um usuário específico. Desse modo, quando o dispatcher (mensagens e análises on-chain para projetos web3) detecta isso, o bytecode apropriado é executado com sucesso. Isso acontece em especial quando as seções do bytecode estão ligadas ao hash da assinatura de uma função. Se esse dispatchernão existisse, não teria um sistema responsável por informar qual bytecode precisa ser executado, já que o hash de bytecode é unidirecional.

A Application Binary Interface (ABI) realiza traduções entre o bytecode e a vontade do usuário de criar funções em um nível decifrável por pessoas. Conforme um contrato é alterado para se tornar em bytecode, a assinatura conforme cada função (onde possui nome, alguns parâmetros entre outras coisas) bytecode de acordo com o corpo dafunção.

Essas funções possuem chamadas próprias para um contrato de usuário ou ainda possuem contratos localizados em formatos diversos, sendo um deles o Javascript Object Notation (JSON) conhecido como Calldata. Sobre o valor hexadecimal que faz parte da calldata se inicia com o hash keccak-256 de 4 bytes da assinatura conforme essa função. Quando há uma chamada de função para um determinado contrato, o bytecode é estabelecido e executado de forma derivada combinando com o bytecode onde há o endereço de 4 bytes conforme é usado o despachante de contrato. Seja qual for os bytes no calldata depois desse valor de 4 bytes é demonstrado parâmetros conforme a função esão representados de acordo com os 32 bytes (que são preenchidos caso seja preciso).

Ao possuir a ABI, é possível interagir com um contato colocado como qualquer biblioteca que seja capaz (como, por exemplo, a Web3) ou site (como, por exemplo, o remix ethereum.org) é possível converter sem muitas dificuldades a função pretendida em seu equivalente de 4 bytes independentemente do parâmetro utilizado podendo aindachamar a função relevante conforme a seção de bytecode implantada.

2.2.6 Segurança de Contratos Inteligentes, Perdas Históricas

Os contratos conseguem dar um tipo de suporte para as transações financeiras em diversos casos de uso, porém é preciso questionar se vale mesmo a pena e se são de fato seguros, podendo ou não possuir alguma confusão na segurança. Diante de uma quantidade pequena de pesquisa, é possível observar que há muitos problemas documentados por conta de contratos inteligentes.

Primeiramente, os contratos inteligentes costumam ser programados no Solidity. Esse é uma dificuldade que deve ser considerada, já que a Solidity é uma linguagem

conhecida como sendo insegura e que seu padrão não dá uma segurança necessária caso haja falhas na programação, como no caso de estouros de números inteiros ou ainda haja estouros contra os quais outras linguagens podem preservar. Fato é que há artigos e pesquisas completas que visam o estudo sobre formas pelas quais os contratos possam se basear em Solidity podendo ser vulneráveis.

Os criadores de contratos inteligentes precisam adicionar de maneira intencional códigos que permitam aproveitar as construções linguísticas inseguras do Solidity. Um bom exemplo para se usar, são os desenvolvedores poderem escrever diversas funções que garantam que o desenvolvedor tenha todo controle sobre os fundos que os usuários colocam em um contrato, embolsando-os na hora que eles escolhem. Alguns desenvolvedores podem cometer alguns erros (erros esses que podem não ser reconhecidos pelos compiladores Solidity) que também conseguem reproduzir construções inseguras de linguagens.

Em segundo lugar, algumas partes mal-intencionadas de diversos tamanhos acabam procurando contratos que tenham erros em sua própria programação e assim explorar suas vulnerabilidades para extrair ETH desses contratos. O acesso costuma ser irrestrito quando há um invasor que sabe os primeiros 4 bytes do keccak256-hash de alguma assinatura que tenha uma função vulnerável e o método seja público. Essas vulnerabilidades são fáceis o bastante para serem exploradas por bots, já outras são maisdifíceis e necessitam de mais análises para serem exploradas.

Há diversos casos muito bem documentos de vulnerabilidades de fontes. Um bom exemplo que pode demonstrar o quão grave essa situação é quando o assunto é um contrato, esse exemplo é o contrato conhecido como contrato Fairwin. Alguns pesquisadores descobriram vulnerabilidades no quesito segurança quando o assunto é contrato de jogos que antes já possuíam cerca de US$ 10,5 milhões em fundos e que hojeem dia possuem US$ 0, ou seja, o prejuízo foi enorme. Uma dessas vulnerabilidades, sendo talvez a mais preocupante, fez com que o proprietário do contrato drenasse de forma completa todos os fundos do contrato (o que demonstra que sem dúvida há diversosproblemas envolvendo a segurança) sendo algo que faz com que muitos pensassem que esse contrato de Esquema Ponzi não é uma boa.

Como não existe um seguro FDIC ou ainda instituições para segurar membros de contratos inseguros, sendo a única opção, podendo ser vista como um tipo de esperança para os investidores, que optaram em tirar seus dinheiros. Possivelmente, a grande maioria dos investidores sacaram seus dinheiros, porém, se os especialistas não tivessem avisado, diversas pessoas teriam perdido todos os seus fundos.

Outro exemplo que pode ser dado foi o contrato DAO, esse tipo de contrato possuía cerca de US$ 150 milhões e foi de forma parcial drenado de fundos ao explorar o que é conhecido de bug de reentrada. Isso causou a perda de milhões. Diante de um movimento incomum que possuem por conta de uma tecnologia que é descentralizada e que não muda, a comunidade Ethereum quis alterar para um bloco anterior antes que a exploração acontecesse, principalmente desfazendo a exploração e substituindo o códigovulnerável. Isso, porém, não significa que é uma característica do Ethereum Blockchain e pode nunca ocorrer.

2.2.6 Uma Pesquisa da Segurança do Ethereum Blockchain

Essa quase perda e o contrato Fairwin são essenciais, isso porque eles demonstramas consequências graves que essas vulnerabilidades causam para os usuários da comunidade.

Milhões de dólares podem ter sido desviados de contratos que eram visivelmente inseguros de forma intencional ou ainda por terem erros não intencionais, tantouma pesquisa como um sistema que verifique a solidez dos contratos, pode ajudar na melhoria e segurança do Ethereum.

Esse exame garante não somente dar uma perspectiva sobre o quão ruim é a situação atual, porém, pode demonstrar as áreas e lugares que os principais especialistas em segurança necessitam focar para ajudar a melhoras ainda mais a segurança do Ethereum. Os resultados podem ser divulgados publicamente, assim, desenvolvedores e usuários necessitam aproveitar essas informações. Essa tese estabelece que a criação de um registro que possua endereços de contratos inseguros ajudaria o ecossistema, ajudando também os desenvolvedores a ficarem cientes dos códigos escritos de maneira errada, cooperando ainda os usuários a não adquirirem contratos inseguros.

Possuir registros dá diversos benefícios para os usuários e desenvolvedores. Os usuários de contratos pesquisam registros prévios antes de utilizarem um contrato. Isso, em tese, diminui o número de investimentos em contratos que não possuem segurança alguma. Para os contratos de hoje em dia, os usuários precisam sacar seus fundos se souberem que um contrato não possui a segurança necessária, evitando assim, que ocorravulnerabilidade.

Os desenvolvedores necessitam decidir reimplantar contratos que tenham bugs, sendo descobertos em seu código e avisar os usuários sobre seus contratos demonstrandoque foi visto uma vulnerabilidade que põe seu ETH em risco para que elas consigam retirar seja qual for o investimento. Caso haja um desenvolvedor que programasse uma maneira de autodestruição, ele provavelmente conseguiria tirar esse bytecode de forma completa da rede, assim nunca mais poderia ser utilizado.

Alguns usuários e desenvolvedores podem não saber de funções de execução simbólica, nem sobre ferramentas de análise estatística e dinâmicas que possam demonstrar vulnerabilidades em contratos inteligentes, por isso, é preciso observar e entender sobre o assunto. Ao conceder um projeto de pesquisa, como o presente trabalho,que pesquise as mais indicadas ferramentas demonstrando assim opções de execução de endereços de contrato no Ethereum, dá aos usuários e também aos desenvolvedores, informações essenciais sobre a segurança dos contratos sem que haja a necessidade de saber sobre alguma lista de analisados simbólicos. Além disso, essas opções de ferramentas necessitam de uma análise mais aprofundada cuidando da documentação e conhecimento de programação de fundo que pode ser um problema de entrada para certaspessoas.

Para conseguir resultados de pesquisa é necessário saber que deverá investir dinheiro e tempo. Possuir um único esforço para usar a varredura e análise de diversas linhas de saída baseadas a diversos contrato é algo benéfico, já que a pessoa economizariauma quantidade considerável de tempo para usar o registro. Sobre os custos de eletricidade, é possível observar que são muito elevados, principalmente quando se considera o esforço colocado para avaliar a segurança de diversos contratos. Ao compartilhar os resultados da análise é possível também perceber que diversas pessoas são favorecidas, já que uma quantidade bem menor de poder computacional é desperdiçada.

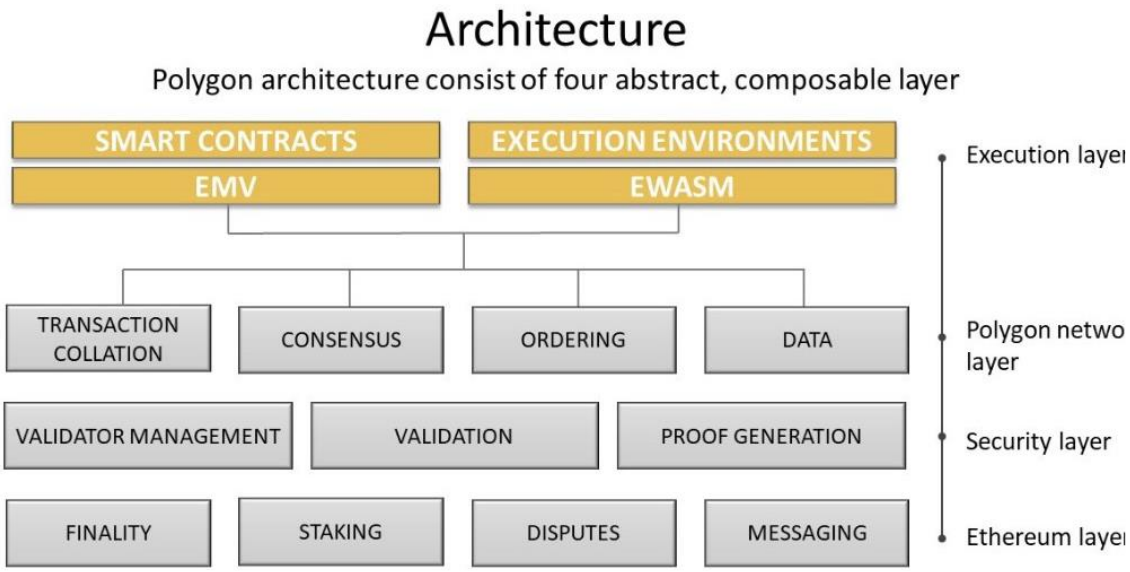
2.2.7 Rede Polygon

A rede da Polygon visa sanar alguns pontos negativos da rede Ethereum. Ela é uma segunda camada da rede Ethereum (vide camadas na Figura 2) e permite que operações sejam executadas com maior escalabilidade e taxas menores. Os contratos inteligentes

construídos na rede Ethereum são compatíveis com a Polygon, sendo que existem as seguintes vantagens em se utilizar a rede Polygon (POLYGON):

- Compatibilidade total com a rede Ethereum
- Escalabilidade
- Tecnologia customizável
- Adoção do modelo de "segurança como serviço"
- Interoperabilidade com outras redes (é possível transferir tokens da Polygon para outras redes e vice-versa por meio de pontes)

Figura 2: Camadas da interação entre as redes Ethereum e Polygon



Fonte: Polygon

2.3 TOKENS NÃO FUNGÍVEIS

ERC significa Ethereum Request for Comments e são padrões técnicos para tokens baseados em Ethereum, disponíveis online como EIPs - Ethereum Improvement Proposals. Os EIPs incluem o que é conhecido como especificações de protocolo principais, que abrangem aquelas que foram implementadas e lançadas, ou aquelas planejadas para serem assim, juntamente com APIs de clientes e padrões de contrato (MA et al., 2022).

Os ERCs compreendem padrões e convenções de nível de aplicativo para Ethereum, incluindo, mas não restrito a contratos inteligentes e padrões de token. E, enquanto o ERC-20 especifica a interface de token padrão, fornecendo uma implementação de modelo para uma API de token de contrato inteligente, o ERC-721 o faz para tokens não fungíveis. Existem dois padrões principais para tokens: ERC-20 para tokens fungíveis (FTs), e ERC-721 para tokens não fungíveis (NFTs). Os FTs representam diferentes quantidades de ativos idênticos (fungíveis) e são muitas vezes empregados para a implementação de criptomoedas em cima do Ethereum. Os NFTs, por sua vez, podem representar a propriedade de vários tipos de ativos distintos, por exemplo, propriedades físicas, como casas ou obras de arte exclusivas, ou colecionáveis, como animais de estimação virtuais ou cartões de jogo (MA et al., 2022).

Atualmente existem diversos padrões de contratos inteligentes, referentes a criação de tokens fungíveis e tokens não-fungíveis (cujo acrônimo em inglês é NFT). O primeiro tipo conta com os padrõesERC20, ERC 777 e ERC1155. Já o segundo tipo conta com o padrão ERC721. Uma vezque este trabalho focará na criação de tokens não fungíveis, o padrão ERC721 será abordado em mais profundidade nesta seção e utilizado no desenvolvimento da aplicaçãodesta dissertação (OPEN ZEPPELING).

O padrão ERC721 é consideravelmente mais complexo do que o padrão anterior ERC20 e possui um conjunto de extensões opcionais. Uma das extensões deste padrão permite o armazenamento de um metadado por token, o que faz de cada token único. No mercado, os modelos fornecidos gratuitamente pela Open Zeppelin têm sido muito utilizados e serão utilizados também neste trabalho (OPEN ZEPPELING).

O padrão ERC-721 fornece funcionalidade básica para rastreamento e transferência de NFTs em sua API de contrato inteligente, levando em consideração não apenas quando os tokens são transacionados por seus proprietários individuais, como também por terceiros consignados. Esses mediadores autorizados podem ser corretores, carteiras ou leiloeiros, e são conhecidos como operadores nesse contexto. Ele também permite que esses aplicativos de corretor/carteira/leilão funcionem com qualquer NFT no Ethereum, fornecendo contratos inteligentes simples e aqueles que rastreiam um grande número de NFTs (OPEN ZEPPELING).

2.4 RECEITUÁRIO MÉDICO DIGITAL NO BRASIL E NO SUS

No Brasil quando falamos sobre receituário médico e SUS podemos citar a telemedicina, que foi aprovada em caráter excepcional e temporário durante a crise causada pelo novo Corona vírus, pela Lei Federal n º 13.989/2020 e pela Portaria GM/MSn º 467 /2020. Com ela veio à tona elementos referentes às prescrições digitais que em termos gerais só são aceitas em farmácias quando atendem determinados requisitos que são: Receituários comuns, que contenham antimicrobianos; receituários de controleespecial (RCE) conforme preconizado pela portaria SVS/MS n 344/1998 (Exemplo de medicamentos: nitazoxanida, citalopram, cloroquina, fluoxetina, haloperidol, hidroxicloroquina, entre outros). No portal do ministério da saúde podemos verificar (MINISTÉRIO DA SAÚDE):

> Os atestados ou as receitas poderão ser aceitas em meio digital como smartphones, tablets, e-mail, plataformas de consulta virtual, WhatsApp, entre outros. A emissão difere do receituário habitual (papel, carimbo e assinatura física), por isso algunsrequisitos precisam ser seguidos para haver um conjunto mínimode informações que permitam a rastreabilidade e assim maior segurança para os profissionais que realizam a prescrição e a dispensa. De acordo com a Portaria nº 467, de 20 de março, a emissão de receitas e atestados médicos a distância será válida emmeio eletrônico mediante: uso de assinatura eletrônica, por meiode certificados e chaves emitidos pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil; uso de dados associados à assinatura do médico de tal modo que qualquer modificação posterior possa ser detectável; ou uso da identificação do médico,incluindo nome e CRM, além dos dados do paciente.

Uma recente iniciativa do conselho geral de farmácias no Brasil, trouxe à tona o sistema, denominado GIT - Farmácia Digital, que foi apresentado ao DataSus com a ideia inicial de realizar a integração entre sistemas e a unificação estabelecendo um canal permanente e ativo de interlocução com a sociedade para que as inovações tecnológicas

possam ser incorporadas aos trabalhos farmacêuticos em benefício de toda a sociedade. Ainda se tem como objetivo agregar informações recebidas da ANVISA (sistemas DATAVISA e SAMMED) e SIASG (Sistema Integrado de Administração de Serviços Gerais), além de manter uma coleção de códigos de barras (formato EAN-13) e dados, no formato Data Matrix, sendo concebida com caráter de dados abertos, permitindo o consumo por qualquer sistema.

Foi proposto ainda nesta iniciativa, termos de arquitetura de uma solução nacionalque permita a troca de informações (interoperabilidade) entre diversos sistemas existentesno mercado, com rastreabilidade de todo o processo, que envolva o trabalho dos farmacêuticos e demais profissionais de saúde, assim como das prescrições eletrônicas, sendo registrado num ambiente imutável de Blockchain.

Outra iniciativa, implementada no SUS, é o Conecte SUS, na qual o paciente pode acompanhar todos os agendamentos, consultas realizadas, histórico de medicação e histórico de exames (GOVERNO DO BRASIL). Contudo, este sistema permite apenas a visualização das informações por parte do paciente e do médico para acompanhamento do histórico. Esta ferramenta implementada pelo SUS não auxilia na melhoria do controlede receitas de medicamentos controlados nem garante a privacidade e confidencialidadedas informações para o paciente, uma das principais contribuições desta proposta.

2.5 OPENEHR

OpenEHR é um padrão aberto mantido pela OpenEHR Foundation, que se esforça para converter dados de saúde de um formato físico para um formato eletrônico e garantea interoperabilidade universal entre dados eletrônicos em todas as formas. O openEHR divide os modelos em dois níveis (modelagem em dois níveis): o modelo de arquétipo (AM) e o modelo de referência (RM). Possibilita a interoperabilidade semântica e o compartilhamento de dados dos EHRs, o que diferencia a representação das instâncias de dados do conhecimento do domínio. A abordagem openEHR é uma modelagem de fonteúnica de vários níveis dentro de uma estrutura de software orientada a serviços. É uma abordagem promissora para facilitar a interoperação de sistemas EHR, que se baseia no fato de que um conjunto de dados EHR completo pode ser totalmente representado usando arquétipos compartilháveis (PAHL et al., 2015; OPENEHR).

A abordagem openEHR tem três pilares principais: RM, AM e terminologia. O RM é um modelo de informação estável e formal que se concentra nas estruturas lógicasde um EHR e define as estruturas e atributos básicos necessários para expressar instânciasde dados EHR, incluindo tipos de dados, estruturas de dados e componentes de um EHR.O AM consiste em arquétipos e modelos. Arquétipos são os artefatos formais e semânticos que facilitam a coleta, armazenamento, recuperação, representação, comunicação e análise de dados clínicos, que podem ser modelados por profissionais clínicos e especialistas em informática em saúde por meio da restrição de RM. Enquanto isso, cada arquétipo é projetado para reutilização; em outras palavras, deve ser acordadoe compartilhado para contribuir para a interoperabilidade semântica entre os diferentes sistemas EHR. Um arquétipo deve representar o conjunto máximo de dados de um conceito de domínio. Os tipos de arquétipos são listados a seguir:

Demográfico: define conceitos genéricos de informação demográfica; inclui PARTY, ROLE e classes detalhadas relevantes.

- Composição: a estrutura de nível superior e “contêiner de dados” contendo arquétipos de seção e arquétipos de entrada, e é considerado equivalente como documento clínico.
- Seção: uma estrutura de navegação que facilita o acesso humano, semelhante ao índice de um documento. Um arquétipo de seção pode conter arquétipos de seção e arquétipos de entrada.
- Entry: define as estruturas genéricas para representação de enunciados clínicos, que possui cinco descendentes da seguinte forma:
    - Observação: representa as observações que ocorreram ao pacienteno passado, incluindo observações clínicas, exames, exames laboratoriais e situações do paciente.
    - Instrução: representa as intervenções a serem realizadas no futuro,por exemplo, prescrição de medicamentos.
    - Ação: representa o que foi executado, por exemplo, a inserção de uma cânula intravenosa.
    - Admin_Entry: usado para capturar informações administrativas, como admissão, compromissos, alta, cobrança e informações de seguro
    - Cluster: representa conteúdo clínico reutilizável que pode ser incorporado em arquétipos de entrada ou outros arquétipos de cluster.
    - Elemento: representa um único item a ser reutilizado em arquétiposde entrada ou arquétipos de cluster.

Um modelo openEHR monta e restringe arquétipos para fins específicos de contexto, que são mais próximos dos usuários e normalmente usados para gerar interfaces de programação de aplicativos (APIs), definições de esquema XML (XSDs), formulários de interface do usuário, esquemas de armazenamento, etc.

OpenEHR é uma abordagem terminológica neutra, que permite referir-se a terminologias externas em arquétipos, como SNOMED CT, ICD, LOINC e assim por diante. O arquétipo desempenha um papel importante na abordagem openEHR, que não apenas suporta a representação da semântica, mas também facilita a manutenção, a escalabilidade e a interoperabilidade e a entrada dos profissionais clínicos (ATAHG et al., 2014; GORDE et al., 2007).

A abordagem openEHR adota o método de modelagem multinível que divide claramente a responsabilidade, ou seja, os técnicos respondem pela codificação dosoftware com RM, e a semântica da informação é definida pelos especialistas do domínio.Como a abordagem openEHR é orientada por arquétipos, a estrutura de armazenamento de dados e a interface do usuário podem ser geradas por arquétipos e modelos. Os arquétipos são computáveis, o que significa que podem ser gerados e reutilizados de forma automatizada. Como resultado, os especialistas do domínio podem participar do desenvolvimento de sistemas por meio da definição de arquétipos e da vinculação de terminologia apropriada. Por outro lado, devido à separação de arquétipos e RM, os engenheiros só precisam se concentrar no desenvolvimento de software ou sistemas baseados no RM sem considerar em qual conhecimento clínico estará envolvido (LEZCANO, 2011).

3 TRABALHOS RELACIONADOS

Este capítulo apresenta uma revisão de outros estudos presentes na literatura que possuem alguma similaridade com o trabalho aqui proposto, por envolverem blockchain aplicada à prontuário médico do paciente e em alguns casos a prescrição de receituário médico. A pesquisa e seleção dos trabalhos mais pertinentes foram feitas utilizando as ferramentas Google Scholar, IEEE e ACM e foram considerados somente trabalhos publicados a partir de 2016. Para filtragem dos resultados foram utilizados os termos: “digital medical prescription”, “blockchain”, “electronic medical records”, “blockchain prescription medical”, e a partir dessa pesquisa, foram encontrados 9 artigos relevantes no que se refere às palavras-chave em questão. O objetivo principal deste capítulo é analisar os trabalhos relacionados à pesquisa atual e os comparar quanto aos aspectos utilizados no modelo apresentado.

2.4 ESTADO DA ARTE

O trabalho de Jiamsawat et al. (2021) aborda os registros EMR dos pacientes e a preocupação que se tem com a falta de segurança da integridade dos dados manipulados onde os pacientes gostariam de estar no centro de todo o processo de troca de informações entre entidades médicas e obter controle sobre seus dados e outras decisões médicas e farmacêuticas. Desta forma é proposto um sistema baseado em blockchain privativa com uma chave hash através de um sistema P2P de ponta a ponta, onde se tem comprovaçõesde hora e data e não permitindo manipulações nos dados inseridos.

O resultado obtido foi uma transmissão em contrato inteligente de 8 nós / pares que se revelaram precisos e livres de erros em todos os nós. Cada par pode atuar tanto como servidor quanto como cliente tendo assim a possibilidade de uma solução de computador confiável para gerenciamento de EMR de enfermaria de emergência hospitalar. Ademais, o autor Jamilet al. (2019) busca a resolução de uma problemática na falsificação de medicamentos, que acarreta graves efeitos colaterais no uso. Envolvendotodo o fluxo de um medicamento através de uma blockchain, ele propõe uma cadeia de processos desde a consulta médica, a prescrição da receita, a retirada do medicamento e o histórico de uso.

Ele afirma que, atualmente, na farmacologia, um dos problemas mais sérios são os medicamentos falsificados. A organização Health Research Funding relatou que, nos países em desenvolvimento, entre 10 a 30% dos medicamentos são falsos. A falsificaçãonão é o principal problema em si, mas, sim, o fato de que, em comparação com os medicamentos tradicionais, esses medicamentos falsificados produzem diferentes efeitoscolaterais para a saúde humana. De acordo com a OMS, cerca de 30% do total de medicamentos vendidos na África, Ásia e América Latina são falsificados.

Ainda enfatiza a relação de falta de segurança em uma receita feita em papel, mesmo que com carimbo e assinada, pois é de fácil falsificação. “Como o fator saúde é uma preocupação principal para todos, muitas organizações de saúde enfatizam a rastreabilidade de medicamentos para evitar a falsificação de medicamentos usando a mais recente tecnologia de TI (ou seja, Blockchain).

Então utilizando uma plataforma open source chamada HyperLedger Fabric junto com uma blockchain privada em um hospital inteligente ele mostra como é possível compartilhar e controlar todas as informações de entrega de medicamentos entre variados departamentos em um hospital, garantindo assim um registro íntegro e seguro.

Além disso, o trabalho dos autores Li e Zhang (2020), traz a problemática da faltade segurança e de privacidade dos dados de pacientes através dos EMR propondo assim um Mecanismo de Proteção de Privacidade e Compartilhamento do EMR com Base no Blockchain de Consórcio Médico onde ele ambos se unem através de um nó e desta forma detém os dados que o EMR gera diretamente na Blockchain e obtém os acessos por estarem dentro deste nó. A cada solicitação de visualização deste EMR é necessária a autorização do paciente dentro da blockchain do consórcio médico.

Eles concluem o artigo tratando esta proposta com três vantagens principais: primeiro, o armazenamento distribuído melhora a capacidade anti-ataque; segundo,apenas os membros do blockchain do consórcio podem ler e gravar dados e enviar transações, aumentando a proteção da privacidade; terceiro, os mecanismos de controle de acesso podem ser implementados usando contratos inteligentes, reduzem custos e resolvem problemas de confiança. E a leitura e gravação de dados EMR devem ser autorizadas pelo paciente para obter a propriedade do paciente e o controle sobre seus próprios dados EMR;

Também tratando da falta de segurança nos registros eletrônicos, Ismail, Materwala e Khan (2020)**,** trazem em seu artigo, a problemática onde cada hospital possuio seu banco de dados e ali guarda seus dados, sofrendo com insegurança, privacidade, vulnerabilidade e espaço de armazenamento destas informações. Além disso, também trazcomo problema que os profissionais de saúde e os pacientes não conseguem ter uma visãounificada do histórico médico de um paciente de todos os centros de saúde visitados. Isso resulta em custos adicionais de tratamento, exames médicos repetidos e maior tempo parao diagnóstico. Desta forma ele propõe um sistema de BlockChain utilizando BlockHR um sistema de gerenciamento de registros de saúde centrado no paciente para atendimentomédico eficiente a um custo ideal.

Como conclusão, eles revelam que o sistema permite que os profissionais de saúde insiram os dados do prontuário médico dos pacientes na rede blockchain e permite que os pacientes insiram seus dados sociais, como hábitos de sono, atividades físicas e localização atual. Consequentemente, o BlockHR fornece suporte aos médicos para um melhor diagnóstico e prognóstico.

Ademais, o trabalho de Flores, Enteria e Pefianco (2020), propõe um banco de dados médico eletrônico para facilitar a interação do paciente com o enfermeiro. Ele é digitalizado para limitar o contato físico e uma interação amigável para dar comodidade e conforto aos enfermeiros e equipe médica durante o trabalho e, por último, exibe um resumo estatístico e uma apresentação gráfica para fins de pesquisa.

Novamente vemos um artigo falando sobre BlockHR mas neste os autores Ismaile Materwala (2020)**,** usaram essa ideia para propor um sistema de suporte médico para profissionais médicos para melhor prognóstico / diagnóstico e acompanhamento dos pacientes. O BlockHR incorpora ferramentas para que os pacientes carreguem dados médicos e de estilo de vida usados para prever o risco de desenvolver doenças crônicas.

Neste artigo, o autor Li (2020), traz à tona a fragilidade da prescrição médica em papel e as dificuldades em armazenar e tratar o seu sigilo, e em casos em que a mesma é perdida, traz transtornos desnecessários ao paciente. Mostra ainda que por mais que as

receitas digitais existam, tem muitas farmácias online por exemplo que não aceitam as digitais e pedem ao final de uma compra o envio da receita em papel escaneada. Então é proposto um sistema de prescrição médica baseado em blockchain e ao mesmo tempo, para proteger de forma eficaz a privacidade dos pacientes, utilizando o algoritmo k- anonymity.

Os resultados experimentais mostram que o método de anonimização de dados baseado em privacidade diferencial não só melhora a segurança dos dados, mas também garante efetivamente a disponibilidade dos dados.

Já o artigo produzido por Yfantis, Leligou e Ntalianis (2020), discute o conceito de Blockchain e sua aplicação à pesquisa em administração pública como uma ferramentapara aumentar a confiança no governo. A contribuição deste artigo é que ele desvenda as vantagens e desvantagens do Blockchain para que tanto os tomadores de decisão (que pretendem adotar esta tecnologia inovadora para aumentar a transparência das transaçõesno setor público) quanto os usuários (cidadãos e servidores públicos) sejam bem- informados e preparados.

Ademais, o interessante no artigo de Dumpeti e Kavuri (2021) é que, por mais queele trate exclusivamente na proposta de uma estrutura para gerenciar certificados e evitara falsificação, o autor propõe o uso de uma Blockchain em conjunto com uma estrutura de Hyperledger com integração IoT para gerenciar as permissões de acesso. O modelo proposto demonstra o uso de Blockchain para desenvolver uma aplicação distribuída e fornece uma maneira fácil de gerar, emitir, manter e verificar os certificados. É um mecanismo à prova de violação para gerenciar certificados digitais. A base do aplicativoestá na geração de hashes e assinaturas digitais, utilizando-os para evitar a manipulação de dados. É um sistema eficiente em termos de velocidade de transação, autenticação, facilidade de uso e nível mais preciso de permissões de acesso.

Azaria et. Al (2016) desenvolveram um sistema chamado MedRec para resolver o problema de interoperabilidade de dados e gerenciamento de direitos para o gerenciamento de registros médicos. A MedRec propõe três tipos de contratos inteligentes, a saber, contratos de registro, contratos de relacionamento médico-pacientee contratos sumários para realizar o gerenciamento de autoridade de dados. O contrato deregistro é utilizado para gerenciar a tabela de informações do usuário, e a chave pública é utilizada como sua identidade para realizar o login anônimo do paciente; o contrato derelação médico-paciente define uma série de indicadores e respectivos direitos de acesso,por meio dos quais são acessados os dados do banco de dados, que é utilizado por um médico para um médico. O contrato resumido é usado para gerenciar todas as coletas dedados de informações médicas geradas pelos pacientes.

3.1 DISCUSSÃO

A Tabela 1 mostra um resumo dos trabalhos relacionados pesquisados, resumo este que relaciona as estratégias de implementação de sistemas seguros relacionados ao gerenciamento de informações sobre prontuário médicos e controle de medicação controlada.

A Tabela 1 apresenta uma comparação entre os principais trabalhos no estado-da-arte e o modelo que irá ser proposto. É perceptível nestes trabalhos acima relacionados ao uso

da Blockchain como base para maior segurança e controle da privacidade dos dados médicos, com alguns utilizando as tecnologias EHR, EMR ou PHR para controle dos dados do paciente. Além disso, é possível observar que muitos trabalhos recentes trabalham com criptografia e auxiliam no controle de medicamentos controlados.

Tabela 1 – Tabela Comparativa

	Controla o receituário médico	Formato do Prontuário Eletrônico	Arquitetura de Armazenamento	Mecanismo de Criptografia	Gerenciamento de Substâncias Controladas
Zaworski e Szpyrka (2021)	Não	PHR	Bitcoin	Chave pública da instituição médica	Nada específico
Jamil et al. (2019)	Sim	Não informa	Blockchain Hyperledger	Hash e Assinatura Digital	Armazena histórico de medicamentos do paciente
Li e Zhang (2020)	Sim	EDR (*Eletronic Drug Record*)	Hyperledger Fabric	Não menciona	Gerenciamento e atualizações da cadeia logística do medicamento.
Ismail , Materwala e Khan (2020) e Ismail e Materwala (2020)	Sim	Armazenamento em nuvem.	Arquitetura do BlockHR, baseada em arquitetura cliente/servidor e blockchain.	Função Hash	Armazena histórico de medicamentos administrados para o paciente
Flores et al. (2020)	Sim	EDR	Bitcoin	Não mencionado	Possibilita a visualização de todo o histórico médico do paciente.
Li (2020)	Sim	PHR	N/A	k-anonymity	Sistema de receitas médicas com garantia de anonimato e privacidade.
Yfantis, Leligou e Ntalianis (2020)	Não	N/A	Blockchain de forma geral	N/A	N/A
Dumpeti (2021)	Não	N/A	Framework próprio baseado em Blockchain	Função Hash	N/A
Proposta	Sim	PHR	Modelo de contrato inteligente para criação de NFTs da OpenZepelling	Chaves públicas e privadas com certificados x.509	Sim. A receita deverá ser assinada digitalmente pelo médico e a cada receita será atribuído um código único que poderá ser validade pela farmácia.

Fonte: o autor

O diferencial do presente artigo em relação às referências citadas, é o formato utilizado na construção dos processos relativos ao receituário digital. Com uso dablockchain e de chaves públicas e privadas, o processo que se utilizará deste sistema possibilitará *(i)* segurança contra compra irregular de medicamentos, *(ii)* privacidade paraos pacientes e *(iii)* controle mais robusto de medicação controlada por parte das agênciassanitárias, que poderão

verificar a comercialização destes medicamentos em tempo real e terão dados mais confiáveis e precisos, devido a contabilização eletrônica não contar coma possibilidade de erros manuais.

Os trabalhos apresentados na Tabela 1 variam para cada proposta. As diferentes propostas adotaram decisões diferentes quanto ao formato de prontuário adotado, criptografia utilizada, framework utilizado na implementação e estratégia utilizada na emissão de receitas médicas (quando adotada estratégia neste sentido). Nenhum destes trabalhos teve como foco a emissão de receitas médicas e por conta disso eles abordaram parcialmente os pontos que serão considerados neste trabalho, cuja contribuição é fazer um estudo amplo sobre como implementar um sistema a ser utilizado no processo de emissão da receita médica e utilização desta receita na compra de medicamento.

Em Zaworski e Szpyrka (2021) não é apresentado nada de específico a respeito da implementação de receituários, contudo o trabalho apresenta um estudo sobre as possibilidades do uso de blockchain em relação ao acesso dos pacientes as suas informações médicas. No trabalho de Jamil et al. (2019) foi feita a implementação de umafuncionalidade que visa gerenciar o histórico de medicamentos administrados aos pacientes. O trabalho de Li e Zhang (2020) apresenta uma forma de se gerenciar a cadeialogística dos medicamentos através de um sistema desenvolvido que tem como base a arquitetura do framework Hyperledger Fabric. No trabalho de Ismail, Materwala e Khan (2020) é feita a implementação de um sistema que armazena os dados médicos dos pacientes através do armazenamento em nuvem, utilizando a função Hash para criptografar os dados. O trabalho de Flores et al. (2020) apresentou um sistema capaz demostrar ao paciente todo o seu histórico médico, mas não apresenta uma solução para a criptografia a ser utilizada.

O trabalho de Li (2020) é o que mais se assemelha a este. Nele é apresentado um sistema de receituário médico com garantia de anonimato e privacidade através da criptografia feita com o k-anonymity. Contudo, neste trabalho não foi explorado todo o processo de expedição da receita e aceite da receita por parte da farmácia, sendo assim não foram solucionadas algumas questões chave sobre como seria mantida a privacidade e confidencialidade do paciente ao mesmo tempo que a *(i)* o médico irá prescrever os medicamentos, *(ii)* a farmácia irá receber a receita e validar esta receita junto a agência governamental e *(iii)* a agência governamental deverá auditar a compra e venda de medicamentos controlada.

É proposto um processo completo que poderá ser utilizado no mercadoe possibilitará a compra e venda de medicamentos controlada provendo maior segurançae possibilidade de auditoria mais consistente para as agências governamentais através dacriação de NFTs. Ao mesmo tempo, esta proposta visa garantir a privacidade do paciente. Ainda não há na literatura artigos acadêmicos que exploram especificamente esta tecnologia para receitas médicas digitas. Dada a relevância que esta tecnologia ocupou atualmente, é importante para a academia que esta tecnologia seja explorada.

4 MODELO PROPOSTO

No modelo proposto, há a construção de uma solução segura para gerenciar o ciclode distribuição de medicamentos, dentro de um controle profissional por sistema de acesso tecnológico. A arquitetura proposta tem como objetivo gerenciar os registros de receitas médicas, além de permitir o controle sobre a aquisição e consumo de medicamentos de uso controlado, mantendo a privacidade dos pacientes através da criação e uso de NFTs.

Considerando os objetivos propostos para o trabalho, definem-se os seguintes requisitos para a arquitetura:

- Garantia de autenticidade e rastreabilidade das receitas e permissões de aquisiçõesde medicamentos;
- Garantia de que permissões de compra serão reutilizadas sem autorização médica;
- Escalabilidade para atender ao sistema de saúde nacional sem causar atrasos em atendimentos médicos ou farmacêuticos.

Dados os requisitos elencados, vislumbra-se uma arquitetura composta pelos seguintes serviços:

- Serviço de identificação: capaz de identificar diferentes usuários e componentesdo sistema
- Serviço de políticas: políticas de acesso e de confiabilidades, a serem implementados através do conceito de chaves públicas e privadas;
- Serviço de blockchain: serviço de distribuição e armazenamento de livro de razãoe algoritmo de consenso;
- Serviço de contrato inteligente: registro de contrato inteligente e gerenciamentode seu ciclo de vida;
- Contrato para geração de NFTs que representam receitas médicas e também geração de NFTs que representam permissão de compra de medicamento restrito.

Além disso, será feito o modelo dos seguintes artefatos, os quais são projetados para serem integrados a implementação testada neste trabalho:

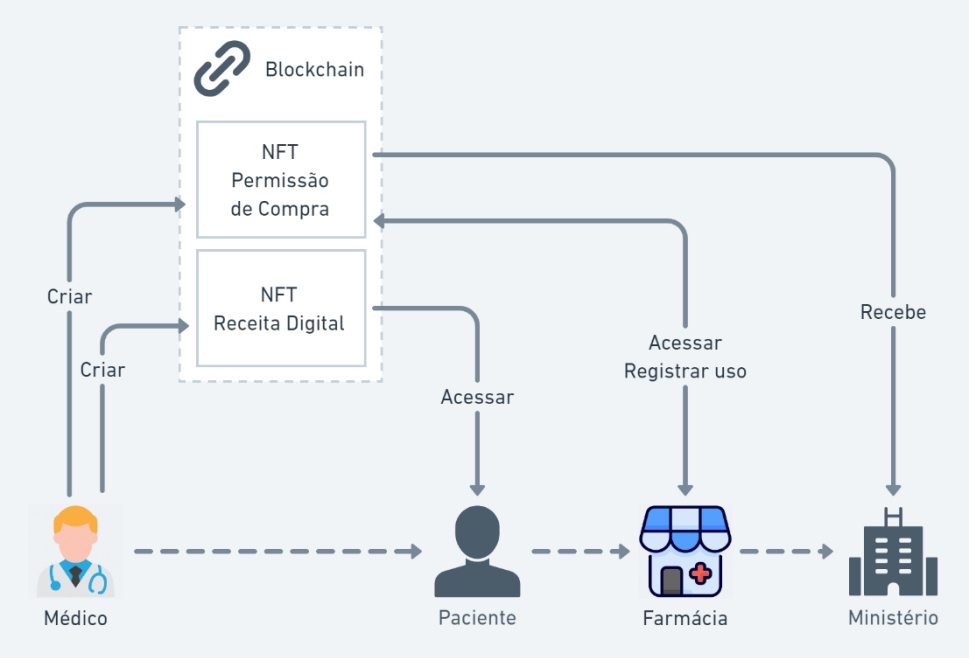
- Template em openEHR para integração do futuro sistema com outros sistemas que usam este padrão.
- Aplicação de criptografia para que dados confidenciais sejam acessados apenas pelo sistema do ministério da saúde.
- Sistema completo que poderá ser utilizado por profissionais de saúde, pacientes e médicos através de seus computadores e também através de dispositivos móveis em geral.

Os dados de saúde do paciente são convencionalmente armazenados em repositórios de profissionais de saúde. Frequentemente, entretanto, esses dados não são compartilhados entre os provedores ou com os pacientes. (ROEHRS, *et.a*l., 2019). O uso da blockchain como proposta viabiliza a maior acessibilidade e melhor informação de dados aos pacientes como um benefício para contenção de exames e armazenamento de histórico de saúde. Neste contexto, o presente capítulo apresenta os atores, artefatos, modelos de dados em processos da proposta em mais detalhes. São apresentadas as tecnologias a serem utilizadas para apresentar os elementos da arquitetura do sistema. Aarquitetura será descrita ao longo da seção, explorando quais os principais atores que

farão uso do sistema, quais os dados que serão utilizados, e quais os processos utilizados para o seu gerenciamento.

Figura 3 mostra a arquitetura do sistema. De forma geral, os passos para o uso do sistema (vide arquitetura na Figura 3) são os seguintes: *(i)* o módulo do sistema do médico poderá ser executado no sistema de informação do médico (que pode ser celular, tablete ou computador pessoal), *(ii)* o sistema do paciente pode ser um celular ou um tablete, *(iii)*o sistema da farmácia pode ser instalado no sistema de informação disponível da mesma também (computador pessoal, celular ou tablete), *(iv)* o sistema da agência governamental será instalado em um servidor e *(v)* o sistema Blockchain poderá ser instalado em um sistema distribuído de uma empresa privada ou do governo. Contratos inteligentes serão utilizados no cadastro de receita e no cadastro de uso das receitas, bem como na validação.

Figura 3: Arquitetura do sistema



Fonte: o autor

4.1 ATORES

Existem três atores principais que irão interagir com a arquitetura proposta, ao longo do processo, sendo estes: médicos, pacientes e farmácias. Os médicos interagem com o sistema para criar a receita digital que será registrada na blockchain e com indicativos específicos para cada paciente, com praticidade para analisar antigos examese propor novos modelos de tratamento, inclusive ao prescrever novos medicamentos. Ospacientes fornecem sua carteira na blockchain para o médico, o que possibilita o médicode enviar a permissão de compra (representada pela NFT criada). O paciente poderá utilizar a NFT na farmácia ao fazer o login no sistema da mesma e transferindo a NFT

para a carteira desta farmácia. O farmacêutico, ao receber a notificação de seu sistema deque a NFT é válida, poderá vender a medicação para o cliente.

O processo de cadastro da receita e das permissões de uso de medicamentos controlados na blockchain são transparentes para todos os atores envolvidos (médico, paciente e farmacêutico) já que ela será realizada através de uma interface que irá abstrairtais detalhes, proporcionando-lhe uma metodologia de trabalho mais confiável e adequada ao mesmo tempo que provem confidencialidade e privacidade para o paciente.

O uso da blockchain é transparente para o paciente, que pode visualizar suas receitas através de um sistema PHR (*Patient Health Record*), o qual é feito para ser acessado em qualquer lugar. O uso deste formato de prontuário permitirá que o pacienteveja todas as suas receitas e ao mesmo tempo trará privacidade ao mesmo, pois apenas com o uso de sua chave privada, os blocos do blockchain referente as receitas proferidasa ele poderão ser acessadas. Cada paciente possuirá assim um canal no Blockchain que permitirá a inserção de blocos por médicos e farmacêuticos através do uso da chave pública deste paciente. O paciente poderá fazer a leitura destas informações e poderá prover o código da receita (que poderá ser um código de barras ou um QRCODE) para ofarmacêutico, que juntamente com os documentos de identificação do paciente poderá verificar a autenticidade do código junto a agência sanitária. Desta forma, o paciente provera apenas as informações que deseja para os outros atores do processo e terá a sua privacidade garantida, ao mesmo tempo que o sistema provera uma forma mais confiávelde emissão de receitas, com validação em tempo real dos procedimentos.

O farmacêutico pode acessar a receita especifica através do código contido no documento entregue pelo paciente; além disso, ele terá acesso aos medicamentos exatos que foram prescritos, incluindo as doses e quantidades necessárias ao tratamento. No atoda compra do medicamento, ele registrará a aquisição feita pelo paciente, de modo que medicamentos de uso controlado não poderão ser novamente adquiridos, aumentado a confiabilidade no controle de seu uso pela população.

A agência governamental visualizará as transações relativas à receita sem ter acesso às informações do paciente. Nas NFTs que representam as permissões de compra,serão registrados apenas o registro MS do medicamento e a quantidade de caixas do medicamento que poderão ser adquiridas através do NFT em questão. Estas agencias terãoum canal dentro dos blocos do blockchain, onde poderão visualizar as receitas e as compras de medicamentos feitos por cada uma das receitas. Além disso, são estas agencias que validação a receita para o farmacêutico, pois o médico irá registrar a receitautilizando também a chave pública da agência governamental. Para que a implementaçãoseja realizada de maneira satisfatória, um conjunto de artefatos de dados se faz necessário,os quais serão descritos logo abaixo.

4.2 ARTEFATOS

Tendo como objetivo habilitar o gerenciamento de receitas médicas através de uma estrutura de blockchain, verifica-se a necessidade de três elementos de dadosfundamentais a serem gerenciados no contexto da blockchain. Estes são: receitas médicas,permissões de uso, e recibos de uso. Primeiramente, uma receita médica é composta pelas seguintes informações (Apêndice A): *(i)* quais os medicamentos em vigência e oselementos de dados contidos nele e *(ii)* frequência de uso do medicamento; informações do médico responsável e o CID da doença. Além disso, para o caso de medicamentos controlados com uso recorrente, tem-se o uso das permissões de uso para validar e controlar a aquisição de tais substâncias. Essa validação é constituída com base na quantidade de uso por um período limitado, que deveria ser renovado de forma mensal pelo médico responsável para a obtenção de um novo receituário digital. Por sua vez, os recibos de compra têm como objetivo registrar o uso das permissões de compra para garantir o uso dos medicamentos conforme a prescrição. Tais permissões são emitidas pelo médico através da criação de NFT, feita por meio do contrato na blockchain, emitidopelo ministério da saúde.

Além disso, as transações feitas pelo médico, a compra e a venda dos medicamentos poderão ser auditadas pela agência sanitária. Todas as transações deverãoser registradas também se utilizando a chave pública da agência sanitária, sem que sejaminseridos os dados do paciente. Serão inseridos para a visualização da agência, dados da receita, do médico e da farmácia. Estas informações ficarão acessíveis para a agência sanitária.

Trata-se, de uma resolução verificada para o processo de gerenciamento farmacêutico (vide o processo apresentado nas sessões 4.4.1 e 4.4.2), que tem como foco fornecer orientações e normatizar processos para que eles sejam realizados dentro da lei e garantindo a autenticidade. Também sendo um meio de controlar a origem destes produtos tendo em vista que surgem implicações e outros tipos de barreiras como fraudes,falsificação de medicamentos, descontrole de uso, entre outros.

O sistema proposto integrará o médico, o paciente, a farmácia e a agência sanitária local através da tecnologia blockchain e as informações serão exibidas para o paciente através de uma interface amplamente acessível. Esta é uma contribuição significativa, pois o trabalho de Roehrs, *et. a*l. (2019, p. 2) apresenta uma barreira enfrentada por EHRe PHR é a distribuição e as limitações da integração de registros de saúde. Outras barreirasestão relacionadas a questões de segurança, como confidencialidade e privacidade dos registros de saúde.

Ademais, Jamil *et. al* (2019), abordam no seu artigo, uma problemática na falsificação de medicamentos, que acarreta graves efeitos colaterais no uso. Sendo assim,a partir do envolvimento do fluxo de um medicamento através de uma blockchain, ele propõe uma cadeia de processos desde a consulta médica, a prescrição da receita, a retirada do medicamento e o histórico de uso.

Como a saúde é uma preocupação em comum para a população, muitas organizações de saúde enfatizam a rastreabilidade de medicamentos para evitar a falsificação, usando a mais recente tecnologia de TI (ou seja, Blockchain), afirmam os autores (JAMIL et. al, 2019). Desse modo, funciona como uma alternativa de prontuárioeletrônico digital para o lançamento de dados da compra do medicamento e ainda evitar problemas como a falsificação de medicamentos. Os artefatos acima apresentados são

materializados na forma de um conjunto de modelos de dados, utilizados para persistênciae transmissão dos dados relativos às receitas médicas. Tais modelos são descritos a seguir.

4.3 MODELO DE DADOS

O sistema proposto criará a receita médica e permissões de compra de medicamentos restritos. A receita médica tem como objetivo auxiliar o paciente no momento de compra do medicamento e quando ele estiver administrando o medicamentoem sua casa. Além disso, a receita médica visa auxiliar o paciente a administrar o consumo do medicamento da maneira correta em sua casa.

O desempenho da Blockchain agrega em termos positivos ao paciente, de modo que haja benefícios *(i)* aos centros de saúde, *(ii)* médicos e profissionais responsáveis, *(iii)* aos pacientes e as agências de controle. A transparência e a segurança de dados são propostas pelo BlockHR com monitoramento de atividades centradas no paciente. (ISMAIL, MATERWALA e KHAN, 2020). De acordo com a visão de Ismail e Materwala (2020), a inserção do blockchain é válida para gerenciamento de registros de saúde (BlockHR), um sistema de suporte médico para profissionais médicos para melhor prognóstico e diagnóstico e acompanhamento dos pacientes. O BlockHR incorpora ferramentas para que os pacientes carreguem dados médicos e de estilo de vida usados para prever o risco de desenvolver doenças crônicas.

Dadas as razões discutidas, a presente proposta fará uso de uma blockchain como mecanismo de armazenamento e autenticação dos artefatos que serão utilizados para o gerenciamento das receitas. Do mesmo ponto de vista para aplicação prática dessa estrutura, os benefícios do registro eletrônico carregam consigo o controle como métododе prevenção na saúde dos pacientes. A partir dessa tecnologia, haveria índices de acompanhamento e informações precisas para estudos médicos presentes e futuros, a depender da função e necessidade considerados. A utilização do blockchain se aplicaria ao desenvolvimento da saúde pública com adicional de recursos para evitar problemas em falsificação e reuso, como no sistema convencional.

O sistema com permissões de compra baseadas em NFTs trará privacidade aos pacientes, uma vez que suas carteiras com endereço de redes de blockchains descentralizadas não as identificam, além disso apesar do sistema também armazenar as receitas nas contas das pessoas, os seus dados serão criptografados e não será possível para terceiros ou entidades terem acesso a informações das pessoas. Esse fato é exploradopor Li (2020), baseado na percepção de fragilidade da prescrição médica em papel e as dificuldades em armazenar e tratar o seu sigilo. Desse modo, nos casos em que a prescrição em papel é perdida, traz transtornos desnecessários ao paciente. No caso das NFTs, estas poderão ser utilizadas apenas uma vez e o registro das transferências das mesmas são armazenadas na Blockchain. Uma vez que os endereços da Blockchain não são vinculados a pessoas físicas.

Além disso, há a demonstração efetiva de que, por mais que algumas farmácias aceitem as demandas autorizadas por receitas digitais, muitas dessas empresas online não aceitam as prescrições digitais e ainda solicitam, ao final de uma compra, o envio da receita em papel. Neste trabalho é proposto um sistema baseado na tecnologia blockchain para implementar os processos de cadastro e utilização de receitas médicas. Através destesistema, a receita será totalmente digital e poderá ser enviada para a farmácia que ao conferir o contrato dela, terá a confirmação da sua autenticidade.

Ademais, chegamos à ideia de visibilidade do Blockchain como um instrumento acessível a todos e parte do Sistema Único de Saúde (SUS), presente no modelo proposto como um formato favorável à qualidade de atendimento e saúde pública no Brasil. Esse impacto revolucionário pode ser aferido a partir da proposta elaborada por Yfantis, Leligou e Ntalianis (2020), em discussão sobre seu conceito e adoção do métodotecnológico para os usuários de serviços públicos.

Tabela 2 - Campos obrigatórios em receitas de medicamentos controlados, conforme regulações da ANVISA:

Campo obrigatório em receitas de medicamento restrito
Sigla da unidade da federação
Identificação numérica fornecida pela autoridade sanitária competente dos estados, municípios e Distrito Federal
Identificação do profissional que está prescrevendo, com sua inscrição no conselho regional com a sigla da respectiva unidade da federação
Nome do medicamento, dosagem, forma farmacêutica, quantidade (em algarismos arábicos e por extenso) e posologia
Símbolo indicativo de riscos
Data de emissão
Assinatura do prescritor. Quando os dados do profissional estiverem devidamente impressos no campo do emitente, ele poderá apenas assinar a notificação de receita. Caso pertença a uma instituição hospitalar, o emitente deverá também utilizar seu carimbo, constando a inscrição no conselho regional
Identificação do paciente, com nome, documento de identificação, endereço e telefone
Identificação do fornecedor, com nome do estabelecimento, endereço, telefone, data e nome do responsável pela dispensação do medicamento
Identificação da gráfica que emitiu o receituário, com nome, endereço e CNPJ em cada folha do talonário. Deve constar também a numeração do início ao fim concedidas ao profissional ou instituição, com número da autorização para confecção de talonários emitida pela vigilância sanitária local
Identificação do registro, com anotação da quantidade aviada, no verso das folhas.

Código 1 - Registro de permissão para uso de medicamento, válido para uma unidade do mesmo

```
{
tipo: "permissao de uso de medicamento"
unidade_federacao: “SP”,
código_receita:[20,40,44,333,347],
codigo_permissao:[50,33,44,77,00,02,78,88]
{
nome_medicamento: “Rivotril”,
Registro MS: 1010000720162
}
```

Fonte: o autor

No que diz respeito às soluções propostas para gerenciamento e impedimento de

falsificação após a permissão de Blockchain, a proposta de Dumpeti e Kavuri (2021), promove a ideia de uso da Blockchain em conjunto com uma estrutura de Hyper Ledger e com integração IoT para gerenciar as permissões de acesso. A ordem da medicação emitida pelo médico do sistema deve seguir os padrões nacionais e internacionais. Um exemplo de ordem feito em OpenEHR é mostrado no Apêndice A.

Exemplo de padrão para prescrição eletrônica de medicamentos é mostrado no Apêndice A. O padrão apresentado permite que o médico especifique todos os detalhes de um medicamento e como o mesmo deve ser administrado ao paciente. Neste padrão, os requisitos obrigatórios para uma receita médica previstos pela ANVISA conforme resumido pela Tabela 2. Os campos obrigatórios previstos na tabela são previstos no exemplo do Apêndice A. Além disso, a permissão de compras pode ser definida em um sistema pelo arquivo JSON do código 1.

4.4 PROCESSOS

Os atores, artefatos, e formatos de dados estabelecidos nas seções anteriores atuamem conjunto para o gerenciamento de receitas através de uma blockchain utilizando dois processos principais. São estes: *(i)* o cadastro de uma receita médica e *(ii)* a aquisição de medicamentos. Estes processos estão dispostos no diagrama BPMN (acrônimo em inglês para *Business Process Modeling Notation*).

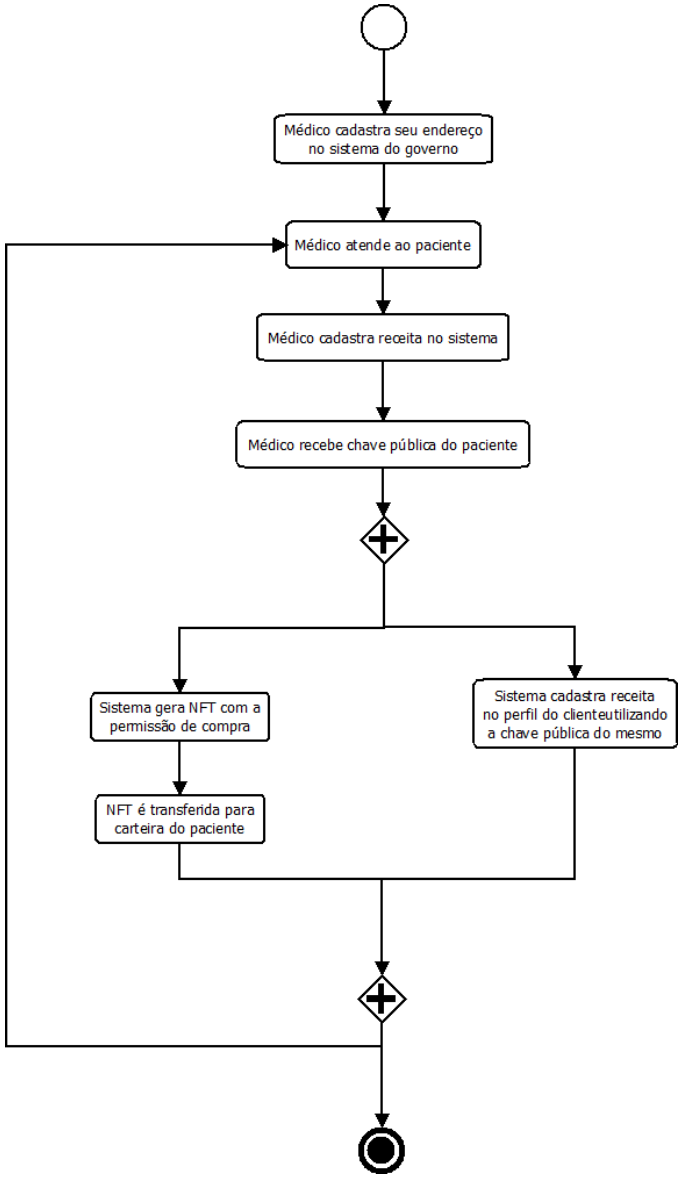
Nestes processos são feitas as emissões da permissão de compra (que é um NFT)e também da receita que será criptografada em um sistema e poderá ser acessada apenaspelo paciente.

4.4.1 Cadastro de receita médica

O cadastro da receita médica de medicamento se dá quando o paciente faz uma consulta a um médico e este médico conclui ser necessário que um medicamento deve ser ministrado devido ao diagnóstico realizado, ele é ilustrado na Figura 4 e o contrato que executa o cadastro da permissão de compra é apresentado no Apêndice B. Neste momento, o médico insere em seu sistema as informações necessárias, no caso de o medicamento ser controlado todas as informações da Tabela 2 serão exigidas para que a receita esteja de acordo com a legislação atual.

O processo de receitas para medicamentos restritos e não-restritos é o mesmo, a única diferença é que o médico deverá inserir todas as informações exigidas pelalegislação no caso de receitas com medicamento restrito, sendo que o sistema o alertará para isso quando o médico for inserir as informações. No caso da emissão da NFT, ilustrado na Figura 5, será necessário apenas a inserção do registro MS do medicamento e a quantidade do medicamento que o médico autoriza o paciente a adquirir. As demais informações já serão recuperáveis, uma vez que o endereço do médico que emitirá a NFTestará gravado na Blockchain e o mesmo deverá estar cadastrado no sistema da agência governamental. Apenas endereços cadastrados pela agência governamental poderãoemitir as receitas.

Figura 4: Processo em que o paciente adquire a receita junto ao médico. É importante observar que o processo é o mesmo para receitas para medicações restritas e não-restritas. A diferença será que o sistema exigirá que o médico insira todas as informações no caso de receitas com medicamentos restritos.



Fonte: o autor

4.4.2 Aquisição de medicamentos

O médico deve cadastrar sua carteira junto a agência governamental de saúde mediante a apresentação dos documentos exigidos pela mesma. A agencia governamental, depois de verificar se o cadastro obedece aos critérios estabelecidos, cadastra a carteira do

médico e a habilita a criar NFTs que representam permissões de compra.

O médico, depois de ter a sua carteira cadastrada no contrato inteligente, atende a seus pacientes e insere a receita médica no sistema. A receita médica é armazenada no sistema pelo médico e os NFTs que representam permissões de compra para medicamentos restritos são gerados. O médico solicita permissão ao cliente para ver seusdados.

Todas as informações necessárias para a venda de medicamento restrito estarão no NFT e no endereço do médico que fez o *deploy* no NFT. Além disso, o contrato que fará o *deploy* das NFTs será único e deverá ser o utilizado pelo médico.

Quando o paciente dá a permissão, o médico terá acesso aos dados médicos do cliente e também ao endereço da carteira. O médico pode então transferir as NFTs para a carteira do cliente. Além de transferir as permissões de compra para a carteira do paciente,o médico pode imprimir a receita médica para o paciente. Desta forma, o paciente poderáler as prescrições médicas na aplicação ou na impressão entregue pelo médico.

A permissão de compra representada pela NFT indica exatamente o medicamentoque foi solicitado pelo médico e a quantidade em caixas do mesmo. Estas informações são exibidas para o farmacêutico. A aplicação irá ler a NFT e informar o médico sobre oque pode ser feito.

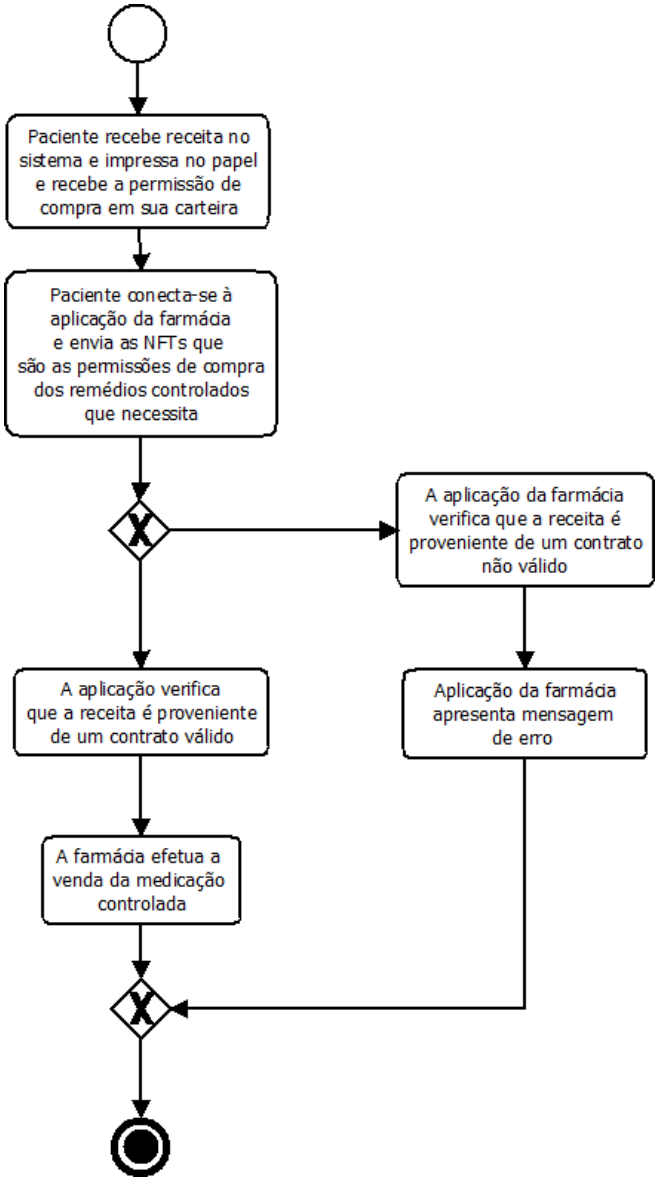
As NFTs servem para o farmacêutico prestar contas junto da agênciagovernamental (Figura 5). A agência governamental verifica de tempos em tempos se a agência governamental possui a quantidade de NFTs que corresponde a quantidade de medicamento vendido pela farmácia, de acordo com a legislação vigente. Quando o paciente for comprar medicamentos de uso restrito, o farmacêutico poderá verificar o contrato que emitiu o NFT. Caso o contrato seja o certificado pela agência governamental,o token é valido.

O paciente pode solicitar o recibo de compra do medicamento (tanto restrito quanto do não-restrito) para o farmacêutico. Além disso, ele poderá acessar esse recibo em seu sistema, ao selecionar a receita utilizada e clicando na opção “recibo de uso”. Nelaconstará o nome da farmácia que vendeu o medicamento para o paciente, o código do medicamento e a data em que o medicamento foi adquirido. Estas transações serão possíveis através de consultas que serão executadas pelo sistema automaticamente. É possível recuperar informações de NFTs emitidas na Blockchain sem custos para o usuário, uma vez que a taxa de gás de uma Blockchain é exigida apenas quando são efetuadas mudanças na mesma.

Nesse sentido, quando o paciente for comprar medicamentos de uso restrito, o farmacêutico poderá verificar o contrato que emitiu o NFT. Caso o contrato seja o certificado pela agência governamental, o token é valido.

Assim, o processo de compra manterá a privacidade do paciente, uma vez que os seus dados médicos ficam armazenados sob a proteção de sua chave privada no sistema da agência governamental e o seu endereço na blockchain não é atrelado a pessoa física do cliente da farmácia. Ao mesmo tempo, o processo a ser implementado através de uma ferramenta de Blockchain fornecerá ao farmacêutico os meios de verificar a validade das receitas médicas e das permissões em posse dos pacientes, sem risco de uso inadequado dos mesmos.

Figura 5: Processo de compra da medicação



Fonte: o autor

4.5 IMPLEMENTAÇÃO DO CONTRATO INTELIGENTE

O contrato das NFTs será criado na blockchain através de linguagem de programação apropriada Solidity, para ser construído na rede Ethereum. Os testes do contrato primeiramente seriam feitos em uma blockchain que possibilite o cumprimentode todos os requisitos apontados acima, contudo foi constatado que a criação das receitase sua transferência requerem mais de um minuto e que a taxa de gás nessa rede é proibitiva.

O contrato inteligente que irá emitir a receita médica e também a permissão de

compras, deverá ser desenvolvido através do padrão ERC721, uma vez que cada receita possui informações próprias e personalizadas. O desenvolvimento do ERC721pode ser feito de duas formas. A primeira, mais utilizada na implementação de NFTs, é fazer o token apontar para um endereço na forma de um URI (Identificador Universal de Recurso) que possui um arquivo JSON com os atributos do NFT. A segunda é inserir as informações específicas do token embarcadas na própria cadeia (também conhecido como *"on chain"*) no próprio token, na rede da blockchain.

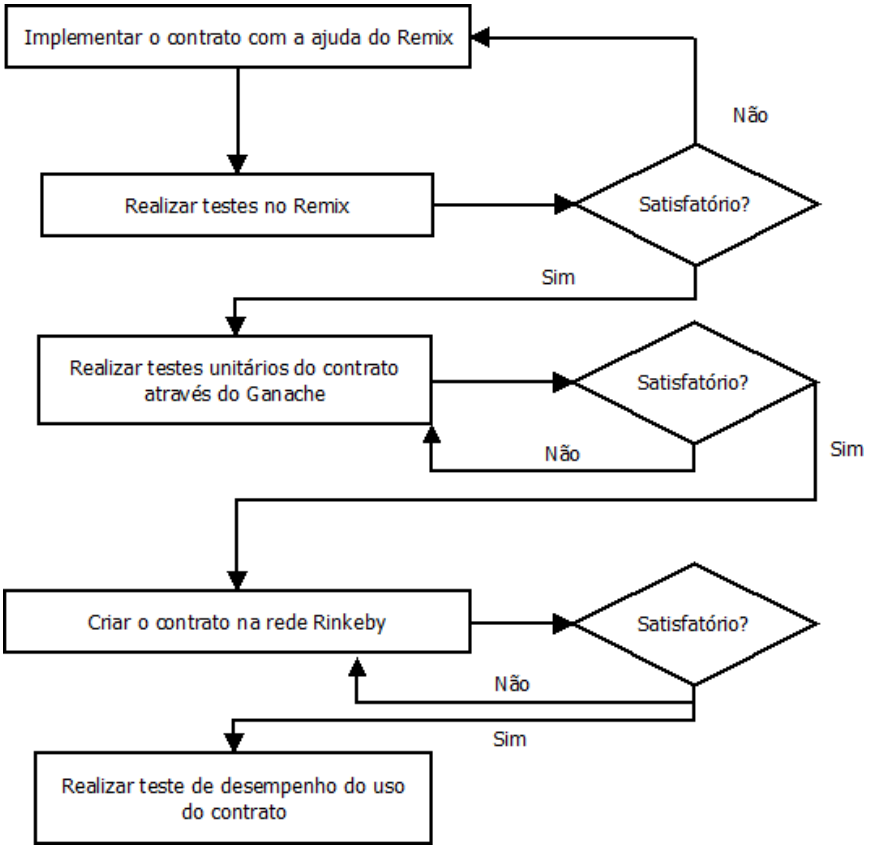
A segunda opção é mais adequada para implementar a metodologia proposta por dois motivos: *(i)* será utilizado uma rede de segunda camada que possui taxas de gás (o custo relativo a transação em uma blockchain) consideravelmente baixas, além de que poucas informações precisaram ser armazenadas *on chain* e *(ii)* o armazenamento *on chain* é mais seguro, uma vez que todas as informações ficam na blockchain sem o risco de serem perdidos ou corrompidos. A Figura abaixo ilustra a arquitetura do sistema proposto.

4.6 FUNCIONAMENTO DO SISTEMA

Esta seção apresenta o funcionamento do contrato de emissão de permissão de compra para medicamentos através da arquitetura do sistema e da interação que os diferentes atores terão com a respectiva arquitetura. Além disso, é mostrado o processo de desenvolvimento do contrato inteligente.

O processo seguido para o desenvolvimento do contrato inteligente é apresentado abaixo na Figura 6. Primeiramente o contrato foi criado através do ambiente interativo do Remix, onde é possível criar e testar as funções uma por uma por meio de uma rede que o Remix cria no browser do desenvolvedor. Depois de criado e testado o contrato no Remix, é possível inseri-lo no ambiente de desenvolvimento feito através do framework Brownie, utilizando a linguagem de programação Python. Foi possível criar testesunitários através do Ganache, de forma a verificar se as saídas para determinadas entradas estavam corretas. Depois disso, o contrato pôde ser criado e testado na rede de testes realda rede Polygon.

Figura 6: Implementação e testes do contrato de NFT voltado para medicamentos



Fonte: o autor

O contrato foi desenvolvido a partir do modelo de ERC-271 disponibilizado pela Open Zeppeling, modelo este amplamente utilizado pelo mercado. Dada a sua utilização ampla e aceitação do mercado, infere-se que ele implementa os requisitos de segurança necessários referentes a posse dos NFTs.

Foram incluídos ao modelo os requisitos necessários a este sistema em particular, como por exemplo a regra de que apenas as carteiras autorizadas dos médicos podem emitir as NFTs com as receitas através do contrato emitido pelo órgão de saúde responsável.

5 EXPERIMENTOS E RESULTADOS

Este capítulo discute o processo de avaliação utilizado para validar as funcionalidades do modelo proposto utilizando a prova de conceito desenvolvida. Primeiro, ele irá discutir a metodologia utilizada para realização dos experimentos com a arquitetura. Em seguida, ele apresenta os resultados e conclusões obtidos através da avaliação.

5.1 EXPERIMENTO

Para simular o funcionamento do sistema proposto acima, neste trabalho foi desenvolvido um contrato que cria NFTs capaz de armazenar as informações de receitas médicas *on-chain, i.e.* as mesmas serão armazenadas na blockchain de forma segura e sem a necessidade de ser custodiada por qualquer pessoa ou instituição.

A implementação foi feita no sistema Windows 10 e através do WSL (*Windows-Subsystem For Linux*). No WSL foi instalado o Ubuntu 20.04. Neste sistema do Ubuntu foi instalado o Python versão 3.8. Para auxiliar no desenvolvimento do contrato inteligente foi instalado o framework Python chamado Brownie que auxilia o desenvolvedor nessa tarefa.

O contrato inteligente foi desenvolvido através do Solidity. Esta linguagem de programação é orientada a objetos e de alto nível utilizada para o desenvolvimento dos contratos inteligentes na rede Ethereum. Ela é utilizada também nas redes de segunda camada da Ethereum, como a Polygon. As redes de segunda camada são soluções que visam aumentar a escalabilidade da rede da Ehtereum e consequentemente reduzir os custos das operações nessa rede.

Inicialmente os testes foram efetuados na rede de testes da Ethereum chamada Rinkeby, porém foi observado que as taxas de transação são consideravelmente elevadase que o tempo para criação das NFTs e transferência das mesmas são consideravelmente elevados. Por conta disso, foi adotada uma alternativa de segunda camada mais escalável,que é a rede Polygon. A rede Polygon possui uma rede de testes chamada Mumbai, na qual foram realizados os testes com a arquitetura proposta.

Na rede de testes da Polygon (chamada Mumbai), para avaliar a escalabilidade da solução, foram realizados testes com numero crescente de requisições em rajadas (10,20,30,50,100,200,300) visando verificar a latência entre as requisições e respostas. Foram realizadas 4340 transações de criação e transferência de permissões de compra de medicamento para verificar a velocidade que as transações são executadas e o custo destas operações na rede depois de implementado o contrato inteligente na rede Mumbai, as transações correspondem a execução da função *create_colectable* e posteriormente a execução da função *transfer* herdada da classe ERC721 (vide o contrato no Apêndice B). Adicionalmente, foi analisada a quantidade de memória principal que a criação do contrato inteligente demanda e que a criação de um token do sistema demanda, visando verificar o requisito de memória dos dispositivos que serão utilizados pela agência governamental, médico, paciente e farmacêutico (que podem muitas vezes desejar utilizar dispositivos móveis). Esta verificação foi feita através do módulo *Memory Profiler* disponível para scripts Python.

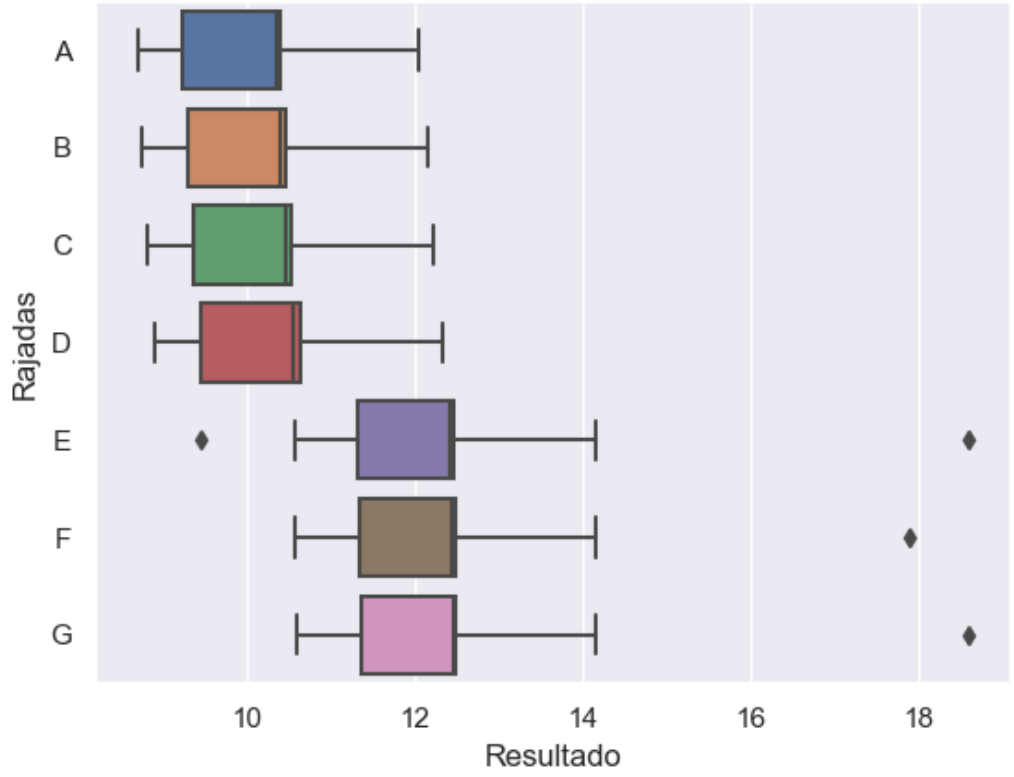
As limitações das rajadas de teste se dão perante o uso de um nó dentro de uma blockchain de terceiro, existe a limitação e um aumento do tempo de resposta desses testes, onde para uma melhor eficácia, seria necessário ter um nó proprietário dentro da mesma. De forma simples, um node (“nó”) de rede é o ponto onde uma mensagem pode ser criada, recebida ou transmitida. Em uma estrutura de blockchain, é sua unidade mais básica e parte crítica, armazenando seus dados e permitindo que toda a comunicação (transações) passe por ele. Além disso, existe também a necessidade da mineração de MATIC, moeda da rede Polygon para realizar as transações, que por mais que possuam um custo muito baixo, se faz necessário.

5.2 ANÁLISE DOS RESULTADOS

O box plot da Figura 7 mostra o tempo para a criação das NFTs em rajadas de 10,20 e 30 solicitações em paralelo, sendo que o tempo considerado foi o tempo de criação mais demorado da rajada. Foram efetuadas rajadas de criação de token em paralelo para verificar se o tempo de criação dos tokens é alterado com requisições feitas em um mesmoinstante. Foi constatado que o tempo médio aumenta levemente quando executadas maisoperações em paralelo devido ao overhead da máquina que executou o teste.

O tempo de execução no experimento da Figura 8 foi menor do que 15 segundosem todas as operações realizadas. Além disso, no experimento as transações gastaram emmédia 0,0009 Matic (o que equivale a R$0,005 durante o período de realização dos experimentos) e o tempo de duração das transações foi em média 10,3 segundos para os experimentos que realizaram poucas rajadas (até 10 rajadas), sendo assim, os resultados foram satisfatórios (10 a 100). De fato, este é o tempo que muitas vezes se espera para a aprovação de compras no cartão de crédito. No caso da execução de centenas de rajadas, há um aumento no tempo médio na execução. Este aumento deve-se provavelmente a limitações da máquina em que os experimentos foram executados. Não deve ocorrer em situações normais em que o equipamento irá executar normalmente 1 por vez operação apenas.

Figura 7: Tempo para a criação do NFT em rajadas de 10 (A), 20 (B), 30 (C), 50 (D),100 (E), 200 (F) e 300 (G) solicitações de criação de tokens em paralelo. O resultado é o tempo em segundos de espera para a execução completa da operação.



Fonte: o autor

Além disso, algumas transações foram executadas em paralelo com carteiras diferentes e elas foram todas bem-sucedidas. O código desta rede é aberto e pode ser utilizado inclusive em uma rede dedicada para receitas médicas caso seja pertinente a implementação da mesma pelo Conselho Federal de Medicina para a emissão de receitas,por exemplo. Nesse caso, os preços de transações seriam similares.

A Polygon é capaz de processar até 65000 transações por segundo (CHRISTODORESCU, 2021). Ou seja, a redecapaz de processar mais de 5 bilhões de transações por dia. No Brasil, são consumidasem média duas doses por habitante, o que (extrapolando, caso fosse gerada uma receita por dose de medicamento – o número de receitas restritas geradas diariamente é bem menor) resulta em cerca 500 milhões de vendas de medicamento por dia (MAGALHÃES et al., 2021). A quantidade de receitas emitidas anualmente é de cerca de 4 bilhões ao ano no País, o que dá em média 11 milhões de receitas diárias, contando receitas restritas e não restritas (LEONARDI, 2020). Assim, a rede da Polygon (que é uma rede de produção onde a solução comercial do sistema pode ser executada) suporta a criação de um NFT gerado por medicamento consumido no Brasil. É importante observar que apenas uma fração destes 500 milhões de vendas é de medicamentos restritos.

Assim sendo, a proposta deste trabalho pode ser implementada na rede Polygon para a venda de todos os medicamentosrestritos que acontecem no Brasil, uma vez que esta rede possui escalabilidade adequada.

A criação dos tokens consome 95 MB de memória principal. Isso pode ser realizado, portanto através de sistemas computacionais com recursos limitados. Celularespopulares a preços acessíveis atualmente possuem 2 GB de memória principal, o que é mais do que o suficiente para processar os scripts de criação das NFTs. Já a criação do contrato inteligente consome 100 MB para ser criado, o que é um consumo baixo e permite que o contrato inteligente seja criado em servidores ou em dispositivos dedicados de baixa capacidade computacional.

Através da execução do sistema na rede de testes de uma segunda camada da Ethereum foi verificado que é possível *(i)* obter taxas consideravelmente baixas para a emissão e transferências de NFTs, *(ii)* o tempo de emissão e transferência de NFTs é consideravelmente baixo, de poucos segundos, sendo que os mesmos podem ser processados em paralelo e em grandes quantidades por conta da escalabilidade da Polygon e *(iii)* a quantidade de memória que a criação do contrato inteligente e de uma NFT requer é baixa, sendo possível fazer este processamento em dispositivos móveis como *smartphones*.

6 CONCLUSÕES

Este trabalho apresentou ao leitor a solução para a arquitetura de um sistema de emissão de receitas médicas que funciona inteiramente dentro da Blockchain. Foi ilustrado o funcionamento deste sistema através da implementação de um contratointeligente na rede de testes da Polygon (segunda camada da Ethereum) chamada Mumbainetwork. A Polygon é altamente escalável e foi feita uma análise que indica a possibilidade de implementação do Sistema em todo o País.

Foi apresentado o modelo de arquitetura para o gerenciamento da venda de medicamentos controlados, completa que é necessária para um sistema de emissão de receitas médicas através da rede Ethereum. Foi apresentada a solução de software para a criação de tokens não-fungíveis (chamados NFTs) que representam receitas médicas. As receitas são públicas por estarem na blockchain, contudo as informações privadas são inseridas de forma criptografada.

No sistema criado e testado neste trabalho, os tokens podem ser criados por carteiras autorizadas e enviados para a carteira dos clientes, que podem transferir para os farmacêuticos. Os farmacêuticos podem então provar através destes tokens como prova de que venderam os medicamentos corretamente.

O contrato implementado é capaz de emitir tokens que representam receitas médicas e possuem as informações da receita armazenados on-chain na blockchain. O contrato foi feito através de modelo amplamente utilizado no mercado e reconhecidamente seguro. Foram realizados testes que demonstraram que o tempo de emissão do token é aceitável (menor do que 15 segundos e em média 10,3 segundos). O consumo de memória por parte do dispositivo que solicita a emissão do token é de menosde 100 MB, o que torna possível a emissão via aparelhos celulares populares, por exemplo. Por fim, a emissão das permissões de compra custa menos de R$ 0,01, o que faz o sistema ser economicamente viável. Os resultados obtidos foram submetidos na forma de um artigo científico para publicação no XXIII Simpósio em Sistemas Computacionais de Alto Desempenho.

Como trabalho futuro, é importante que seja feito um teste de aceitação do sistema junto ao público, tanto médico quanto dos pacientes dos médicos. É interessante verificar como as diferentes classes sociais podem aderir ao uso do sistema eletrônico e estudar alternativas para mitigar possíveis resistências de cada um destes públicos e verificar como estes grupos aceitam a possível monetização do sistema.

REFERÊNCIAS

ATALAG, Koray et al. Evaluation of software maintainability with openEHR–a comparison of architectures. **International journal of medical informatics**, v. 83, n. 11, p. 849-859, 2014.

MA, Fuchen et al. Pied-Piper: Revealing the Backdoor Threats in Ethereum ERC Token Contracts. **ACM Transactions on Software Engineering and Methodology**, 2022.

CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. Blockchains and smart contracts for the internet of things. **Ieee Access**, v. 4, p. 2292-2303, 2016.

MATTILA, Juri. The blockchain phenomenon. **Berkeley Roundtable of the International Economy**, v. 16, 2016.

SWAN, Melanie. **Blockchain: Blueprint for a new economy**. " O'Reilly Media, Inc.", 2015.

CHRISTODORESCU, Mihai et al. Universal Payment Channels: An Interoperability Platform for Digital Currencies. **arXiv preprint arXiv:2109.12194**, 2021.

AUTOMEDICAÇÃO. Biblioteca Virtual em Saúde, 2012. Disponível em: https://bvsms.saude.gov.br/bvs/dicas/255_automedicacao.html. Acesso em: 26 mai. 2021.

SILVA, Angélica Baptista et al. Electronic health records in high complexity hospitals: a report on the implementation process from the telehealth perspective/Registro eletronico de saude em hospital de alta complexidade: um relato sobre o processo de implementacao na perspectiva da telessaude. **Ciencia & saude coletiva**, v. 24, n. 3, p. 1133-1143, 2019.

LOPES, Maick Roberto. Lucas Santana Freires Jessicamaki Hirakawa Terra. **Gestão e Eficiência**, p. 46. 2019

AZARIA; EKBLAW; VIEIRA; LIPPMAN. "MedRec: Using Blockchain for Medical Data Access and Permission Management," **2nd International Conference on Open and Big Data (OBD)**, 2016, p. 25-30, set. 2016. Disponível em: https://ieeexplore.ieee.org/abstract/document/7573685. Acesso em: 16 mai. 2021.

LEONARDI, Egle. Nova lei obriga prescrição médica eletrônica no Brasil. Disponível em: https://ictq.com.br/varejo-farmaceutico/1289-nova-lei-obriga-prescricao-medica-eletronica-no-brasil.

BUTERIN, Vitalik. **Ethereum White Paper**: A NEXT GENERATION SMART

CONTRACT & DECENTRALIZED APPLICATION PLATFORM. **Blockchainlab**.

2017. 2017 p. Disponível em: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform- vitalik-buterin.pdf Acesso em: 16 nov. 2020.

CHICARINO, Vanessa R. L; et. Al. Uso de Blockchain para Privacidade eSegurança em Internet das Coisas. ResearchGate, Sociedade Brasileira deComputação – SBC, p.1-51, cap. 4. Disponível em:https://www.researchgate.net/profile/Vanessa-Rocha-Leandro-Chicarino/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas/links/5a3b92aaaca272774f9baf5a/Uso-de- Blockchain-para-Privacidade-e-Seguranca-em-Internet-das-Coisas.pdf. Acessoem: 26 mai. 2021.

DUMPETI, Naveen Kumar; KAVURI, Radhika. Uma estrutura para gerenciar certificados educacionais inteligentes e impedir a falsificação de um blockchain permitido. **Materials Today: Proceedings,** Índia, v. 44, jan. 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214785321008373. Acesso em: 16 mai. 2021.

FLORES, Nikka; ENTERIA, Maryl; PEFIANCO, Marco. Electronic Medical Record Database with Accessible Online Summary and Statistics. Acm Digital Library, p; 86-90, set. 2020. Disponível em: https://dl.acm.org/doi/fullHtml/10.1145/3429551.3429592. Acesso em: 27 mai. 2021.

GIT-Farmácia Digital/CFF conhece a experiência do Conect SUS. Conselho Federal de Farmácia. 2019. Disponívelem:https://www.cff.org.br/noticia.php?id=5573. Acesso em: 18 mai. 2021.

GOVERNO DO BRASIL. Você Conhece o SUS? Aplicativo Mostra Toda a SuaTrajetória de Atendimento no Sistema Único de Saúde. Disponível em:https://www.gov.br/pt-br/noticias/saude-e-vigilancia-sanitaria/2021/04/voce- conhece-o-conecte-sus. Acesso em: 27 de junho de 2021.

HIPERLEDGER-FABRIC. Developing Applications. Disponível em: https://hyperledger-fabric.readthedocs.io/en/latest/developapps/wallet.html. Acesso em: 29 de junho de 2021.

IBM. What are smart contracts on blockchain. Disponível em: https://www.ibm.com/topics/smart-contracts. Acesso em: 27 de junho de 2021.

ISMAIL, Leila; MATERWALA, Huned. BlockHR: uma estrutura baseada em Blockchain para gerenciamento de registros de saúde. **12th International Conference on Computer Modeling and Simulation,** Austrália, p. 164-168, jun. 2020. Disponível em: https://dl.acm.org/doi/10.1145/3408066.3408106. Acesso em: 16 mai. 2021.

ISMAIL, Leila; MATERWALA, Huned; KHAN, Moien AB. Avaliação dedesempenho de uma estrutura de gerenciamento de registros de saúde baseadaem Blockchain centrado no paciente. **2nd International Electronics Communication Conference,** Cingapura, p. 39-50, jul. 2020. Disponível em: https://dl.acm.org/doi/10.1145/3409934.3409941**.** Acesso em: 16 mai. 2021.

JAMIL, Faisal; et al. Um novo modelo de blockchain médico para gerenciamento de integridade da cadeia de suprimentos de medicamentos em um hospital inteligente. **Electronics**, Coréia, v. 8, n. 505, p. 1-32, abr./mai. 2019. Disponível em: https://www.mdpi.com/2079-9292/8/5/505/htm. Acesso em: 16 mai. 2021.

JIAMSAWAT, Watchara; CHOKSUCHAT, Chidchanok; MATAYONG, Sureena. Blockchain-Based Electronic Medical Records Management of Hospital Emergency Ward. In: **2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)**. IEEE, 2021. p. 674-679.

LEZCANO, Leonardo; SICILIA, Miguel-Angel; RODRÍGUEZ-SOLANO, Carlos. Integrating reasoning and clinical archetypes using OWL ontologies and SWRL rules. **Journal of biomedical informatics**, v. 44, n. 2, p. 343-353, 2011.

LI, Jian. Um novo sistema de transferência de registros médicos eletrônicosbaseado em Blockchain com privacidade de dados. **Instituto de EngenheirosElétricos Eletrônicos: 5ª Conferência Internacional sobre Ciência da Informação, Tecnologia da Computação e Transporte (ISCTT),** Shenyang,China, nov. 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/9363808/references#references. Acesso em: 16 mai. 2021.

LI, Zhiyong; ZHANG; Lihui. Um Mecanismo de Proteção de Privacidade e Compartilhamento de EMR com Base no Blockchain do Consórcio Médico. **International Conference on Computer and Technology Applications,** p. 160-164, abr. 2020. Disponível em: https://dl.acm.org/doi/10.1145/3397125.3397153#sec-ref. Acesso em: 16 mai. 2021.

MARTINS, Geraldo José Dolce Uzum. **Avaliação do blockchain aplicado no processo de compras de uma organização**. 2019. Tese de Doutorado. Universidade de São Paulo.

MAE, Zifa. MATIC (Polygon) Is Exploding. Here is Why. 2022. Disponível em: https://changelly.com/blog/matic-polygon-is-exploding/. Acesso em: 27 de nov de 2022.

MARTINS, Geraldo José Dolce Uzum. **Avaliação do blockchain aplicado noprocesso de compras de uma organização.**. São Paulo, 2019. Dissertação (Engenharia de Produção) - Universidade de São Paulo. Disponível em: https://teses.usp.br/teses/disponiveis/3/3136/tde-07052019-083831/pt-br.php Acesso em: 3 jul. 2021.

MASSI, Viviane. Como funciona a compra de medicamentos pelos SUS. ICTQ. Disponível em: https://www.ictq.com.br/varejo-farmaceutico/826-como-funciona- a-compra-de-medicamentos-pelo-sus Acesso em 07 jun. 2021

MIERS, Charles; PILLON, Maurício; KOSLOVSKI, Guilherme; SIMPLICIO, Marcos. Análise de Mecânismos de Consenso Distribuído Aplicado a Blockchains. Researchgate. 2019. Disponível em: https://www.researchgate.net/publication/338913728_Analise_de_Mecanismos

_para_Consenso_Distribuido_Aplicados_a_Blockchain/download. Acesso em:28 de junho de 2021.

MINISTÉRIO DA SAÚDE. Emissão de Atestados e Receitas Médicas na teleconsulta. 2020. Disponível em: https://aps.saude.gov.br/noticia/8316. Acessoem: 21 de junho de 2022.

MIRAZ, Mahdi H.; ALI, Maaruf. **Applications of Blockchain Technology beyond Cryptocurrency**. **arxiv.org**. 2018. 6 p. Disponível em: https://arxiv.org/ftp/arxiv/papers/1801/1801.03528.pdf Acesso em: 15 nov.2020.

OPEN ZEPPELING. ERC721. Disponível em: https://docs.openzeppelin.com/contracts/4.x/erc721. Acesso em: 8 de abr. de 2022.

OpenEHR. What is OpenEHR? Disponível em: https://www.openehr.org/about/what_is_openehr. Acesso em: 11 de maio de 2022

PAHL, Christina et al. Role of OpenEHR as an open source solution for the regional modelling of patient data in obstetrics. **Journal of biomedical informatics**, v. 55, p. 174-187, 2015.

POLYGON. POLYGON WHITEPAPER. Disponível em:

https://polygon.technology/lightpaper-polygon.pdf. Acesso em: 11 de maio de2022.

Prescrição Digital. Media CRFRS. 2020. Disponível em: https://media.crfrs.org.br/publicacoes/materiais-impressos/ebook- prescricao.pdf. Acesso em: 18 mai. 2021.

ROEHRS, Alex; et al. Analisando o desempenho de uma implementação de registro de saúde pessoal baseada em blockchain. **Journal of Biomedical Informatics**, ScienceDirect, v. 92, p. 1-9, abr. 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S1532046419300589. Acesso em: 16 mai. 2021.

ROUMELIOTIS, Nadia et al. Effect of electronic prescribing strategies on medication error and harm in hospital: a systematic review and meta- analysis. **Journal of general internal medicine**, v. 34, n. 10, p. 2210-2223, 2019.

SEOK, Byoungjin; PARK, Jinseong; PARK, Jong Hyuk. A Lightweight Hash- Based Blockchain Architecture for Industrial IoT. **Applied Sciences**, Korea, v.9, n. 18, p. 3740, 2019. Disponível em: https://www.mdpi.com/2076-3417/9/18/3740/pdf Acesso em: 15 nov. 2020.

SILVA, Eduardo; FERNANDES, Dione; TERRA, André. Uma Abordagem Ao Uso Indiscriminado De Medicamentos Benzodiazepínicos. 2019. Disponível em: https://repositorio.faema.edu.br/bitstream/123456789/2175/1/UMA%20ABORDAGEM%20AO%20USO%20INDISCRIMINADO%20DE%20MEDICAMENTOS%20BENZODIAZEP%C3%8DNICOS.pdf. Acesso em: 18 de Agosto de 2022.

SILVEIRA, M. UNIVCHAIN: **Um modelo para autenticação de documentos acadêmicos. Tese** (Pós-Graduação em Computação Aplicada). Universidade do Vale do Rio dos Sinos - UNISINOS. São Leopoldo, p.89. 2020.Wang, S; Ouyang, L; Yuan, Y; Ni, X; Han, X; Wang, FY. **Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends.** *IEEE Trans. Syst. Man Cybern. Syst.* 2019, *49*, 2266–2277.

WANG, S .; Ouyang, L .; Yuan, Y .; Ni, X .; Han, X .; Wang, FY Blockchain- Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* 2019 , *49* , 2266–2277.

YANG, Baohua. Welcome Hyperledger Fabric 2.0. Enterprise DLT for Production.

YFANTIS, Vasileios; LELIGOU, Hellen C.; NTALIANIS, Klimis. Novo desenvolvimento: Blockchain - uma ferramenta revolucionária para o setorpúblico. **Taylor e Francis Online,** set. 2020. Disponível em: https://www.tandfonline.com/doi/figure/10.1080/09540962.2020.1821514?scroll

=top&needAccess=true. Acesso em: 16 mai. 2021. Zheng, Z; Xie, S.; Dai, H .; Chen, X .; Wang, H. Uma Visão Geral da Tecnologia Blockchain: Arquitetura, Consenso e Tendências Futuras. **Proceedings of the 2017 IEEE 6th**

LUCENA, Antônio, HENRIQUES, Marco. Estudo de Arquiteturas dos blockchains Bitcoin e Ethereum. IX Encontro de alunos e doscentes da DCA/FEEC/UNICAMP. Disponível: https://diegoazziufabc.files.wordpress.com/2017/08/estudo-de-arquiteturas-dos-blockchains.pdf. Acesso em: 13 de nov. de 2022.

International Congress on Big Data (BigData Congress), Honolulu, HI, EUA,25-30 de junho de 2017; pp. 557–564.

ZAWORSKI, Korand; SZPYRKA, Marcin. Patient Managed Patient Health Record Based on Blockchain Technology. Advances in Diagnostics of Processesand Systems, p.173-184, jan.2021.Disponível:https://www.researchgate.net/publication/347601379_Patient_Managed_Patient_Health_Record_Based_on_Blockchain_Technology. Acesso em: 28 mai. 2021.

Zheng, Z .; Xie, S .; Dai, H .; Chen, X .; Wang, H. Uma Visão Geral da TecnologiaBlockchain: Arquitetura, Consenso e Tendências Futuras. Em Proceedings of the 2017 IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI, EUA, 25-30 de junho de 2017; pp. 557–564.

MAGALHÃES Alline; WERNECK Carolina, BATISTELLA Paulo, BERALDO Paulo, AGUIAR, ABDO, Sara; TEÓFILO Sarah. Nas farmácias, venda de remédio subiu 42% em cinco anos. Estadão. 2021. Disponível em: https://infograficos.estadao.com.br/focas/tanto-remedio-para-que/checkup-1.php#:~:text=Em%20um%20ano%2C%20o%20brasileiro,ajuda%20de%20programas%20do%20governo. Acesso em: 2 de novembro de 2022.

APENDICE A – Exemplo de prescrição médica em OpenEHR

Exemplo de prescrição encontrada no site oficial do padrão OpenEHR disponível no seguinte endereço: https://openehr.atlassian.net/wiki/spaces/healthmod/pages/62062602/Examples+of+use+of+Medication+order+archetype+and+associated+cluster+archetypes

Template Name	ePrescription (FHIR)
Meta Data	Template IS: ePrediscription (FHIR) MetaDataSet:Sample Set: Template metadata sample set
Purpose	Example of na openEHR Medication order, profiled to fit a FHIR Medication Orders

Data

Prediscription Composition	Set of medication orders communicated to the farmacy
Other Context	
Prediscription Identifier	an identifier for the prediscription as a whole
Medication order Optional,Repeting	Instructions for use of a medication, vaccine or other therapeutic item
Order Activity Optional, Repeting	Order
Medication item Text Mandatory	Identification of the medication, vaccine or other therapeutic item being ordered
Preparation Cluster	The strength and form of the medication substance, including details of the specific ingredients where required by an ad-hoc preparation of infusion.
Substance Name Text	The name of the medication substance. Should be coded if possible.
Form Text	The formulation of presentation of the medication

Strength Quantity	The value of the strength of the medication
Strength unit	Strenght of a dose of the medication

Diluent Cluster	The strength of any diluent used as part of the preparation
Diluent amount Quantity	The value of the amount of diluent used as part of the preparation
Diluent unit text	The unit of the preparation diluent
Ingredient Cluster	Details of a ingredient
Ingredient substance Cluster	The strength and form of the medication substance, including details of the specific ingredients where required by an ad-hoc preparation of infusion.
Substance Name Text	The name of the medication substance. This item should be coded
Form Text Optional, Repeat	The formulation of presentation of the medication
Category Code, text	The nature of compound product consisting of multiple ingredients
Strength Text	The value of the strength of the medication
Strength unit Text	Strenght of a dose of the medication
Description Text	A description of the substance when it is not possible to describe this fully using numerical strengths

APÊNDICE B – Contrato ERC721 das permissões de compra

```
contract AdvancedCollectible is ERC721 {

    bytes32 internal keyHash;
    uint256 public fee;
    event requestedCollectible(address indexed senderAdd);
    mapping(address => bool) public medico_cadastrado;

    uint256 public tokenCounter;
    uint256 public medicosCount;

    address public agencia_governamental;

    struct Remedio {

      uint256 registroMS;
      uint256 quantidade;

   }



    mapping(uint256 => address) public requestIdToSender;
    mapping(uint256 => Remedio) public tokenIdToRemedio;
    mapping(uint256 => uint256) public requestIdToTokenId;



    constructor() public ERC721("GeradorReceitasMedicas",
        "Receita")
    {
        agencia_governamental = msg.sender;

        tokenCounter = 0;
    }

    function add_medico(address medicoAddress) public{

        require(msg.sender==agencia_governamental);

        medico_cadastrado[medicoAddress] = true;

        medicosCount = medicosCount + 1;
    }
```

```
    function createCollectible(uint256 registroMS, uint256 quantidade)
    public returns (bytes32) {

        require(medico_cadastrado[msg.sender]);

        uint256 newItemId = tokenCounter;

        tokenCounter = tokenCounter + 1;

        Remedio memory newRemedio = Remedio({
           registroMS: registroMS,
           quantidade: quantidade
        });

        requestIdToSender[newItemId] = msg.sender;
        address receitaOwner = requestIdToSender[newItemId];

        _safeMint(receitaOwner, newItemId);

        tokenIdToRemedio[newItemId] = newRemedio;

        emit requestedCollectible(receitaOwner);

    }


}
```